ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (PhD) THESIS FOR HOME DEFENSE

SILVANA QOSE

Cybersecurity in Blockchain Technology (Case study Healthcare)

Supervisor: Prof. Dr. Rajnai Zoltán

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

Date:13/February/2026

Contents

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Since the start of Blockchain in Satoshi Nakamoto's 2008 study[1], it has evolved as a popular way for safeguarding the storage and movement of information in an environment that is devoid of trust. A literature review of decentralized technology and peer-to-peer systems is included in this thesis. Additionally, a scientific study of the blockchain security applications that are most frequently used in cybersecurity activities is presented. Based on the findings, the Internet of Things (IoT), machine visualization, and public-key cryptography are all suitable for blockchain applications. Especially true when it comes to the safe storage of identifiable information as well as online applications and certification schemes. This study is based on systematized research that was published in several different scholarly journals. The purpose of this research is to provide a supplementary appraisal of prospects in Blockchain and cybersecurity research. More specifically, the research will concentrate on the safety of Blockchain in the Internet of Things and sidechain security, as well as blockchain security for artificial intelligence data.

Recently, blockchain technology has received much interest due to the extraordinary tamper-resistant properties it possesses as well as the robust security it offers. It is anticipated that the industry will reach 1.2 billion United States dollars by the year 2030, expanding at a rate of 82.8 percent on an increasing annual basis[2].

In recent reports, many vulnerabilities and breaches in blockchain technology have been discovered; this highlights the vital demand for a robust blockchain security and proficient management to guarantee safety and optimal functionality.

Research Goals and Questions

To narrow the scope of the task, that is, examining previous studies and their conclusions, we have established the two research questions given in the table below:

Table 1. Research Questions

Research Question 1: What is the role of the Blockchain in enhancing Cyber Security? Blockchain characteristics may address issues with the security of devices, networks, and users.
Research Question 2: Which are the most recent blockchain security applications? Blockchain applications have expanded beyond money. A survey of the most recent practical applications will help comprehend the entire scope of blockchain technology's influence on cyber-security.
Research Question 3: What are the Blockchain-Based applications in the healthcare industry: challenges and limitations?

Integration, safety and privacy, sustainability, efficiency, and patient engagement have been identified as barriers to creating blockchain-based applications. Concerns have been raised about the security and privacy of blockchain-based healthcare applications because, despite the encryption methods, it may still be feasible to determine a patient's identity on a public blockchain by connecting enough data related to that patient.

1.1. Research Aims and Their Relevance in the Context of the State-of-the-Art

For the purpose of investigating the use of blockchain technology in a variety of crucial industries that are necessary for the development of technology, such as the military, finance, and healthcare. A case study of the healthcare industry served as the basis for this implementation, which was designed to ensure safety.

A summary of the study endeavors in blockchain applications for cybersecurity and their deployment in the healthcare sector is going to be provided by this research. The purpose of this research is to investigate the present studies and the findings that they have reached. Subsequently, we will establish a policy that asserts that employing Blockchain

for the storage of all healthcare data is the most secure option, hence boosting user-friendliness. This policy will be based on previous studies regarding the security of Blockchain. In addition, it might be helpful in other research that concerns protecting the privacy of patients. Why not create a system that can be used all over the world and that can be implemented within hospitals? The system would provide them the ability to fund themselves using the cryptocurrency that is generated by the integrated Blockchain.

1.2. Organization of The Thesis and Main Directions

The profound theoretical aspects of control and signal processing are pervasive in all mechanical or electrical systems. This theoretical aspect offers a systematic methodology for designing control and signal processing algorithms for practical engineering challenges involving big data. Consequently, more advanced algorithms are necessary in adaptive systems like Blockchain. This project proposes novel algorithmic strategies for collecting and protecting substantial amounts of sensitive data, and a policy that might be followed for better security.

1.3. Research Methodology

We have selected cybersecurity in Blockchain Technology, both theoretically and practically, as the focus of this Ph.D. thesis based on the research design. In principle, cybersecurity trials rely on on-chain data; nevertheless, software development's current status and centralization complicate this process. We have successfully implemented it in a bank in Albania to assess how the Blockchain interacts with sensitive and large datasets.

CI has conducted a comprehensive study on Blockchain Technology, including an in-depth analysis of historical cyber dangers and the steps implemented to mitigate them. Thus, we refrain from undertaking studies that have already been conducted. Additionally, we investigated the potential applications of Blockchain within the medical system to facilitate its internationalization. Based on the information collected, we developed these three algorithms to serve as the primary framework for implementing Blockchain in healthcare.

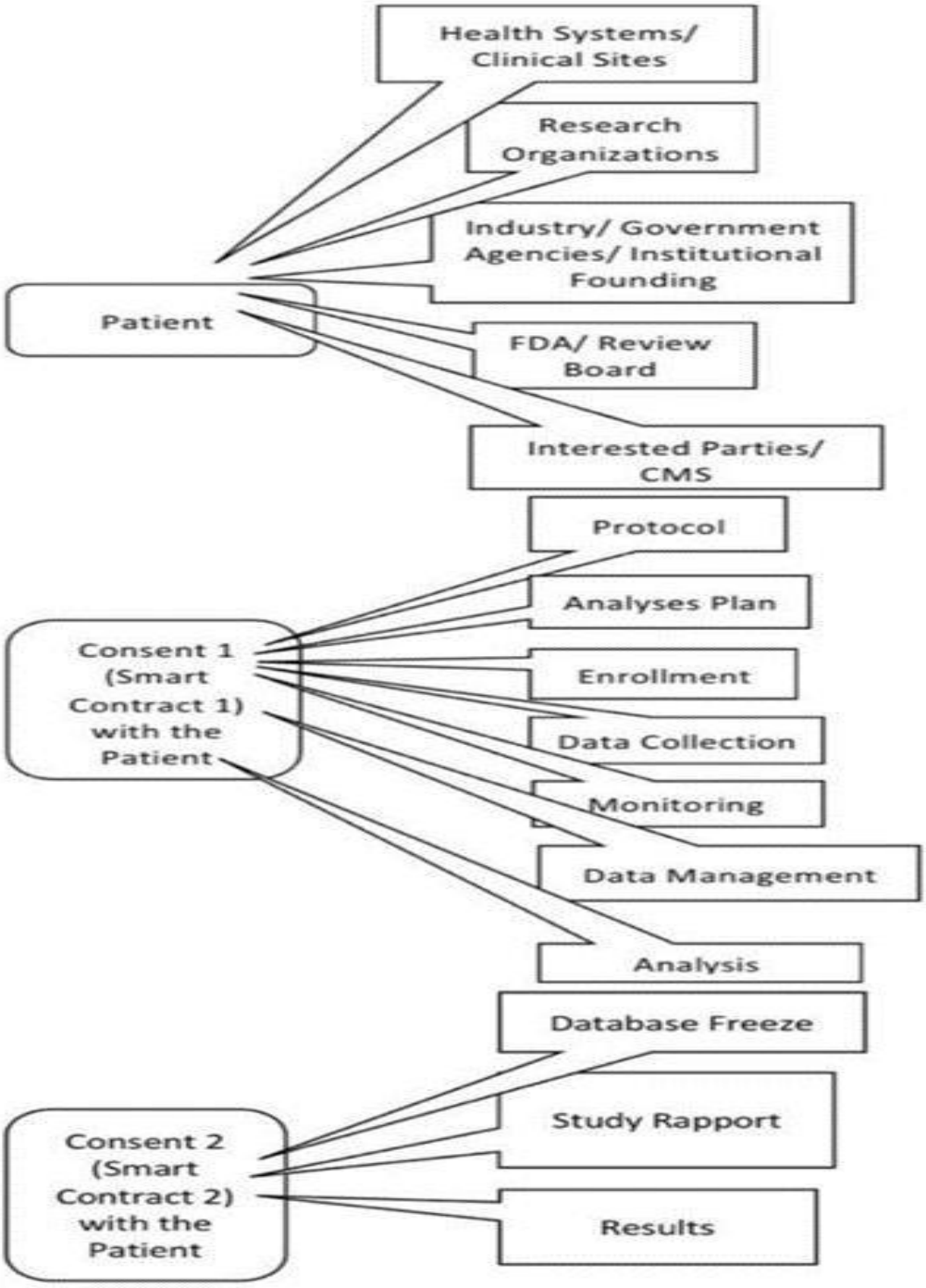


Figure 1. Main Algorithms

2. LITERATURE ANALYSE

We have collected data and conducted research using RStudio and the Biblometrix library to enhance our comprehension of existing Blockchain studies and identify future research directions for a deeper understanding.

This research commenced in January 2022 and is scheduled to conclude in May 2025. The criteria employed to select the research include actual data about Blockchain and its security, the publications in which it appears, and the citations it has received. Among the selections, we identified numerous research studies; however, those pertinent to the research questions yielded 986 findings, which were then reduced to 894 after removing duplicates. After reviewing them and the criteria required for this study, we selected only 20 for the first review. However, we have chosen an additional 124 for the forthcoming research.

Upon analyzing the study data and their efficacy, we selected nine publications to inform our work. The paper should be critiqued, focusing on the application of blockchain technology to address a specific issue. Secondly, the study must have sufficient material to precisely elucidate the application of the Technology to a specific context, solve the research questions we have posed, and clarify the security concerns and data collection methods. We can evaluate the accuracy and the methodology of data collection, measurement, and presentation.

For this Ph.D. thesis, we have selected the topic of cybersecurity in Blockchain Technology, encompassing both theoretical and practical aspects, based on the study design. In principle, cybersecurity trials rely on on-chain data; nevertheless, software development's current status and centralization complicate this process.

We have conducted a comprehensive study on Blockchain Technology, including an in-depth analysis of previous cyber threats and the steps implemented to mitigate them. Thus, we refrain from undertaking studies that have already been conducted. Additionally, we have investigated the potential applications of Blockchain within the medical system to facilitate its internationalization.

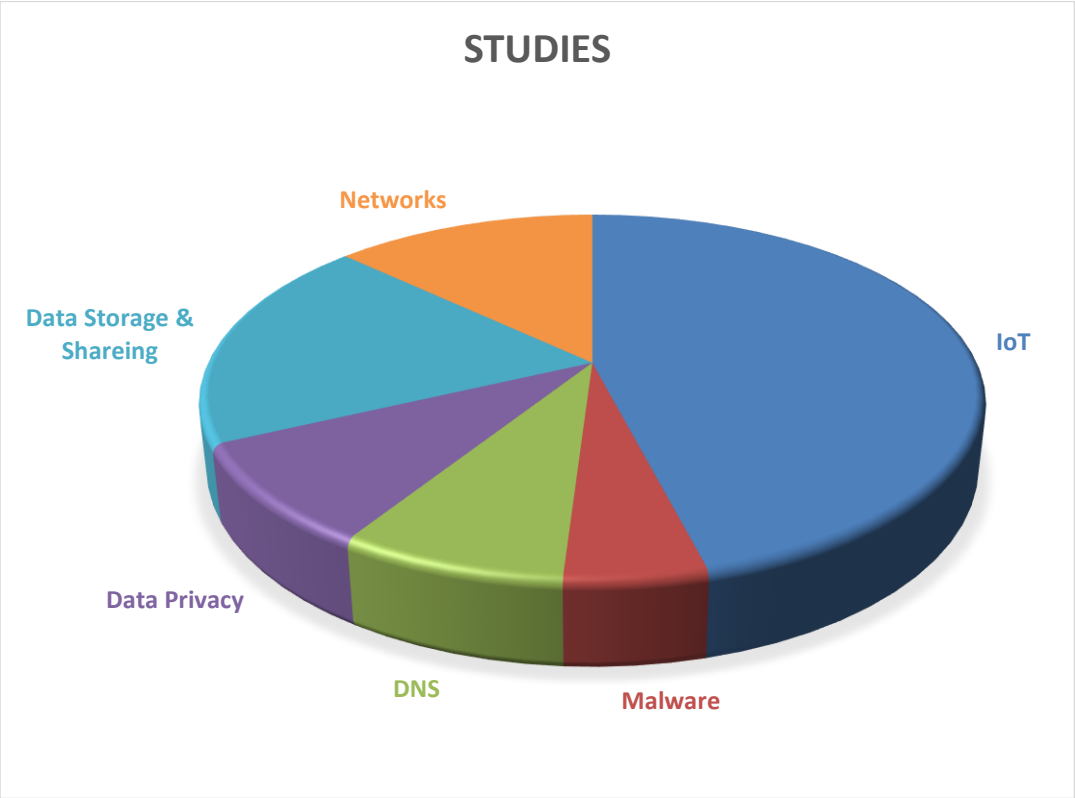


Figure 2. Studies' percentage related to my research topic. (HEALTHCARE)[1]

In the theoretical study, we analyzed numerous articles and studies related to the objectives and two research issues. A technique was employed to select the principal research conducted in recent years. Subsequently, we eliminated any duplicates to pick the primary studies conducted thereafter. We reviewed the abstracts of the chosen study to ensure alignment with the research questions pertinent to the paper's objective. We then reviewed the entire document to identify the primary implications of their research and select the key elements for further investigation.

Based on the study, further research is necessary in Data Storage and Sharing, as it is the primary subject with the most issues. The Internet of Things (IoT), a field with extensive research and current popularity, should address issues, particularly in smart homes and Healthcare, if we explore new methods for securing data within blockchain technology.

[1] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

This report offers further proof of Blockchain Security research. It has contributed to a greater comprehension of the principal areas that require further investigation. Additional research is necessary to examine the resolutions of Data Storage and Sharing issues.

Blockchain technology may eliminate the necessity for one central authority to oversee and authenticate agreements and transactions among many parties. All mining nodes cryptographically hash and authenticate each transaction in the Blockchain. It produces immutable, secure, and accessible time-stamped records for all parties. A significant topic that is swiftly gaining prominence is artificial intelligence (AI), which enables robots to gather information from data and make decisions based on their acquired knowledge, despite numerous competing technologies designed to render data in smart homes impervious to attacks. The progression of distributed ledger technology is considered one of the most promising methods for safeguarding network connections from command-and-control attacks on encrypted data and providing a secure interface for all networked devices. The blockchain nodes reach a consensus to guarantee the permanent recording of all transactions. Consequently, executing a controlled attack on information transmitted or saved within a singular transaction is challenging. Consequently, for an attack to succeed, the supremacy of centers must be compromised. The concept of decentralized artificial intelligence has progressed in recent years. Decentralized AI, or blockchain-based AI, integrates both technologies. It enables the transmission and preservation of dependable, precisely labeled, and disseminated data on the Blockchain in a collaborative and intermediary-free manner. Currently, it is anticipated that Blockchain will provide a secure platform for data storage, whereas simulated intelligence is expected to operate with substantial data quantities. Smart contracts can be inscribed into blockchains, facilitating reliable third parties to manage user data sharing and access. Algorithms may adapt and learn once integrated into an electronic system, under various technological conditions; This results in accurate and reliable decision-making outcomes that receive universal consensus from all blockchain network nodes. Consequently, trust and endorsement for these decisions may originate from all parties invested in the outcome. Blockchain-based AI methodologies facilitate the decentralized determination of optimal strategies to foster trust and security in disseminating information and decision-making outcomes among numerous independent participants who contribute to, organize, and vote on future resolutions. The integration of AI with

blockchain technology yields numerous beneficial consequences. Blockchain technology enables the secure storage of patient records in the healthcare sector. Medical practitioners may acquire valuable insights from the patterns identified by AI in this data if granted access. BurstIQ, a blockchain-based company offering data solutions for the healthcare sector, utilizes Blockchain, artificial intelligence, and big data to manage patient Information through a health wallet, which exemplifies innovation. Medical practitioners may utilize the wallet to access patient health data as needed. The integration of these technologies is revolutionizing the financial services sector by enhancing transaction speeds and fostering mutual trust. This study will analyze the literature on the combination of AI and Blockchain to aid new researchers, stay up to date with developments in the field, and provide suggestions for improving the quality of future research.

2.1. Blockchain Security, AI and Healthcare

The responses to the RQs from the critical review that came before are included here. The application of the AI, blockchain, and healthcare combo has significantly advanced thanks to this study. This section discusses the foundations, variants, development teams, systems, and consensus mechanisms of the AI and smart contracts combo. In the future, more in-depth discussions will be held on the significance and uses of blockchain technology in conjunction with AI. Here are the answers to the RQs from the previous comprehensive examination. This research improves distributed ledger technology and AI combined to help the healthcare industry and others.

We used RStudio to conduct this research. The research is included below in Why RStudio.

2.2. Analysis of Databases and Bibliometric Data

The primary pertinent issue is the growing accessibility of bibliometric data [3]. Datasets may be amalgamated and reevaluated to tackle various research questions. The availability of many types of organized, unstructured, and semi-structured data [4] that can be integrated in diverse ways. In recent years, there has been an increase in large-scale databases and the growth of various data type typologies, including full texts,

abstracts, citations, keywords, and co-authors [5]. Scientometrics is an emerging field that is currently evolving. Mingers and Leydesdorff (2015) [6]illustrate the various phases in the evolution of regions. The authors identify various phases in the sector's development.

Scientometrics encompasses distinct phases that can be delineated: Garfield articulated the quotation's significance and introduced the Science Citation Index [7] The relevance was associated with the network analysis of various papers, considering de Solla Price's work (1965)[8], which emphasized the significance of paper networks. The expansion of the paper network is notable and aligns with the overall increase in datasets within the sector.

In the literature on Symbolic Data Analysis [9], an approach has been developed that focuses on aggregate observations, referred to as 'higher observations,' which represent 'higher-level concepts,' rather than solely on individual observations. [10]examined an approach that facilitates the consideration of big data. The author examined extensive network data, decomposing it and representing it as symbolic observations.

Symbolic observations (aggregate data) enable the conduct of big data analysis. Relevant knowledge will be extracted from these data, specifically from co-occurrence networks, co-authorship networks, and co-citation networks. Relevant knowledge will be extracted from these data, specifically from co-occurrence, co-authorship, and co-citation networks.

The initial step involved the creation of the library data set.

Data were collected from the SCOPUS database on January, 2022, using the query "regression and discontinuity," which was then limited to the technology field.

We have conducted a targeted search for papers in AI, Economics, Finance, and Econometrics. A total of 969 papers have been collected. The papers were gathered using bibliometric data, including the title, authors, abstract, keywords, and related elements.

Ultimately, we achieved the initial summarization of the relevant literature by examining its overarching bibliometric trends.

We have explicitly considered various data types, including numeric data (e.g., the year) and textual data (e.g., the abstract). The primary transformation of the initial data matrix is the capacity to generate a network that illustrates the co-occurrence of the keywords analyzed in the studies.

2.3. How Bibliometric Works on Big Data Analysis.

Below, you can find the reasoning behind my choosing Bibliometrix to analyze the data that I gathered for the literature review.

The adjacency matrix A_{ij} is as follows: A_{ij} if an edge exists between the distinct vertices i and j; otherwise, A_{ij} = 0. [11]

We commence by defining a network in this manner:

G = (V, E) [11]

Let V represent the network's vertices, and E denote the edges that connect the various vertices[12]

Networks are defined as undirected, unweighted graphs devoid of self-loops. A graph G is defined as a pair G = (V, E), where V = $\{v_1, ..., v_n\}$ represents a finite set of vertices

with |V| = n, and E = $\{e_1, ..., e_m\} \subseteq V \times V$ denotes the set of edges with |E| = m.

A graph can be depicted using an adjacency matrix of size An × n. The generic element is as follows: $a_{i,j}$ = 1 if $(v_i,v_j) \in E$; $a_{i,j}$ = 0 if $(v_i,v_j) \notin E$.

The adjacency matrix of an undirected graph is generally symmetric.

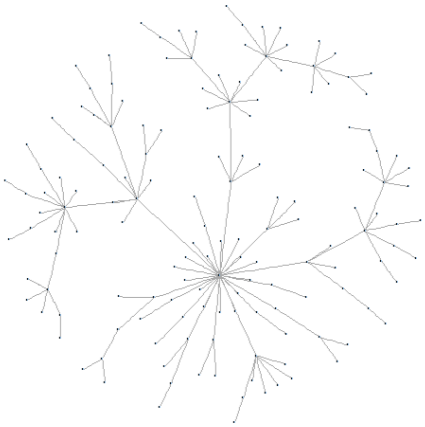


Figure 3.Network Visualization[2][3]

For each vertex v_k, we calculate the structural indicators for the complete networks, specifically the Freeman degree:

$C_D(v_k) = \sum_j a_{k,j}$ j and the betweenness centrality:

$C_B(v_k) = \sum_{k \neq i \neq j \epsilon v} \sigma_{i,j}(v_k) \Big/ \sigma_{i,j}$

σij k≠i≠j∈V, which denotes the centrality of each vertex vk within the network.

At the end:

$C_C(v_k) = \left(\sum_{j=1}^{n} d(v_k, v_j)\right)^{-1}$

[2] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

[3] https://blogs.cornell.edu/info2040/2022/09/03/graphs-as-adjacency-matrices/

Where d(v_k,v_j) is the distance between two distinct nodes, the clustering coefficient, which measures the degree to which different nodes are likely to cluster on a specific network, can also be considered.

$$C_i(v) = 3 * \text{number of network triangles} \Big/ \text{number of connected triple of nodes}$$

Simultaneously, pertinent metrics for the entire network can also be represented.

Density: The ratio of the total number of vertices to the potential number of vertices in a network. Centralization of the network for each structural indicator of centralization

$$C_x = \sum_i^n C_x(z^*) - C_x(z_i) \Big/ max \sum_{i=1}^n C_x(z_i)$$

$C_x(z^*)$ represents the highest value of the structural indicator inside the network, and $C_x(z_i)$ denotes the value of the individual observation i.

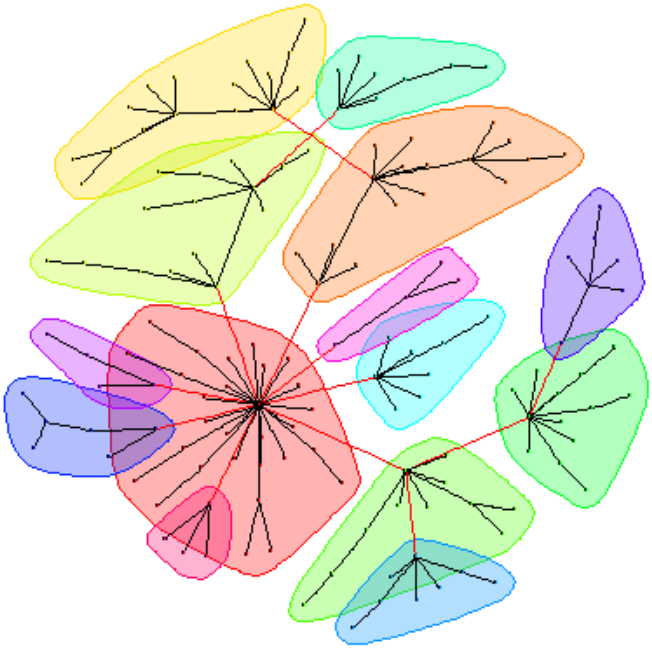


Figure 4. Community Composition[4][5]

A network has a specific community structure if the nodes can be grouped into densely connected sets with" many edges joining vertices of the same cluster and comparatively few edges joining vertices of different clusters"[13]

Communities typically provide a distinct and pertinent role inside a network.

Distinct patterns, such as analogous node properties, typically define them.

[4] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

[5] https://blogs.cornell.edu/info2040/2022/09/03/graphs-as-adjacency-matrices/

A pertinent issue is identifying communities inside a network. The precise number of communities remains undetermined. The many communities inside a network can be distinctly defined by their sizes and densities. A variety of algorithms have been presented to accomplish this task. It is essential to evaluate the computational expense of employing a community discovery technique on extensive networks [14]

Community structure

The definition of interval is:

$I[X]=[\alpha,\beta]=\{X \in R:\alpha \leq X \leq \beta\}$

We represent the community structure with interval data [15]

In particular, we consider each community as a single interval by considering the different structural indicators of each community [16]

Thus, we acquire interval data, each representing a distinct community:

$I[X]^b = [\alpha^b, \beta^b]$

Each structural indicator or property b possesses a distinct interval $[\alpha^1, \beta^1]$, $[\alpha^2, \beta^2]$,…, $[\alpha^B, \beta^B]$

The intervals exhibit pertinent qualities that may be significant in applications: the radii and the midpoints.

We can determine the midpoint of the interval:

$$X^b_{cener} = \frac{1}{2}(\alpha^b + \beta^b)$$

The radius of the interval:

$$X^b_{radius} = \frac{1}{2}(\beta^b - \alpha^b)$$

The communities can be regarded as distinct entities denoted by their intervals. To get the mean for each community [17]we can proceed as follows:

$$I[\bar{X}]^b = {}^1\!/_n \sum_{i=1}^{n} I[X]^b$$

Ultimately, we depict the complete community structure by utilizing interval scatterplots.

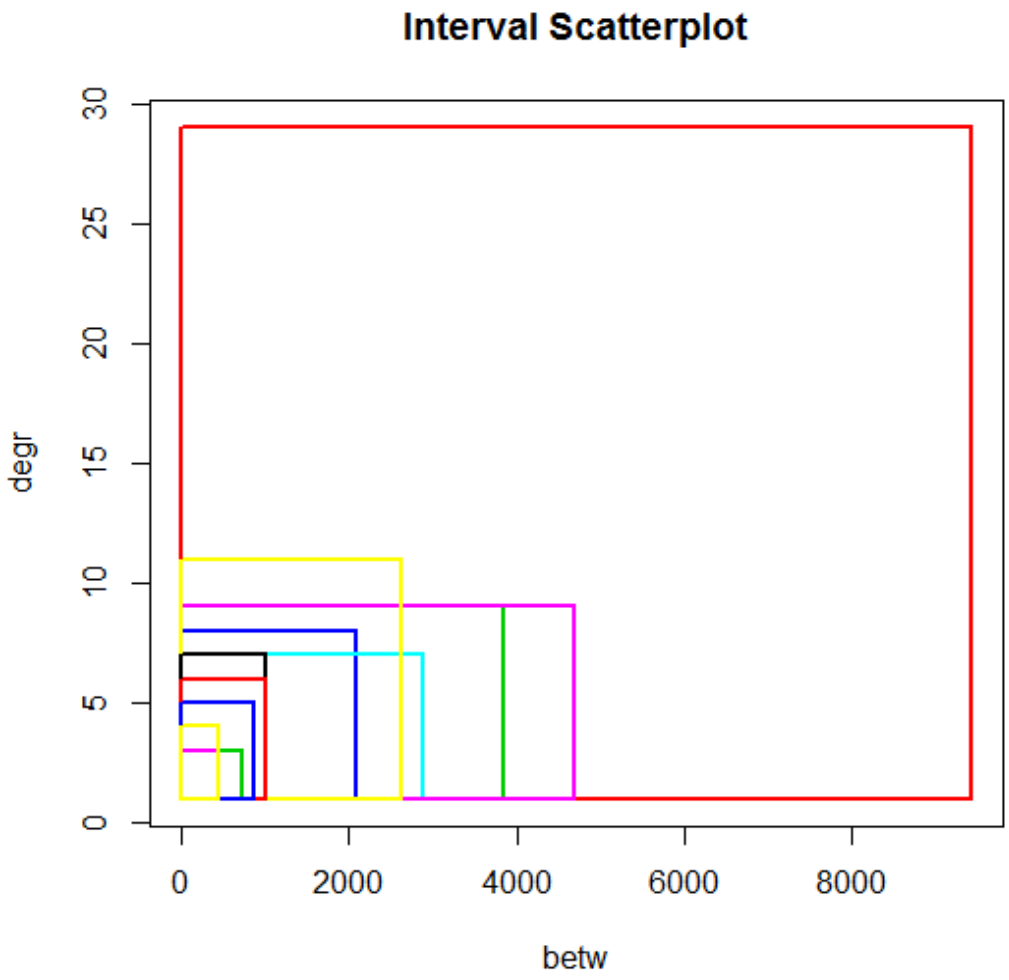


Figure 5. Community Composition: Example[67]

[6] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

[7] https://blogs.cornell.edu/info2040/2022/09/03/graphs-as-adjacency-matrices/

K-means clustering can be applied to interval data to categorize various communities while considering their characteristics.

The objective is to partition n observations into k ≤ n sets, denoted as S = $\{S_1, S_2, \ldots, S_k\}$, representing the various sets under consideration.

Multiple criteria exist to determine the number of sets k in the clustering process.

We have $I[X]^1, I[X]^2, \ldots,$ and $I[X]^m$, which can be derived from standardized variables [18]

It is essential to minimize the sum of squares across the various clusters.

We can determine:

$$argmin_S \sum_{i=1}^{k} \sum_{X_{center}^b \in S_i} \left\| X_{center}^b - \mu_i \right\|^2$$

In this context, μ_i represents the mean of each distinct cluster S_i.

Specifically, we focus on the centers of the examined intervals. Prototypes can be derived from the centroids.

Finally, we may interpret the results.

We examine many simulated networks with distinct structural attributes to test the algorithms.

- The Forest Fire Network Model [19]
- The Barabási-Albert Model [20]
- The Random Erdős-Rényi Model [21]

We have also evaluated various network sizes.

This exemplifies the Barabási model with 50,000 nodes.

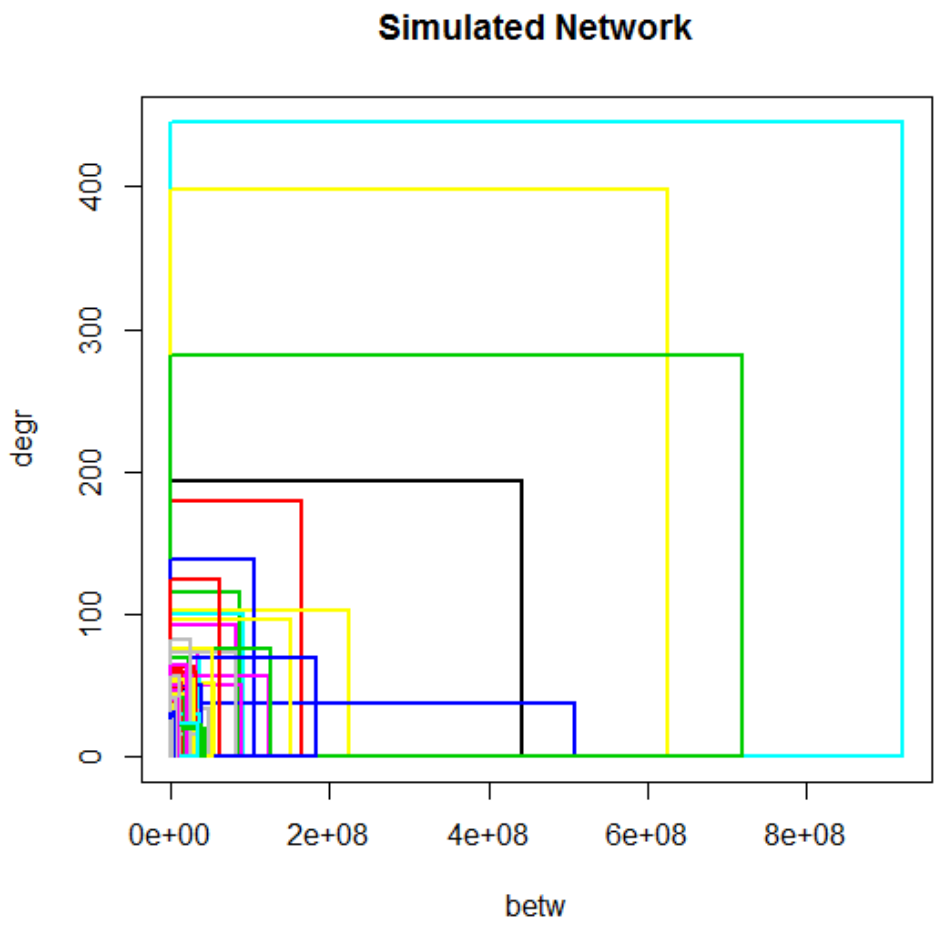


Figure 6. Community Composition. Example[89]

We can evaluate these interpretative principles derived from our simulations:

The interpretation of the scatterplot graphic depends on the selected variable. Similar communities can be identified by inspecting their shapes.

Identification of pertinent nodes: Nodes with elevated values are distinguished by a certain morphology.

[8] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

[9] https://blogs.cornell.edu/info2040/2022/09/03/graphs-as-adjacency-matrices/

Due to the network's centralized topology, the communities are often represented on scatterplot diagrams as overlapping. Greater betweenness is associated with a higher degree. In other instances, the outcome is not evident.

The lower bound is of minimal significance in the simulations conducted. In this context, the upper bound demonstrates significant disparities among the communities. The discrepancies in the upper bound dictate the variations across the distinct intervals.

The statistics pertain to the network of researchers in theoretical physics. The dataset is available on the SNAP website [22]

Specifically, we utilize the dataset about the "General Relativity and Quantum Cosmology collaboration network"[23]

Utilized methodologies: conventional procedures in Social Network Analysis, community detection, definition of interval data, statistical analysis of communities, visualization of community structure through structural indicators, and clustering via the K-Means algorithm.

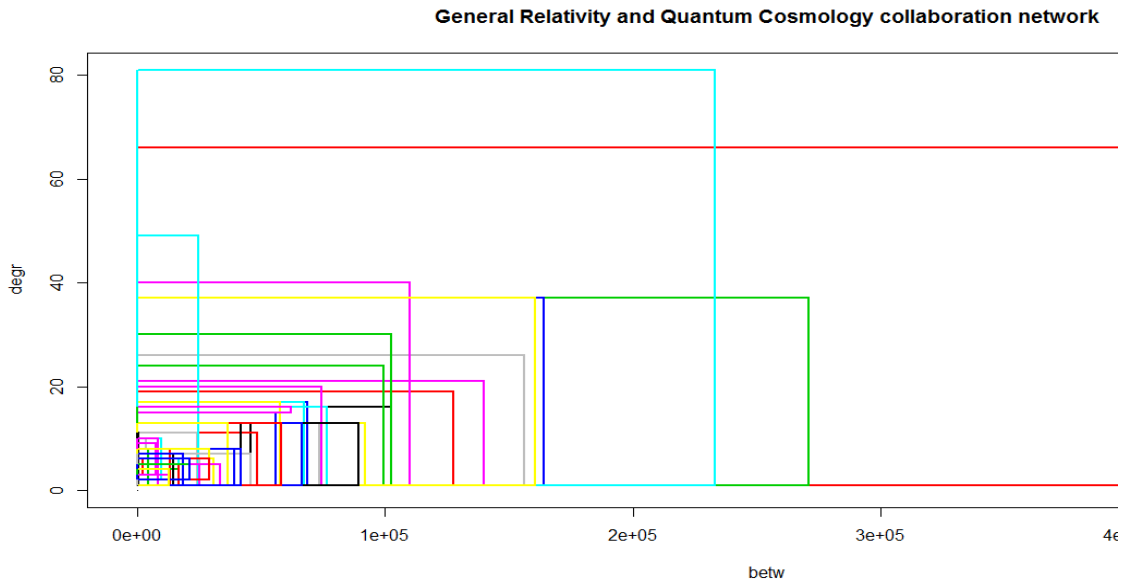


Figure 7. Community Composition: Example[1011]

After analyzing the network in question, we conducted a community detection assessment to identify the relevant communities that reveal significant patterns worth extracting from the literature. We employed the Walk Trap Community Detection Approach [24] yielding significant findings in the existing literature.

The approach outlined in "Symbolic Data Analysis" [25] facilitates the identification of pertinent communities of symbolic data that can be regarded as distinct "data" entities. Consequently, we can analyze and interpret the various observations as a significant collective. R has seen extensive application in computing [26]

Ultimately, we considered 1207 keywords in our network analysis [27]. The various keywords were examined through the lens of centrality indices, including Freeman's degree.

[10] https://blogs.cornell.edu/info2040/2022/09/03/graphs-as-adjacency-matrices/

[11] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

The significance of these two specific approaches in our examination lies in their ability to effectively illustrate the centrality patterns within our network. The significance of the literature within the network can be assessed by evaluating multiple metrics. The relationship is a comprehensive measure of centrality, determined by the ratio of paths that facilitate movement from a specific node to the entirety.

The degree is a local centrality measure, quantifying a node's connections with its neighboring nodes. The degree is the number of connections, referred to as "edges," that a single node can have with other nodes [27]. The primary objective of community detection is to identify groups of keywords that exhibit maximal connectivity within the works [28]. This may be pertinent for visualizing and identifying the relevant groups of keywords among the various w. The results facilitate identifying several communities in the literature associated with various groups of keywords.

2.4. The findings

Regarding community interpretation indicate a connection between the various themes associated with applying regression discontinuity and the methodologies that define or are related to regression discontinuity. The symbolic data facilitates comprehension of the centrality range applicable to each community or group.

Each community can be regarded as a "semantic core" within literature in this context.

Notably, the "1" community, pivotal to literary growth, is founded on regression and has significant applications in policy formulation, labor markets, and education.

Community "8" illustrates the relevant facets of health concerns. This community is associated with the interplay between health technology and regression discontinuity. This group is founded on the premise that the methodology of regression discontinuity, or causality analysis in general, is highly pertinent to health.

Notably, the term "propensity score" is included in this semantic core. This indicates a demand for applying this particular methodology within this specific domain, and observing this phenomenon in this context is intriguing.

This study addresses a critical issue in the application of Big Data.

An approach utilizing Symbolic Data Analysis has been considered, alongside a method that converts various communities within networks representing the original large data sets into symbolic observations. These specific data typologies enable us to examine semantic cores compared to isolated keywords.

We have identified the most pertinent features of the economics literature concerning "regression discontinuity," focusing on significant applications and methodologies employed.

Simultaneously, we have pinpointed pertinent focus areas for the new implementation of approaches and gained new insights into the existing literature.

The value derived from the literature is contingent upon the results obtained by examining various themes and keywords associated with the extracted communities.

After knowing why I have used Bibliometrix, we can provide the data selection to make the literature study.

2.5. Bibliometrix Research

This search produced 144 items in total, 144 of which were examined. This critical review includes all articles. The chosen papers are presented below, and the classification's general findings are described. Using RStudio ges' >library(bibliometrix), web-interface >biblioshiny().

Bibliometrix is a R package developed for quantitative analysis in scientometrics and bibliometrics. It offers instruments for importing bibliographic data from scientific databases (such as Scopus, Web of Science, PubMed, etc.), refining and analyzing the data, and producing visual representations.

2.5.1. Below are several significant characteristics of Bibliometrix:

Data Import: Compatible with formats exported from Web of Science, Scopus, PubMed, Dimensions, CrossRef, and others.

Descriptive Analysis: Provides insights into publishing trends, authorship patterns, significant sources, and keywords.

Network Analysis: Develops and examines co-authorship, co-citation, and keyword networks.

Thematic Mapping: Utilizes clustering and mapping techniques to identify emerging or declining subjects.

Visualization Tools: Produces graphs and plots for bibliometric mapping and summary.

2.5.2. Why Biblioshiny for interface?

Biblioshiny is the web-based interface for the Bibliometrix R package. It is intended for users who prefer a point-and-click graphical user interface to scripting in R. It enables the execution of robust bibliometric analysis and the interactive generation of visuals.

Essential Features of Biblioshiny: Import and examine bibliographic data from Scopus, Web of Science, PubMed, and other sources.

- **Descriptive analysis:** publishing trends, leading authors, most cited papers, etc.
- **Network analysis:** co-authorship, keyword co-occurrence, and co-citation networks.
- **Thematic analysis:** development of themes, thematic cartography.
- **Interactive visualizations:** tailored plots and graphs.

2.6. What is the current state of the research field?

This critical study examines the descriptive information obtained from the various publications published each year, the publication sources, and the average annual number of citations that academic publications receive. It also examines research papers that integrate AI and blockchain-based health, published between 2017 and 2025. Most of the articles on this topic were published in the Web of Science (WoS) journal (144 articles). Using RStudio.

Cybersecurity is a paramount worry linked to the proliferation of internet-based Technology, products, services, and networks. If cybersecurity constitutes prevention, then cyber forensics serves as the remedy. Both are equally vital components of digital security. This report offers a comprehensive bibliometric analysis of cybersecurity and Blockchain research published in the Web of Science over the last decade (2017–2025). The analysis encompassed annual publications, types of publications, and trends across many sectors, including publishing sources, organizations, researchers, nations, and keywords. The whole counting method was employed for citation analysis.

In contrast, fractional counting was utilized to examine co-citation, co-author collaborations, and keyword co-occurrences across all three domains. Additionally, timeline and burst detection analyses were conducted to elucidate notable topic trends and citations during the past decade. The study presents bibliometric findings for authors, organizations, countries, keywords, sources, and documents that exhibit the strongest collaborative linkages globally in cybersecurity and forensics. Current trends in subjects that have not been sufficiently explored, as well as prospective avenues, are also outlined.

The main information about the literature review is based on Bibliometrix.

In the figure below, we will find the main information about this research. Firstly, the timespan is based on the research conducted from 2017 to 2025. The sources for the articles are 106. The documents used are 144. Based on the articles, the biblioshiny has an annual growth rate of 26.36%. There are 542 authors in total, and 8 of them have articles alone. So 39.58% are International Co-authorships. The average number of co-authors for documents is 4.1, and the total keywords is 488. References are 8739 of all the documents taken into consideration. Documents' average age is 2.31, meaning most are in their last years. The average citation for the document is 15.81.

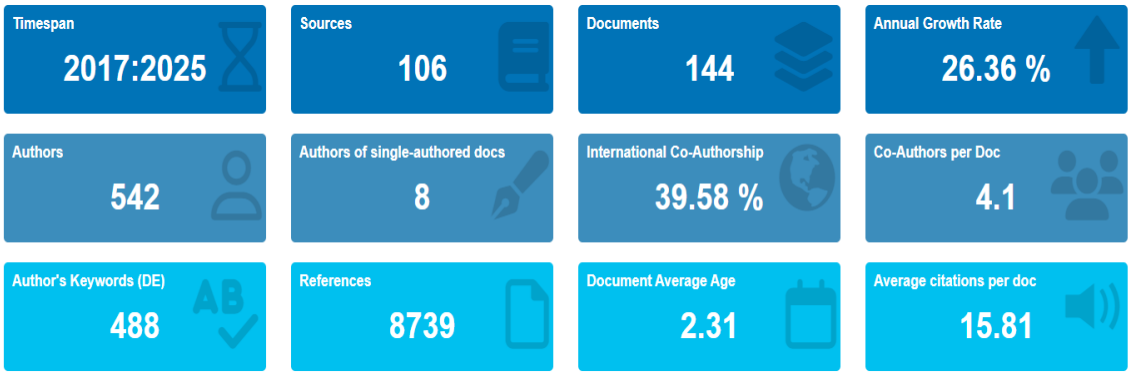


Figure 8. Main Information[12]

Key Words in the First Exploration: The full Records (Blockchain* AND cybersecurity* AND Healthcare*) is limited to English.

Key Words in the First Exploration: Full Records (Blockchain*OR cybersecurity* OR Healthcare*) is limited to English.

For both searches, we added AI, but it did not make any change. The change was with 2% which is the reason why we decided to use AND for the research, and without adding AI to the keywords.

The objective of the present study is to offer profound insights into, firstly, the principal contributors and collaborations in the domains of cybersecurity and Blockchain over the last decade and, secondly, to elucidate the most critical research areas, temporal trends of topic clusters, keywords, and scholarly articles. In light of the aforementioned studies, this work guides future research in this rapidly evolving field. The significance of this study is apparent due to the essential functions that cybersecurity and Blockchain serve in safeguarding the integrity and dependability of our digital information and transactions. Any concession in this matter may result in breaches of sensitive information or functioning, causing significant and irreversible losses. This research is significant for its bibliometric analysis, which comprehensively contributes to cybersecurity and Blockchain. Acknowledging the most influential researchers, institutions, nations, and

[12] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

journals and their collaborative efforts in this sector benefits the scientific research community. Secondly, the chronological progression of study subjects, topics, and keywords during the past decade aids researchers in directing their inquiries into obscure and underexplored areas. This study identifies significant future and emerging themes to assist forthcoming scholars and businesses in this sector.

Data origin, acquisition, and preliminary processing: bibliometric analysis of the current study. This database comprises an extensive collection of high-quality, high-impact research articles published in the world's most prestigious journals. It comprises a database of publications released in indexed journals from 1990. The Emerging Science Citation Index (ESCI), Science Citation Index Expanded (SCIE), Social Sciences Citation Index (SSCI), Arts and Humanities Citation Index (AHCI), Conference Proceedings Citation Index—Social Sciences and Humanities (CPCI-SSH), and Book Citation Index—Social Sciences and Humanities (CPCI-SSH) constitute the core collection of the Web of Science (WoS). BCI-SSH (Book Citation Index—Science), CPCI-S (Conference Proceedings Citation Index—Science), and BCI-S (Book Citation Index—Science) are also incorporated in WoS. This study's WoS document search string was formulated as follows: (Blockchain OR Cybersecurity OR Healthcare) covering a decade, from 2017 to 2027. The search parameters for the aforementioned phrases were configured to 'full record and cited references.' The search conducted in February 2025 resulted in 1,041,343 entries when employing the term "OR," and 144 entries while utilizing "AND" (Blockchain AND Cybersecurity AND Healthcare). We pulled the relevant articles from the database in BibTeX format for this research, which focuses on the intersection of Cybersecurity, Blockchain, and Healthcare. The search yielded accurate document entries that closely aligned with the keywords about cybersecurity, Blockchain, and Healthcare.

2.6.1. Analysis of publication structure

This section elucidates the distribution of the examined articles based on publication years, types, source titles, subjects, and trends in cybersecurity, Blockchain, and Healthcare studies. Furthermore, the leading nations, organizations, authors, and nationalities in cybersecurity, Blockchain, and Healthcare research, and their respective publication totals are also included. All results in this section were derived directly from

the Web of Science's filtered analysis options and applied to the complete document corpus retrieved using the search phrase referenced in the preceding section.

2.6.2. Annual publication analysis

Figure 9 illustrates the annual progression of Web of Science research publications in the domains of cybersecurity, Blockchain, and Healthcare. The x-axis represents the publication years spanning from 2017 to 2025, whilst the

The y-axis represents the quantity of WoS publications. The precise publishing counts are at the top of the annual publication bars. Between 2021 and 2025, the quantity of Cybersecurity, Blockchain, and Healthcare papers steadily rose. Since 2017, these figures have escalated significantly, indicating an increasing interest and demand in cybersecurity Blockchain Research in Healthcare. The volume of publications from 2021 to 2025 substantially increased compared to previous years. In 2021, the number of cybersecurity and Blockchain articles published in WoS exceeded four times the number of manuscripts released in the early years of the previous decade.

The proliferation of social networking and internet usage has led to an increase in cybercrime, necessitating accelerated research initiatives in cybersecurity and Blockchain. Consequently, scholars' interest in this perennial subject is expected to persist, as demonstrated in Figure 10. This Figure illustrates an exponential decrease in 2017-2019 citations, but between 2020-2021, we can see an exponential increase and then a drop somewhat until 2025 for cybersecurity and Blockchain WoS publications. This subsection delineates the various categories of WoS publications in this domain.

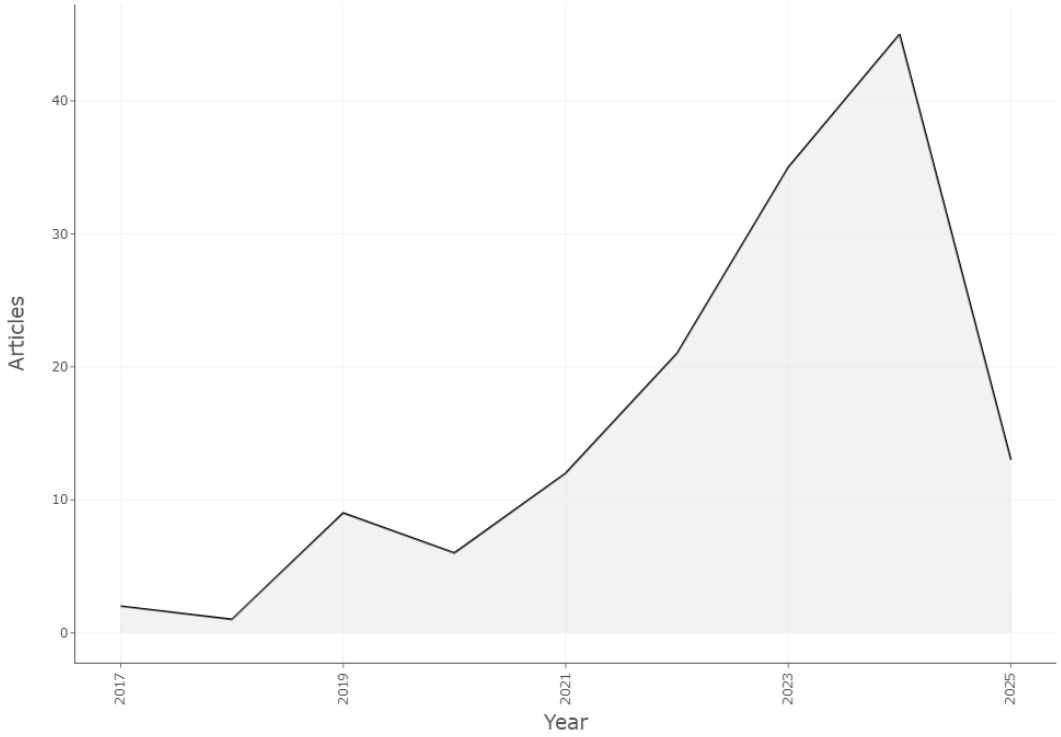


Figure 9. Annual Scientific Progression of Cybersecurity, Blockchain, and Healthcare from 2017-2025[13]

[13] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

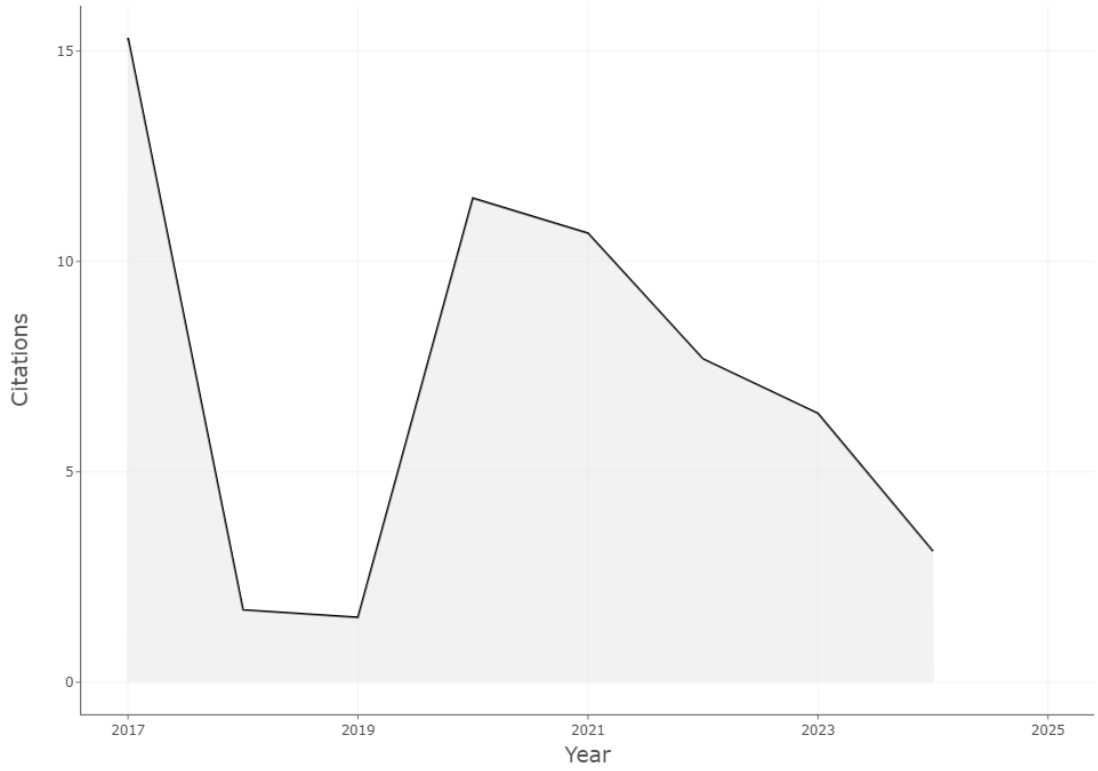


Figure 10. Average annual citation per year.[14]

2.6.3. Publication Type

The WoS database search produced 144 publications in cybersecurity, blockchain, and Healthcare, including research articles, conference proceedings, review papers, early access materials, and additional formats. Figure 11 illustrates all categories of publications together with their respective counts.

[14] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

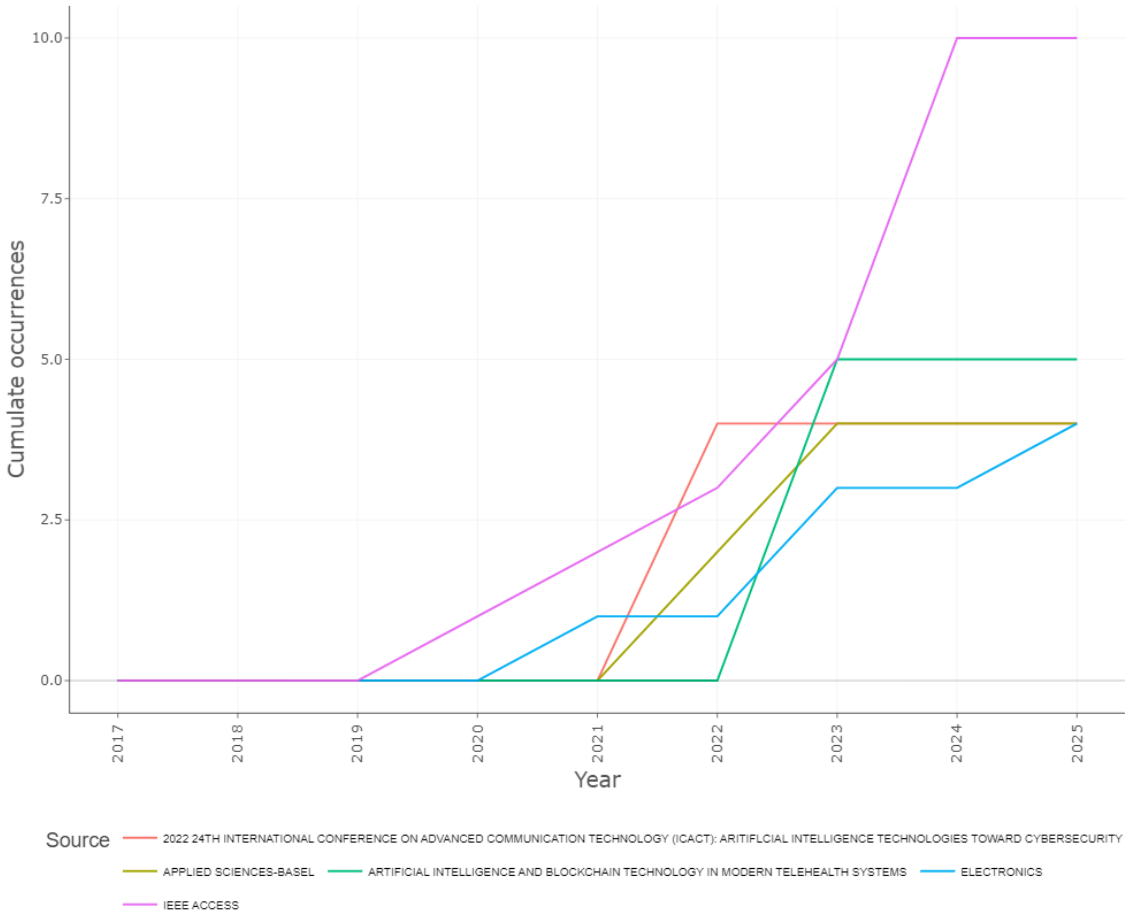


Figure 11. source Dynamics[15]

Source: RStudio Bibliometrix

2.6.4. Co-occurrence analysis utilizing author keywords

This subsection provides a co-occurrence analysis of keywords cited by writers in cybersecurity research publications over the previous decade. The co-occurrences of these keywords were examined with the fractional counting approach, with a minimum threshold of 10 occurrences per term. A total of 122 keywords were identified as meeting this requirement. The ten co-occurring terms with the best TLS values are presented in Figure X. This graphic illustrates the thirteen primary keywords cited by researchers in

[15] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

their cybersecurity and forensics research publications published in WoS. The list indicates that the keyword 'Blockchain' was present in 144 published publications (P). authentication systems, network schemes, medical technologies, technological networks, cloud security, frameworks, cybersecurity concerns, management, Healthcare, consortium blockchain, industrial applications, artificial intelligence, information system device assaults.

The term' Machine Learning' co-occurred with 458 other blockchain author-keywords in these papers. The TLS of 'security' is 2707, representing the aggregate of its co-occurrences with each of the 109 other terms, each having a minimum of 10 occurrences. In this context, if 'n' author-keywords co-occurred in an article, the strength of the link between each pair of co-occurring keywords was calculated as 1/n (attributable to the citing article). The green-hued co-occurrence network comprises author keywords including 'security,' 'internet of things,' 'scheme,' 'frame,' 'artificial intelligence,' and 'system,' among others.

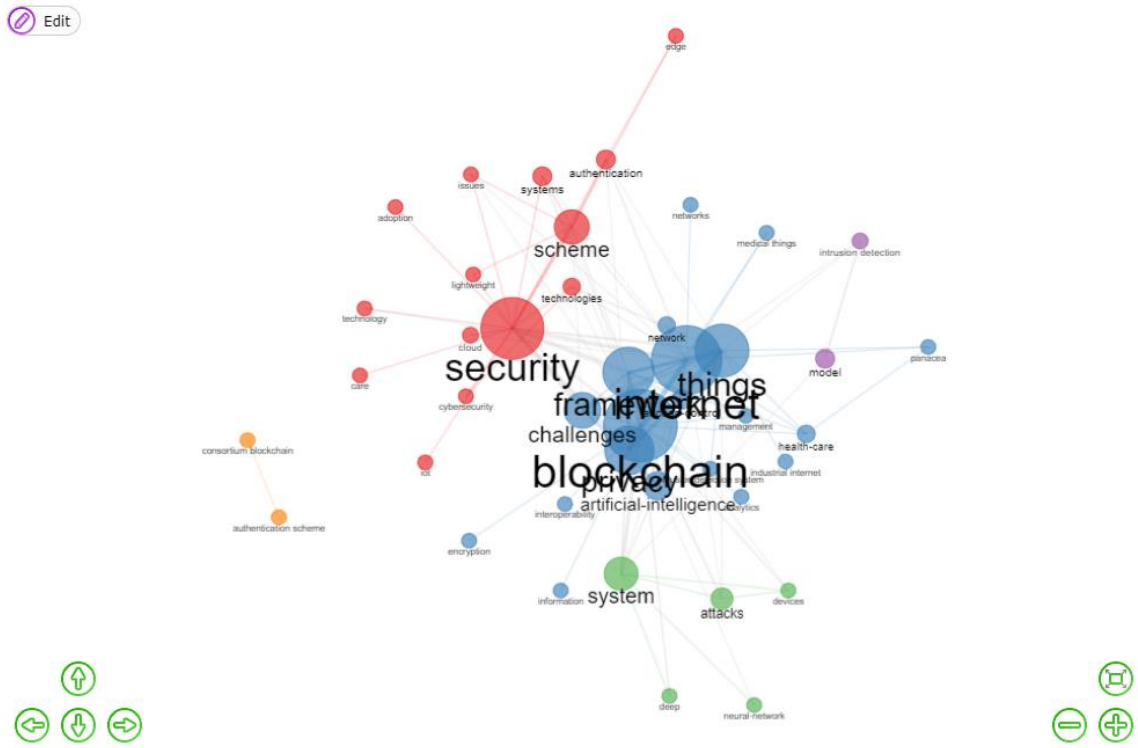


Figure 12.Co-occurrence[16]

As we can see from Figure 11, the main sources listed are IEEE, Scopus, and the Web of Science. The primary sources listed do not change if we add the AI word. Based on this research, we can display, as shown below in Figure 13, the Three with the main research in terms of citations for cybersecurity, Blockchain, and Healthcare systems.

[16] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

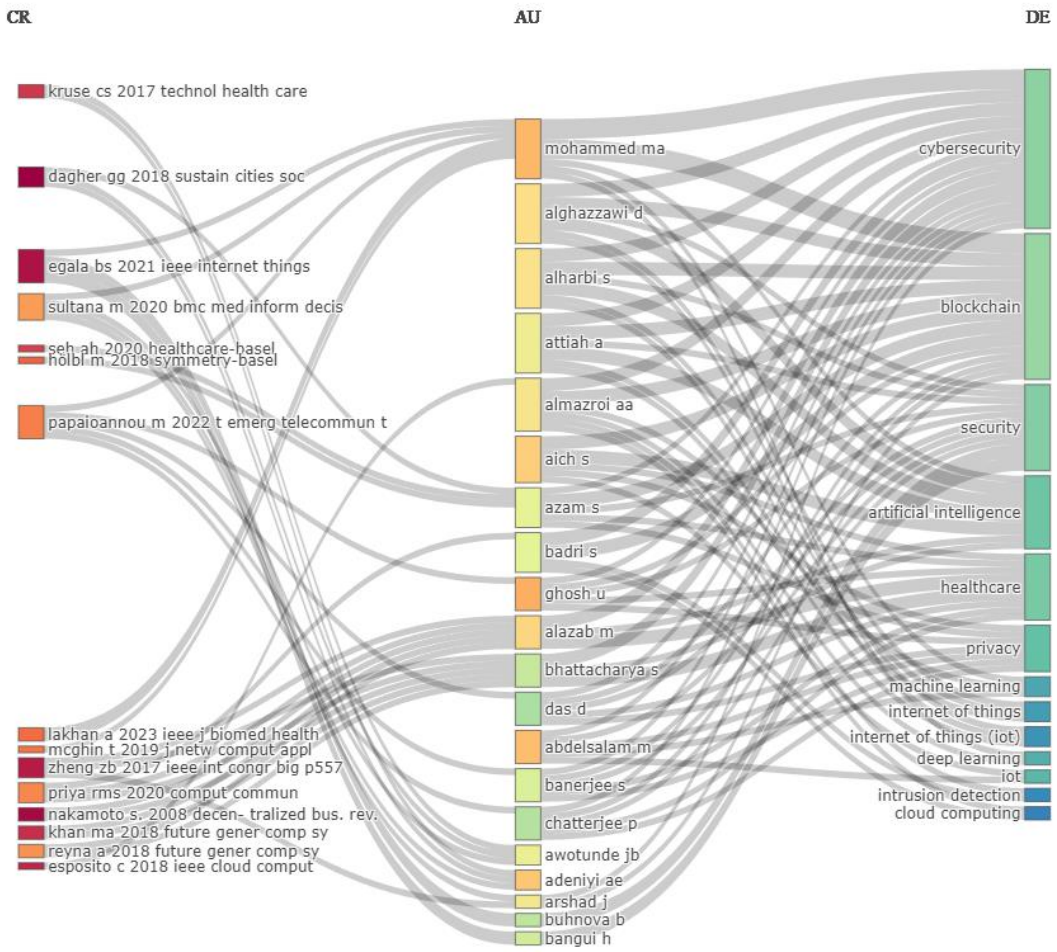


Figure 13. Displays the three-field plot from 2017 until 2025.[17]

Based on the tree-field plot in Figure, we can see that the main research was done in Cybersecurity, Permission Management, Blockchain, Smart Contracts, Service Providers, Deep Learning, the Internet of Things, Privacy, IoT, Security, Artificial Intelligence, Machine Learning, and Cryptography.

[17] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

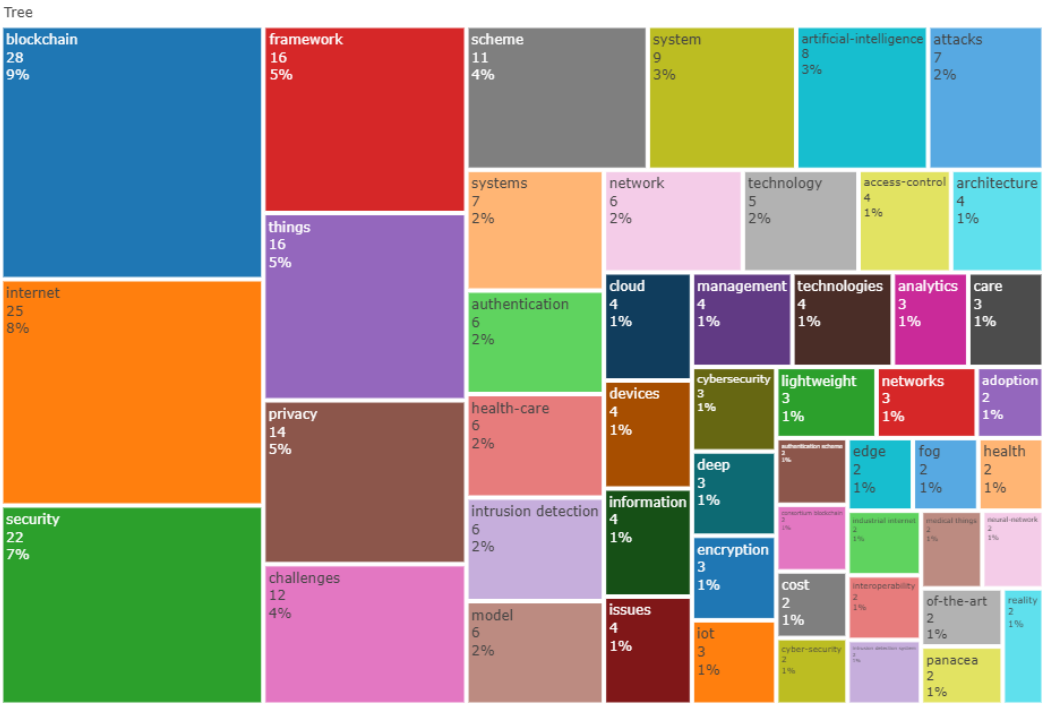


Figure 14. Displays the tree map based on the research using R Studio[18]

Additionally, the articles used the following 50 keywords frequently (at least 10 times each): "Blockchain," at 9%, "Internet" at 8%, "Security" at 7%, "Framework" at 5%, "Internet of things" at 5%, "privacy" at 5%, "challenges" at 4%, "scheme" at 4%, "system" at 3%, "Artificial Intelligence" at 3%, "attacks" at 2%, ["systems," "network," "technology," "authentication, ""healthcare," "intrusion detection", "model"] at 2%,…(for more see the Figure above).

Based on the tree map, we can see word dynamics with the frequency that it has grown from 2017-2025. From this, we can see that the word Blockchain has started to grow exponentially from 2022 until now. So, the most used words are Artificial Intelligence, security, Blockchain, challenges, internet, privacy, scheme, security, system, and things. In the Figure below, we can see their frequency of growth through the years.

[18] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

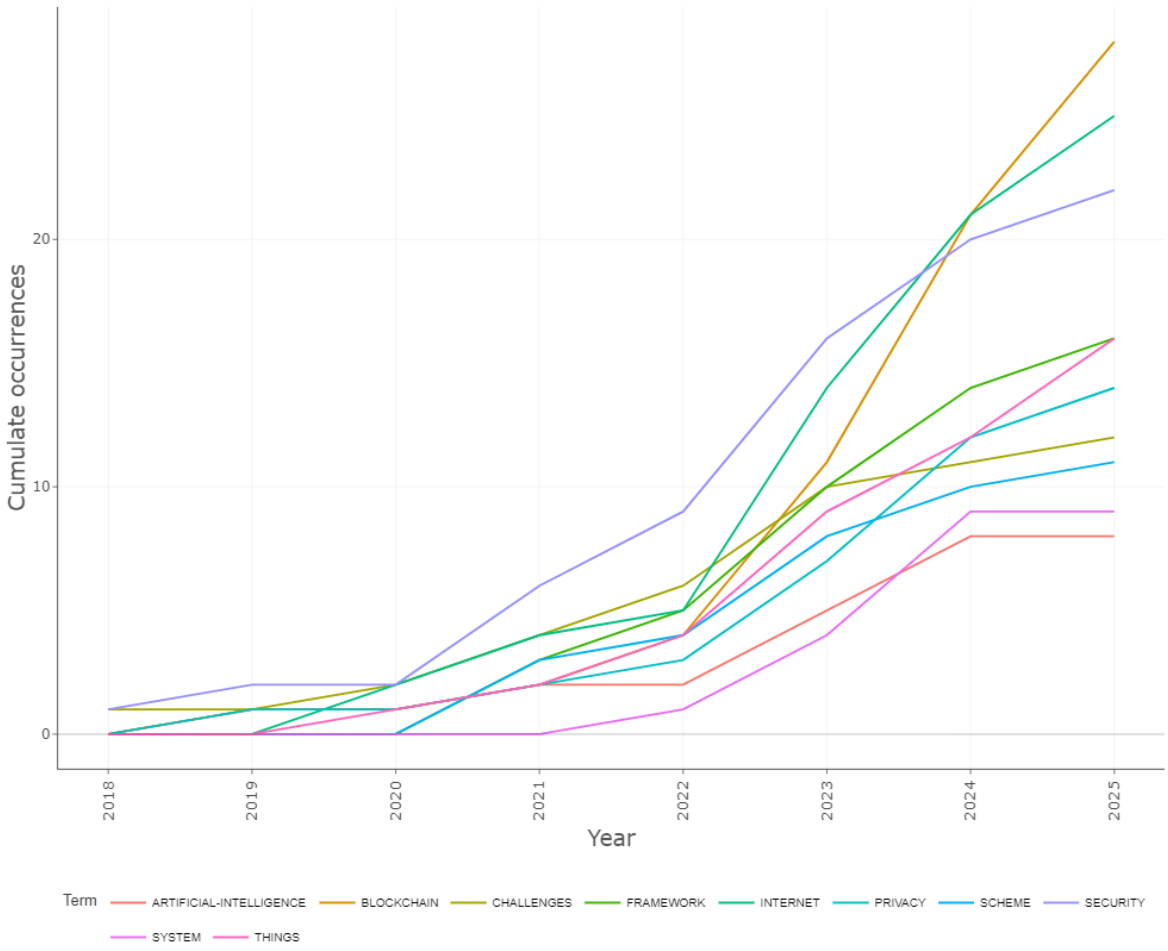


Figure 15. Occurrences[19]

2.6.5. Citation analysis based on documents.

Below, you can find the most globally cited documents, almost the same as those in the most cited countries.

[19] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

Figure 16. Most global cited sources on WoS[20]

Most cited documents, we can see, are the same as most global cited sources.

[20] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

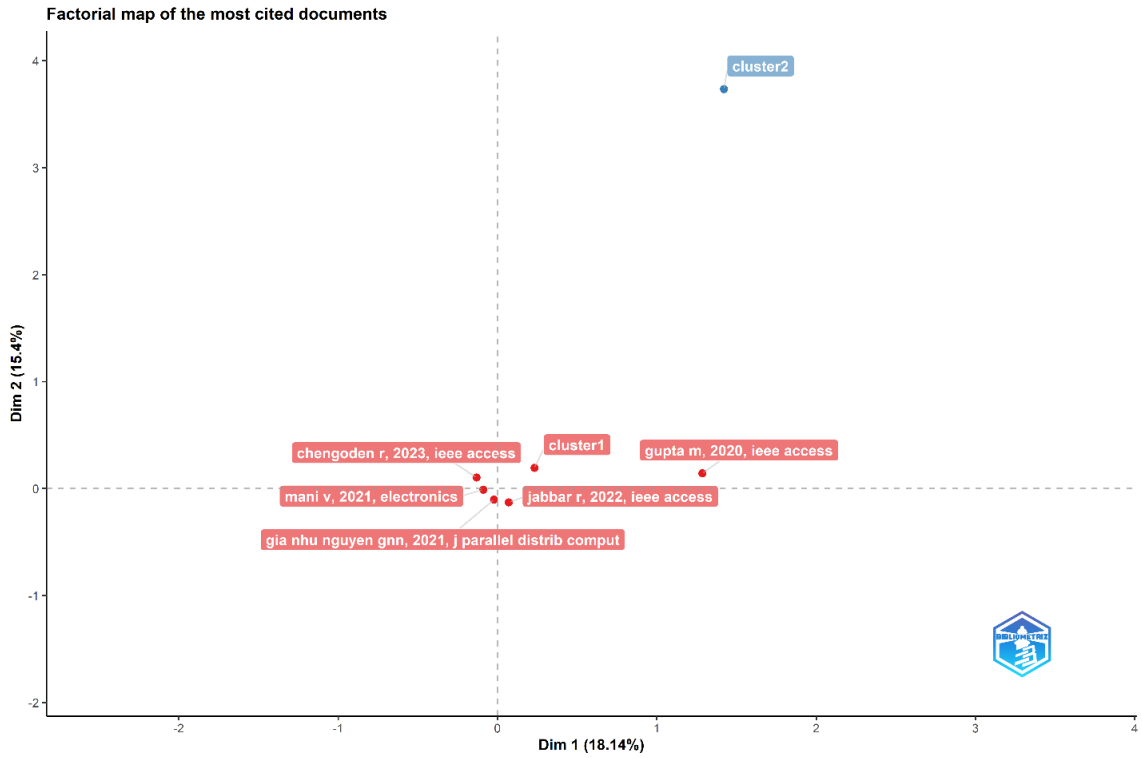


Figure 17. Most cited documents[21]

[21] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

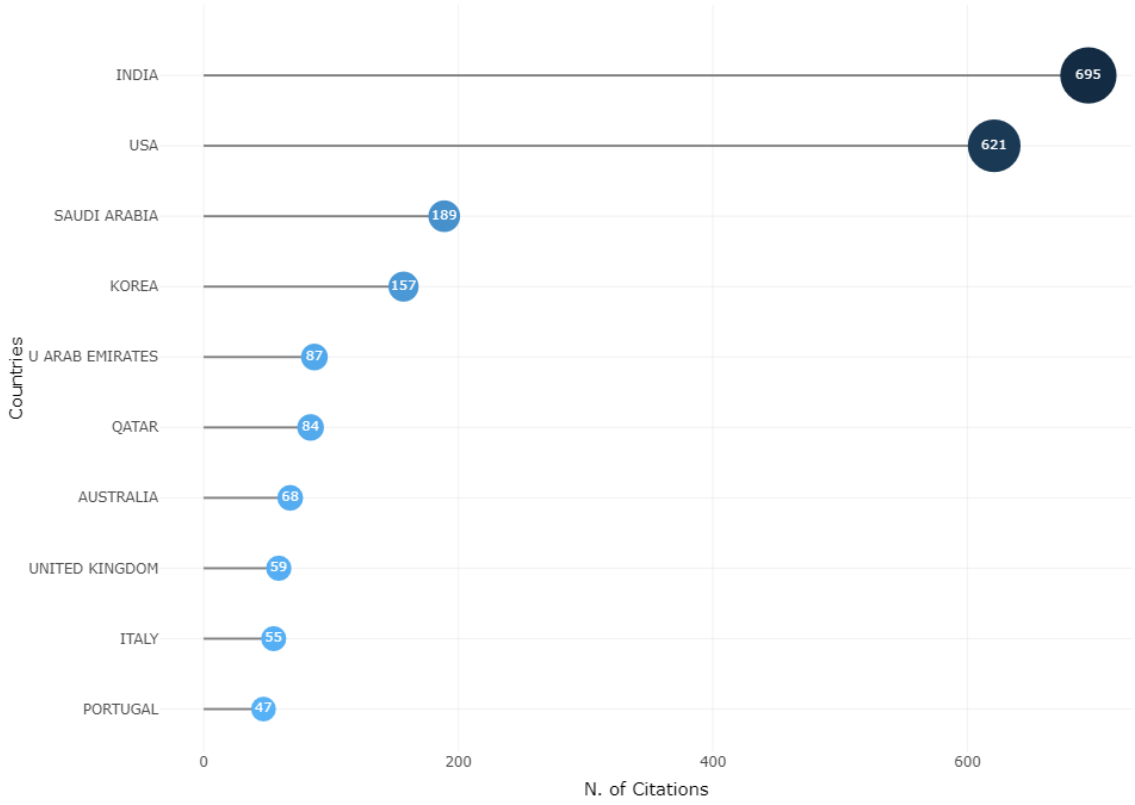


Figure 18. Most cited countries[22]

Co-citation network: Since most of the articles have co-authors, we can have a map of the citation network between the authors.

[22] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

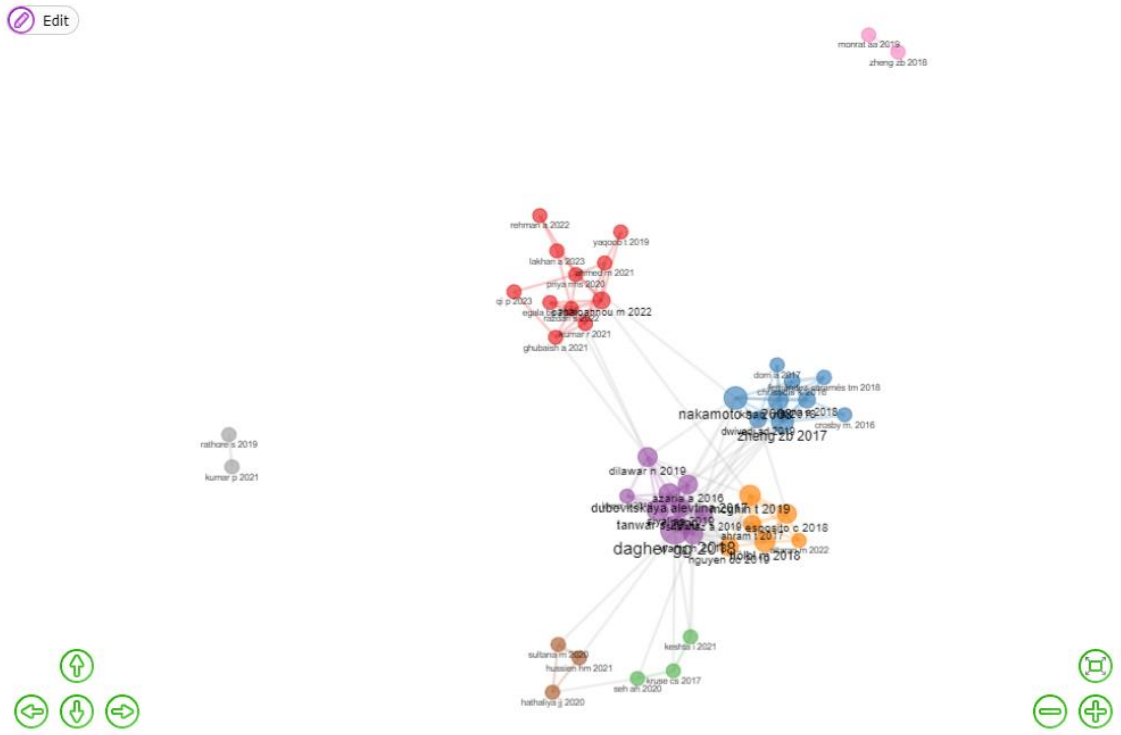


Figure 19. co-citation-network.[23]

This Figure shows the most relevant authors on whom this paper is based. By naming these authors, we can see the density of the degree of relevance of studies done until this moment. Figure 20 shows the thematic evaluation (using time slice 1) from 2017 until 2025, the same as the most cited authors.

[23] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

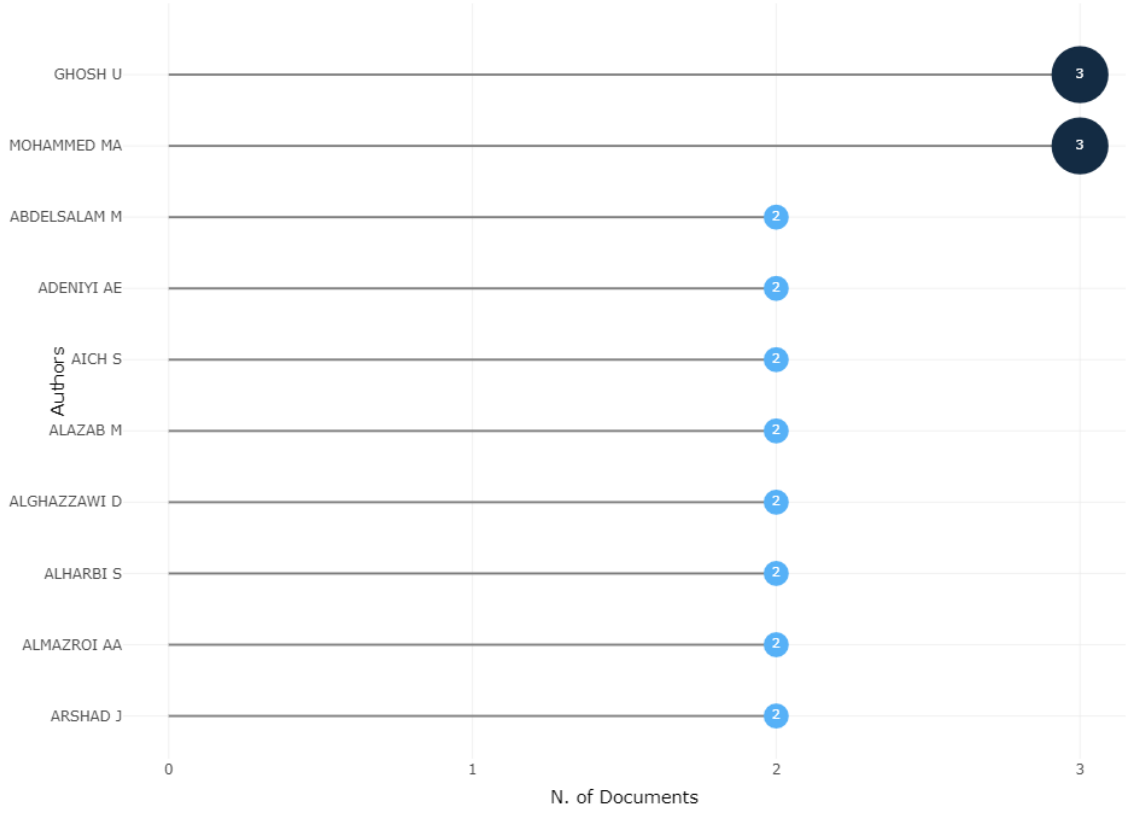


Figure 20. Most Relevant Authors.[24]

2.6.6. Best sources.

Below, you can find the most relevant sources, beginning with IEEE, then Artificial Intelligence and Blockchain Technology, International Conference on Advanced com, applied Sciences-Basel, Electronics, Internet of Things, Sensors, 2019 IEEE Southeast,

[24] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

ACM Computing Surveys, and Cluster Computing -The Journal of Networks Software.

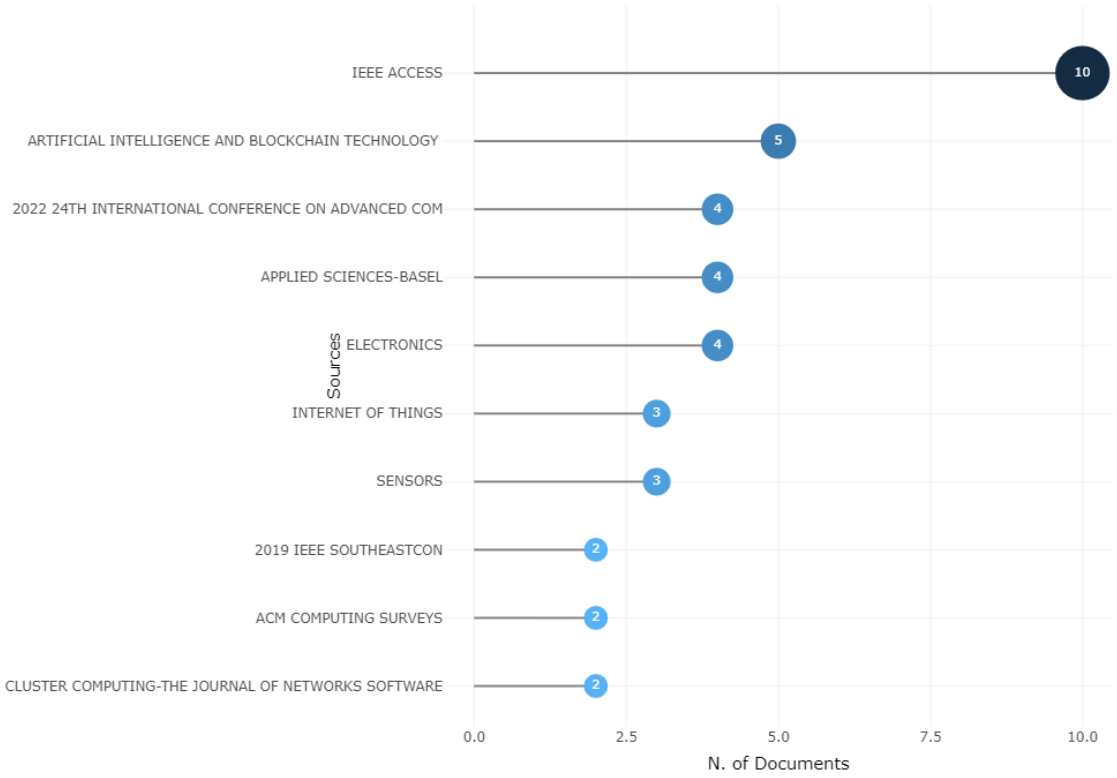


Figure 21. Most Relevant Sources.[25]

The majority of contribution documents, as we can see from the Figure 22, are from 2020 until 2024. Based on cluster 1, we can see a factorial map with the most contributed articles.

[25] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

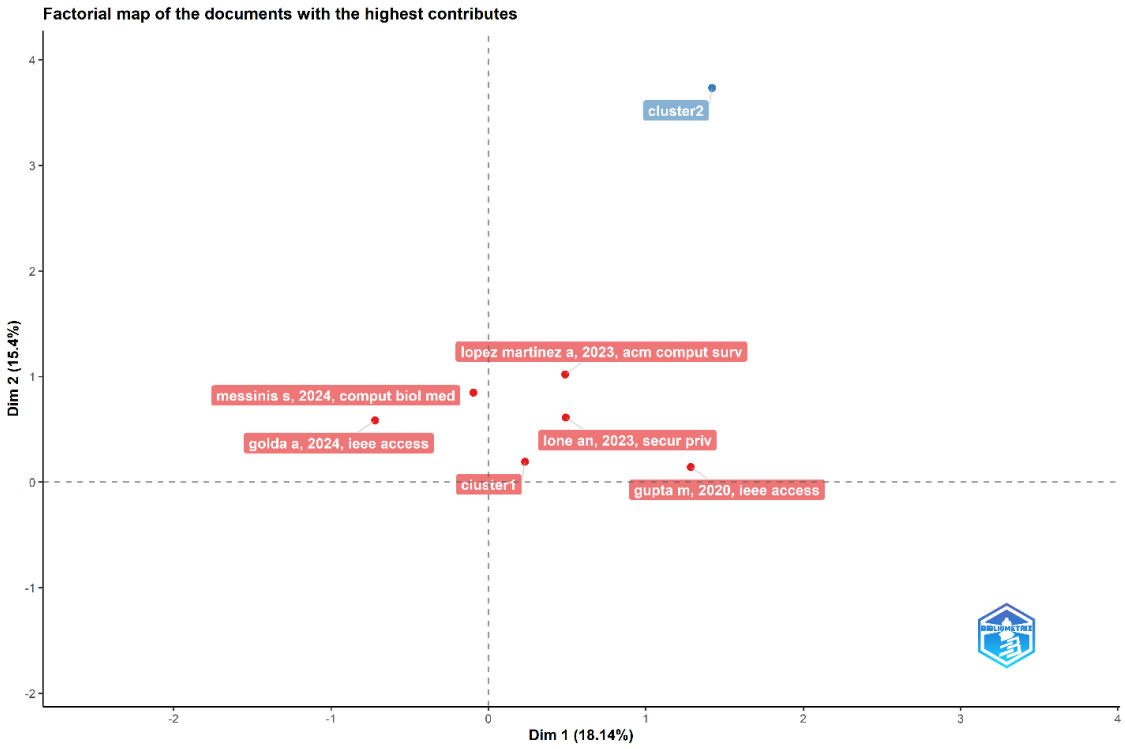


Figure 22. Most contribute documents from 2017-2025.[26]

2.6.7. Thematic evaluation from 2017-2025

The thematic evaluation figure shows the differences from 2017-2023 and 2024-2025. It makes a big difference even though it doesn't seem like it in daily life. So, as we can see, the "authentication," "issues," "network," and "scheme" from 2017 until 2023 were studied separately. From 2024-2025, they are studied by "intrusion detection". Moreover, "scheme," "encryption," and "attacks" are now in the framework capacity. Moreover, the main difference is the "security," which was one field from 2017 until 2023. Now it is part of Framework, Challenges, and Blockchain. We can see a big difference in the security field. So, we are giving it the importance that is needed.

[26] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

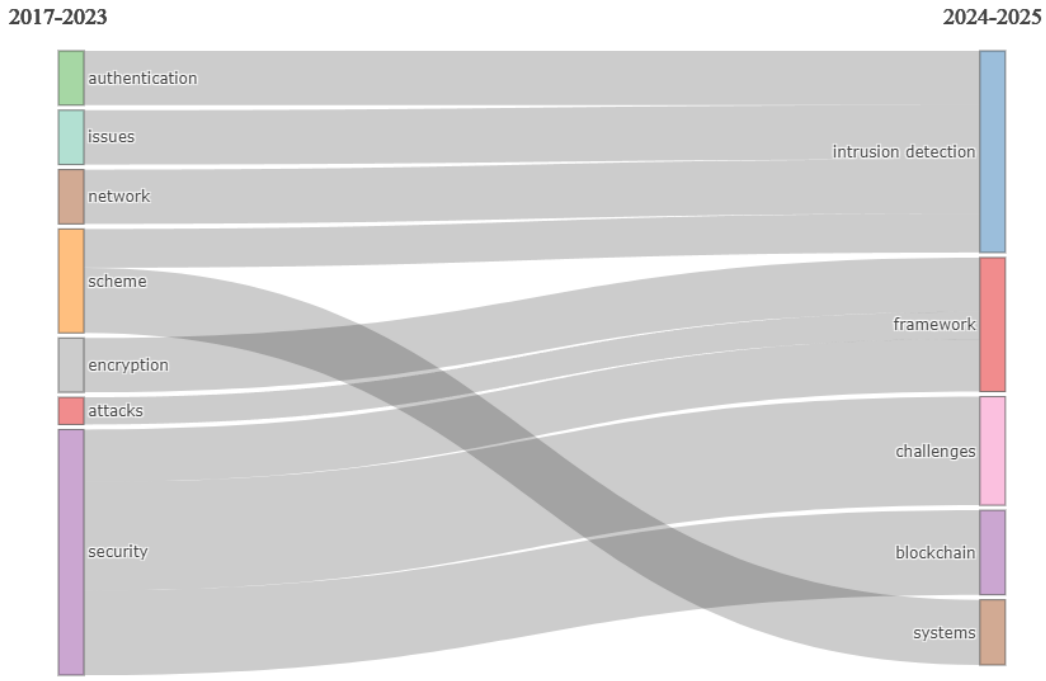


Figure 23. Thematic evaluation.[27]

2.6.8. Best topics for research.

Topics that are more popular at the moment are:

- Blockchain
- Privacy
- System
- Internet
- Security
- Framework
- Challenges

[27] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

As we can see from the figure 24, this topic has been trending since 2021. The importance of Blockchain and security has grown over the last few years.

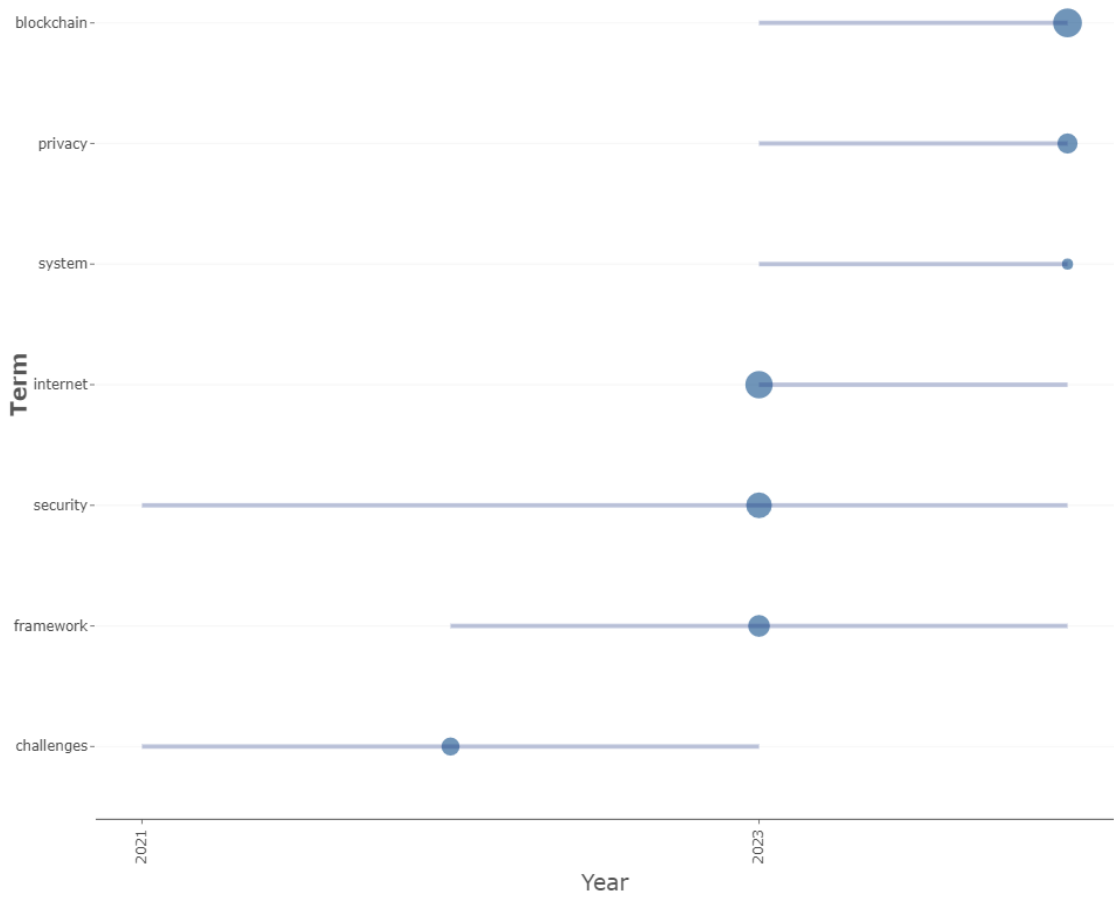


Figure 24. Trend Topics[28]

The collaboration between universities has grown over the years. Even though Blockchain security and Healthcare have been touched on in recent years, the collaboration seems to be global in terms of research. It is crucial to exchange information and experiences so we can have better quality research and reach the end faster. Below, you can find the country collaborations from 2017 until 2025.

[28] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

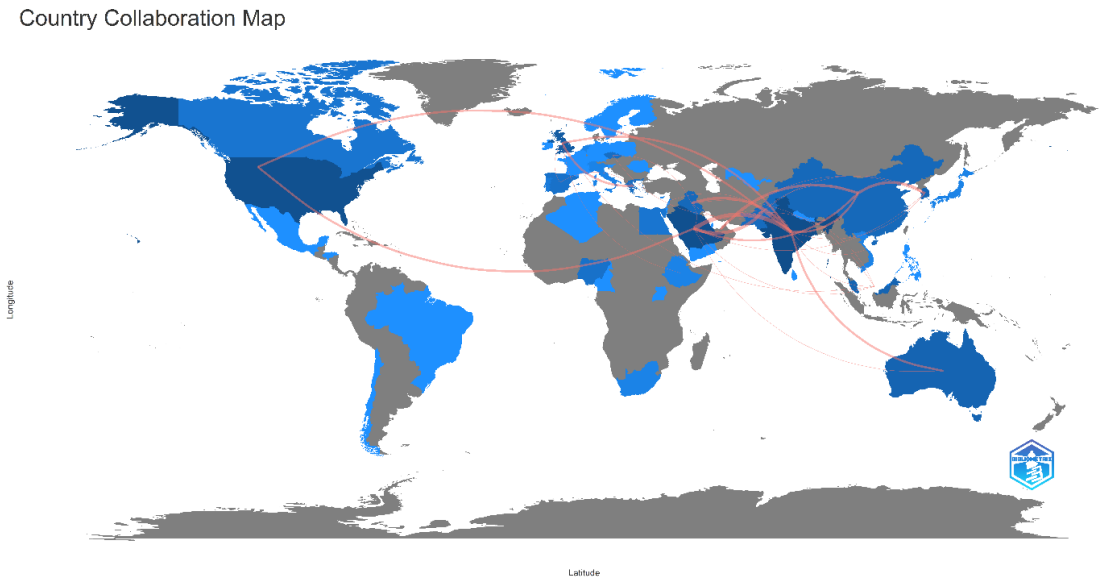


Figure 25. Country Collaboration[29]

2.6.9. Reference burst detection

Based on the Figure 26, we can see that from 1999 until 2021, there was no big change in the research on Blockchain, Security, and Healthcare. This is why the reference spectroscopy graph shows no change. However, from 2013 until 2025, we can see a big difference in the reference spectroscopy. This shows that this topic is getting the attention it deserves.

[29] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

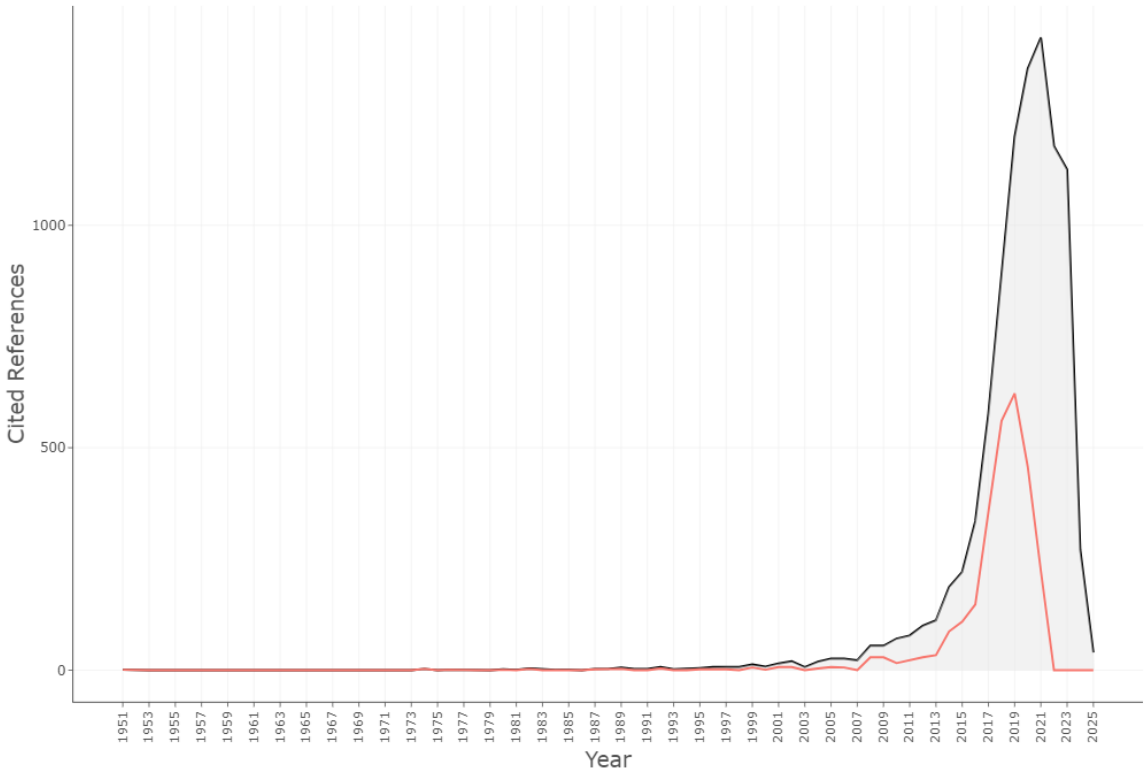


Figure 26. References Spectroscopy[30]

At the end of this literature review, this topic has much to gain and needs more research in all the countries.

Future research in cybersecurity, blockchain, and healthcare combined studies, informed by a comprehensive bibliometric analysis from the past decade, may explore advanced deep learning and transfer learning architectures to enhance anomaly and threat detection, classification, and expeditious resolution with increased precision. System condition monitoring, cybersecurity, data modeling, and security necessitate more exploration. Significant potential exists for cybersecurity, Blockchain, and Healthcare research in hardware architectures, automation control systems, and multi/interdisciplinary software applications—applied physics, military, banks, government systems, instrumentation, image science, and photographic Technology. Researchers may perform comprehensive bibliometric analyses in specific domains of cybersecurity, Blockchain, and Healthcare

[30] https://www.bibliometrix.org/home/index.php/layout/biblioshiny

research, such as malware detection and deep neural networks, to uncover underlying trends that influence current cybersecurity and Blockchain and shape the future of information and data security. The aforementioned observations and recommendations guide broader and more diverse applications in this domain, favorably influencing several disciplines and industries worldwide toward a more digitally secure future.

3. ADVANTAGES OF COMBINING HEALTHCARE WITH BLOCKCHAIN.

3.1. Main Advantages

1. **Authenticity** (The issue of explainable AI is solved by using the digital copy that blockchain technology provides to better understand the underlying structure of AI and the information sources it is using. As a result, confidence in data and AI-generated ideas increases. Security measures may be improved whenever a blockchain transmits and maintains AI models, especially when paired with AI.)

2. **Extension** (Blockchain-based business networks get a competitive advantage from AI's ability to scan, evaluate, and find that it is possible with lightning speed and depth. Blockchain allows access to vast volumes of data from both within and outside the organization, allowing for more useful insights, greater control over information use and model distribution, and a more secure and transparent data market, all of which help AI advance. Using oracles, or third parties, to process data)

3. **Automation** (Blockchains, AI, and automation may add value to cross-business processes by requiring less human involvement, increasing throughput, and promoting improved data integrity. Incorporated AI models in smart contracts that are put into place on a blockchain could, among other things, recommend recalling out-of-date products, reordering, paying for, or buying shares based on specified threshold values and events, settling issues, and selecting the most environmentally friendly shipping option)

3.2. Healthcare

AI may improve nearly every element of Healthcare, from highlighting medicinal discoveries and supporting user requests to identifying insights from trends and clinical information. Blockchain technology allows electronic medical records (EMR) and other sensitive patient data to be safely shared between healthcare providers.

Conventional EHR systems are built on a centralized design, which delegates the entire system's management, coordination, and supervision to a single entity. AI is quick enough to evaluate healthcare data rapidly and has the computational power to handle massive amounts of patient data. Some doctors are still hesitant to employ AI to influence a patient's health despite the Technology's amazing capabilities, which have demonstrated that it can complete numerous dynamic and cognitive tasks faster than a person. Information hiding, which uses technologies like encrypted multi-party computing and zero-knowledge evidence to transactions worldwide without divulging any personal information and to ensure the validity of the results, successfully protects the user's transaction privacy. However, the system becomes less successful due to the intricacy of the computations, necessitating additional effort to maximize its effectiveness in real-world settings. Understanding how to utilize AI algorithms effectively to enhance subpar performance can be challenging. Additionally, a dispersed environment requires a revision of the present AI system. However, past research has shown that model inversion assaults could be utilized to reverse-engineer Private AI, which was recently designed to integrate AI with encryption techniques to tackle the data security problem.

The main usages of the blockchain technology combined with AI in the HealthCare sector are:

- Health Data Analytics,
- Biomedical research and education,
- Remote patient monitoring,
- Health insurance claims, and

Pharmaceutical supply chain

3.2.1. The main reasons for an approach to applying Blockchain Technology are:

- data Login,
- Data Versioning,
- Non-Repudiation,
- Data Integrity, and
- Access Control.

3.3. Security

Because blockchains have built-in encryption, data is highly secure. Storing sensitive and confidential data on a blockchain, such as health records or personalized recommendations, is an excellent idea. AI requires a constant flow of enormous volumes of data. The intense research and development emphasize AI algorithms that can securely process encrypted data.

However, there is a different perspective on improving security. Although the Blockchain has high security, any additional layers or technologies are not impenetrable. Machine learning in the banking industry will hasten the adoption of blockchain technology and make it possible to anticipate potential system flaws.

It is impossible to ignore the speed with which blockchain and AI-based concepts are gaining popularity. Although both paradigms provide something fresh, there are significant differences in originality and complexity. Blockchain technology may one day automate payments and enable the safe, distributed transmission of sensitive data, Information, and transaction records due to the widespread usage of digital money in today's society. Blockchains and AI have both lately received attention. Blockchain technology uses a decentralized, secure, and reliable method to automate Bitcoin payments and provide users with access to a shared ledger of transactions, records, and data. The smart contracts of blockchain technology may not require a central authority to regulate user interactions. Contrarily, artificial intelligence (AI) endows robots with human-level capacities for reasoning and decision-making. However, fusing these two technologies might result in a significant shift in the industry. Although both technologies

are cutting-edge, they might be combined to expedite and simplify operations. This understanding prompted a thorough examination of papers that combine security, Blockchain, Healthcare, and AI, published between 2017 and 2025.

The use of blockchain technology in cybersecurity is essential. The pursuit of building huge electronic circuits raises the possibility of hacking even the most contemporary cryptography techniques. Cybersecurity in the healthcare industry is a significant and challenging topic because of the ethical and legal ramifications of a patient's medical data. Image secrecy is highly susceptible to several kinds of attacks. For this reason, special care must be taken regarding data protection when creating a cybersecurity model for healthcare applications. The blockchain algorithm maintains the security of the medical image by using a hash function.

The study sheds light on using blockchain technology to secure health services. A blockchain system's security is paramount in preventing manipulation, ensuring privacy, eliminating double-spending, and enhancing credibility. Its distributed nature and lack of reliance on trust make the security defense of the blockchain system one of the most crucial measures.

This study recommends strengthening the healthcare system by integrating blockchain technology with big data, IoT, AI, and machine learning. The aim is to stimulate further study and discussion on blockchain security and to offer more reliable security assurances for the application and advancement of blockchain technology, in response to the ever-evolving threats and challenges, which necessitate continuous upgrades and enhancements in defense technologies.

Blockchain technology upends the status quo by providing a productive and decentralized platform for data management. Blockchain is a data management system that has the potential to enable accountability and transparency. Every computer network user may have a duplicate copy of the Blockchain, a ledger of transactions where network members validate data submitted into the ledger; once entered, the data cannot be changed. Revenue cycle administration, doctor credentialing, electronic health records, and supply chain administration are applications in the healthcare industry. However, their widespread adoption is threatened by prospective government regulation and internal concerns.

Additionally, the fact that the data in the Blockchain is duplicated across all of the network's nodes fosters openness and transparency, enabling healthcare stakeholders, particularly the patients, to understand how, by whom, when, and how their data is utilized. More crucially, since the data in the ledger is duplicated throughout several nodes in the network, it has no impact on the ledger's current state. As a result, Blockchain, by its very nature, can defend against possible data loss, corruption, and security threats like ransomware assaults.

In a cross, multi-system world, blockchain technology is rapidly used to facilitate transaction security and safety, supply Chain, cryptographic protocols, and identity authentication. This facilitation occurs because blockchain technology, a digital ledger of exchanges cloned and distributed across an entire computer network, structures the recording of critical data unchanging and transparent to anyone and everyone, making it difficult, if not impossible, to change or hack without being discovered. Given these advantages, it is no surprise that Blockchain is gaining traction in various industries, including financial services, energy, Healthcare, real estate, telecoms, and others involving several entities whose accounts or activities could not be verified. The advantages of Blockchain may also be applied to another critical sector for different states: national security. Through its capacity to assure confidence in communication and information technology (ICT) and malware protection and verification, which are critical to the functioning of 5G and communication infrastructure, the technology shows potential for resolving some of today's cybersecurity challenges. More methods, use cases, and guiding principles are smoothing the route forward while new blocking hurdles emerge daily. A skills gap resulting from a scarcity of blockchain engineers has worsened the problem. Innovative solutions will be driven by high customer demand from enterprises eager to utilize blockchain technology, despite its complexities. With the continuous usage of Blockchain, ICT technology's 5G network will change. The advent of Blockchain presents the world with the opportunity for improved mutual trust beyond boundaries between untrusted external stakeholders, something the world sorely lacks. It allows providers to automate and link communities and societies worldwide.

Blockchain health information technology (HIT) has advantages, including assuring data security and privacy of health data, easing interoperability of diverse HIT systems, and

enhancing the standard of health care results. Security and privacy flaws, user reluctance, high computer power needs, implementation costs, ineffective consensus algorithms, and difficulties integrating Blockchain with existing HIT are all obstacles to adopting blockchain technology to construct HIT.

Only trust can underpin the interaction between a patient and a healthcare practitioner. Every medical record must be protected. All health information about any specific patient will always be kept private by the doctor and any other healthcare team members with the legal and professional authority to access such data. Such Information must always be kept secure to prevent access by unauthorized parties and disclosure to family members unless required by law or when the patient has expressly requested it in writing. As far as safely securing the data from unauthorized sellers, the evidence from any of the results mentioned above indicates

Blockchain technology still needs to do so. This theoretical assumption is that medical records should always be preserved in a secure location without fail. The theocentric system must be used when entering patient data following the generally accepted medical record-keeping standard. Anyone accessing the data must log in and enter a password. This element is irrelevant because each data set in Blockchain is presented in blocks and may be viewed separately.

Additionally, it is crucial to back up all data to a portable storage device, allowing for data recovery in the event of system failure. When a dental professional divulges private Information about a patient to a third party without the patient's consent or a court order, it is always a violation of confidentiality. Equally, while being a popular technology used in many nations worldwide, Blockchain needs appropriate Standardization. Blockchain has been shown to lack appropriate security standards, particularly inside networks and worlds. When appropriate security control systems are in place, such attempts may be thwarted even though those not concerned with the patient's data may deliberately try to access Information on the patient's identity or location by intercepting communication between the patient and the healthcare providers. Many breaches may be avoided by implementing a top-notch security strategy focusing on the blockchain system's most straightforward and frequent causes of data breaches.

Table 2. Types of Blockchain[31]

	Type One Only Cryptocurrency C2C	**Type Two Cryptocurrency+ Business B2C**	**Type Three Only Business B2B**
Mode of Peer-to-Peer	Public Blockchain with no permissions	Public Blockchain	Authorized Blockchain
Consensus Mechanism	Proof-of-Work (PoW)	Public or Private Blockchain	Private blockchains
Scalability	Low-Performance Scalability and High Node Scalability	Proof-of-Work (PoW) Low-Performance e Scalability and High Node Scalability	Pluggable Consensus Algorithm, which is PBFT at the moment
Cryptocurrency	Integrated	Integrated	Low Scalability of

[31] S. Qose, Z. Rajnai and B. Fregan, "Blockchain Technology in Healthcare Industry: Benefits and Issues," *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania, 2023, pp. 171-176, doi: 10.1109/SACI58269.2023.10158669.
keywords: {Industries;Law;Supply chains;Medical services;Writing;Regulation;Blockchains;4.0 Technology;Healthcare system;Blockchain Security;Smart Contracts;Cybersecurity},
https://ieeexplore.ieee.org/document/10158669

	cryptocurrency y is known as (Bitcoin)	cryptocurren cy ncy as (Ether)	Nodes Scalability for high performance No cryptocurrency integrated
Programming Language	C++ has extremely few programming options and makes developing applications challenging.	Solidity- written smart contracts with significant developme nt potential (Dapp)	Golang chain code with a lot of development potential

Public, private, and consortium Blockchains are the three forms of Blockchain. Every node can access the Blockchain-based system and engage in Blockchain activities in a shared Ledger, such as Bitcoin. A private Blockchain is a limited Blockchain that functions within a private network within an entity, with just a few people participating in the Blockchain network. When Scalability, accordance with data protection standards, and other regulatory difficulties are necessary, private Blockchains are utilized, upwards of one organization, to manage the Consortium Blockchain. Banks and network providers are the most common users of consortium blockchains. The following are the significant components and properties of Blockchain:

1. A smart contract is a programmable binary code stored on the Blockchain and activated when specific circumstances are satisfied.
2. Consensus—In a peer-to-peer network, the agreement includes an agreement among many active nodes to authorize a transaction.
3. There is no dependence on a third party to ensure the Information's legitimacy and security. Using a consensus process, the Decentralized network of interconnected nodes defends the network and creates confidence.
4. Shared database or ledger — A shared database or ledger is an incremental backup database that records all transactions and is accessible to all participants.

5. Transparency - All participating nodes know all operations and can authenticate each one effectively.
6. Provenance- All internet backbone interactions may be monitored and verified to see how data ownership has shifted.
7. Immutability—All data collected on the Blockchain is tamper-proof. Transforming the data recorded on Blockchain necessitates ownership of most nodes inside the Blockchain network (51 percent assault).

The new generation of mobile Technology, 5G, connects everything and everyone, providing new opportunities for customers, society, and industries[29]. However, the trust related to the reliability and security of 5G equipment and systems has been the main topic of several discussions. Blockchain-based models can facilitate the exchange of automotive and traffic data. Our work identifies and debates significant open research problems that the research community should address and provide answers to fully harness the considerable benefits of upcoming 5G networks and services. We conclude that Blockchain can transfer Information between participants in a safe, dependable, and controlled manner that is constantly monitored and evaluated with the help of specialized tools.

3.4. Blockchain for better seciurity

3.4.1. Distributed Storage

Ethereum is a blockchain-based platform that makes the Blockchain programmable. Blockchain is a costly storage medium, particularly when handling vast amounts of data. As a result, the Interplanetary Storage Device (IPFS), Swarms, Filecoin, BigChainDB, and Storj are launched as distributed peer-to-peer storage systems[30]. As a result, the advantages of Blockchain became evident, leading to the creation of Digital Assets.

3.4.2. Decentralized Apps (DApps) and Smart Contracts

DApps[31], decentralized applications, are frontline user applications that interact with payment systems by triggering transactions that call innovative contract functionalities. A smart contract is software that manages the interactions and agreed-upon terms and conditions among participants. All decentralized and trustworthy nodes verify and agree on the conclusion of the smart contract's execution.

3.4.3. Blockchain Platform Types

There are three types of blockchain platforms: permission-less, which means the blockchain network is open to the public; private Blockchain, which means the blockchain network is secure and personal references award connectivity; and network management is typically completed by a known superintendent, and partnership agreement, which is a hybrid of permission-less and validates transactions. The blockchain administration is carried out by several administrators and not in cooperative, federated, or hybrid blockchains, which are analogous to permissioned networks.

Future 5G mobile carriers are expected to gain more from employing a collaboration or permissioned Blockchain. Because consumer and supplier data are made publicly available, a public blockchain may threaten privacy. A public or private blockchain would be preferable if the operator intends to utilize the Blockchain for internal purposes. A blockchain network would be more suited when providers offer telecommunications services to vertical businesses, such as roaming cost settlements involving several corporate relationships.

3.4.4. Verified Oracles

Smart contracts are unable to obtain external data on their own. Oracles or source streams should call particular functions within smart contracts to relay outside data and Information to the smart contracts. It is impossible to trust a singular oracle to publish data. As a result, numerous oracles are required to report inputs to smart contracts. Smart contracts must examine and review reported data from multiple oracles to ensure that the data is reliable. The oracles employ decentralized sharing, consensus, and reputation processes to establish high confidence in the available results.

In this work, we have introduced two significant approaches: NESAS and Blockchain integration[32]. NESAS is focused on the technical aspects of product development, which rely on the legal and policy aspects defined by processes.

The implementation of Blockchain-based models may be used as a rapid and permanent record for settling vehicle insurance claims. The need for a massive network of IoT

systems to interact with each other through millisecond latency in situations including green infrastructure and UAV [33] fleets may be met by blockchain-enabled administration and verification of such equipment. Thus, we outlined blockchain technology and the decentralization elements that make it possible, such as consensus mechanisms, distributed storage, and decentralized applications. In addition, future and innovative opportunities and use cases that result from combining Blockchain with 5G networks (not previously explored in the literature) are highlighted.

Blockchain in the cloud data center eliminates the need for a scheduler, resulting in lower energy costs and excellent reliability. Handling a sequence of requests uploaded to the Blockchain as a transaction and confirmed by consensus by participating data centers reduces the energy cost. Thanks to the Blockchain, the data center can plan requests for resource allocation without relying on a centralized scheduler. A smart contract is run every time a transaction is received, and the request and V.M.s are migrated. The data center with the least traffic accepts requests, and virtual machines present a Blockchain-enabled federated cloud infrastructure to close the breach detection gap (BDG).

This research has shown how Blockchain, including accompanying decentralized technologies, may be used for 5G by providing technical specifics inside system implementation architecture and diagrams. Nonetheless, as in every system, Blockchain naturally faces some challenges in social media. The present study revealed that there are still problems related to guidelines and regulations in many countries: delayed frameworks, key protection, self-centered excavators, information control, cloud stockpiling, limit obliges, fork problems, smart contracts, and property.

More research is needed to enhance and expand the opportunities offered by this Technology. Blockchain has potential for social media and several research topics such as economics and business, social interaction, and national and international security. Therefore, future research should concentrate on the opportunities in specific areas and investigate the present and possible issues. Further enhancement is still needed in the security area.

Table 3. Advantages of blockchain applications in healthcare[32]

Enhanced privacy and data security	Every health information on the Blockchain is timestamped, encrypted, and added in Chronological sequence. The The identity or privacy of the patients is further protected by using cryptographic keys to store health Data on the Blockchain.
Ownership of health data	Patients must be the owners of their data and in charge of how it is Utilized. Patients should be able to notice instances of Data misuse requires the assurance that third parties will not misuse their health Information.
Decentralization	A decentralized management The Structure is necessary for Healthcare. because of the spread of Stakeholders. Blockchain has the potential to become the
	integrated healthcare delivery data Management.

[32] https://ieeexplore.ieee.org/document/10158669

Trust and Transparency	Blockchain fosters confidence in distributed healthcare apps because of its openness and Transparency.
Authenticity of data	The legitimacy and integrity of the Records kept on Blockchain may be confirmed even without access to Their plaintext.
Accessibility and robustness	The availability of health data saved on Blockchain is ensured Since records are duplicated across numerous nodes, making the system resistant to data loss, data corruption, and various security Attacks on accessibility.

3.5. Innovation and Design.

Between early 2018 and 2025, we identified over 933,224 research studies relevant to Blockchain, cybersecurity, or healthcare. We subsequently selected only primary research that conformed to the quality assessment criteria. We researched using the following terms: Blockchain, Cybersecurity, and Healthcare. Based on these criteria, we obtained 144 results from the Web of Science. We may incorporate other studies into analyses in future research; nevertheless, this is sufficient for progressing to the subsequent investigation quickly after the initial assessment. We meticulously assessed the data contained within the subset of the study and publications. We presented the data to convey the study, insights, and reflections on the supply chain and security domain. Ultimately, we outline the current terms and strategies for implementing Blockchain to enhance the security of existing and emerging cyber technologies.

We conducted a literature study by examining 20 publications or studies relevant to the topic we have presented for this occasion. We can thoroughly analyze the research on a single issue.

3.6. Primary Studies

Applying keywords to the search functionalities of specific publications or search engines yielded all relevant studies and the principal research articles. All selected keywords were intended to promote the dissemination of the research findings to meet the research questions. The primary keywords included cybersecurity in Blockchain, blockchain technology, security problems, security challenges within the chain, data privacy, and blockchain assessment. The platforms consisted of:

1) Web Of Science
2) IEEE Explore Digital Library
3) Research Gate
4) ScienceDirect
5) Google Scholar

Based on the keywords, we have extracted seven papers, which you can find in the table below.

Table 4. Keywords and Research Papers keywords Papers Research

keywords	**Papers** *Research*
Cyber security in Blockchain	A systematic literature review of Blockchain cyber security [17] How the development of Blockchain affected cybersecurity [18] Bitcoin and Blockchain Security [19] BSS: Blockchain Security over software-defined. [20]
Blockchain performance	Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications [21]

keywords	Papers *Research*
Data Privacy in Blockchain	Cybersecurity, Data Privacy, and Blockchain: A Review [22] AI-empowered, Blockchain and SDN integrated security architecture for IoT network of cyber-physical systems [23]
Blockchain technology security concerns	Four ways Blockchain Technology will Disrupt Telecommunications [24] Cybersecurity Risks of Blockchain Technologies [25]
Blockchain in Healthcare Technology	Distributed Ledgers: Definition, How They're Used, and Potential [6] A survey on blockchain technology and its security," Blockchain: Research and Applications [7]

This study analyzed many publications and studies concerning the objectives and two research inquiries. A process was employed to choose the foremost research conducted in recent years. Rapidly review the entire report to identify the substantial implications of their research and select the primary elements for conducting this study. Subsequently, all duplicates will be eliminated to pick the primary studies conducted; thereafter, the chosen abstracts will be reviewed to ensure their alignment with the research issues pertinent to the objectives of this work.

According to the study, we have determined that further research is necessary on Data Storage and Sharing, as it is the primary area with the most issues. Furthermore, the Internet of Things (IoT), a highly researched and now popular domain, should focus more on addressing the challenges it faces, particularly in smart homes, and devising innovative methods to safeguard data within Blockchain technology.

This report offers further proof of Blockchain Security research. It has improved comprehension of the principal domains that warrant further investigation.

Blockchain technology disrupts the existing paradigm by offering an efficient and decentralized framework for data management. Blockchain is a data management technology capable of facilitating accountability and transparency. Each computer network user may possess a duplicate of the Blockchain, a transaction log wherein network participants authenticate the data entered; once recorded, the data is immutable (OECD, 2020). Revenue cycle management, physician credentialing, electronic health records, and supply chain management are applications within the healthcare sector. Nevertheless, their extensive implementation is jeopardized by potential government regulation and internal apprehensions (OECD, 2022)[34].

The duplication of data across all nodes in the Blockchain promotes transparency, allowing healthcare stakeholders, especially patients, to comprehend how, by whom, when, and in what manner their data is employed. More importantly, the duplication of data among multiple nodes in the network does not affect the present status of the ledger. Consequently, Blockchain protects against data loss, corruption, and security risks like ransomware attacks. Transparent and immutable record-keeping is essential in the healthcare sector for specific transactions, including procuring and distributing pharmaceuticals and medical equipment and overseeing personnel access to facilities, patient records, and other health-related data. The necessity of blockchain technology for preserving the integrity of these transactions poses an issue for policymakers. Do its costs and benefits surpass rival technologies, such as a traditional, centrally managed database?

Blockchain health information technology (HIT) offers benefits such as ensuring data security and privacy of health information, facilitating interoperability among various HIT systems, and improving the quality of healthcare outcomes. Obstacles to implementing blockchain technology for constructing Health Information Technology (HIT) include security and privacy vulnerabilities, user apprehension, substantial computational power requirements, implementation expenses, inadequate consensus algorithms, and challenges integrating Blockchain with current HIT systems.

Trust is the fundamental basis for connecting a patient and a healthcare practitioner. All medical records must be safeguarded. All health information on any specific patient will consistently be kept confidential by the physician and other healthcare professionals

possessing the legal and professional capacity to access such data. Such Information must be safeguarded to prevent unlawful access and disclosure to family members, except when mandated by law or when the patient has explicitly requested it in writing. The Information from the aforementioned outcomes suggests that blockchain technology still needs improvement in securely safeguarding data from unauthorized vendors. This theoretical premise posits that medical records must invariably be maintained in a secure location. Theocentric methodology should be employed when inputting patient data by established medical record-keeping standards. Access to the data requires users to log in and provide a password. The presentation of each data set in Blockchain as distinct blocks renders this element meaningless.

Furthermore, it is imperative to back up all data to a portable storage device to facilitate recovery during system failure. A dental professional's disclosure of a patient's private Information to a third party without the patient's consent or a court order constitutes a breach of confidentiality. Similarly, despite widespread adoption across numerous countries, Blockchain requires proper Standardization. Blockchain has demonstrated insufficient security standards, especially inside networks and ecosystems. When suitable security control systems are implemented, such attempts may be obstructed, despite individuals unrelated to the patient's data intentionally seeking Information regarding the patient's identity or location by intercepting communications between the patient and healthcare providers. Numerous breaches can be averted by employing a superior security strategy that targets the blockchain system's most fundamental and prevalent sources of data breaches.

3.7. The expected result and applications:

The rapid ascent of Blockchain and AI concepts is undeniable. While both theories offer novel contributions, they exhibit substantial disparities in originality and complexity. Blockchain technology has the potential to automate payments and facilitate the secure, decentralized transmission of sensitive data, Information, and transaction records, owing to the prevalent use of digital currency in contemporary culture. Both blockchains and artificial intelligence have recently garnered attention. Blockchain technology employs a decentralized, secure, dependable mechanism to automate Bitcoin transactions and grant

users access to a communal ledger of transactions, records, and data. Blockchain technology's smart contracts may operate without a central authority to govern user interactions. Conversely, artificial intelligence (AI) equips machines with human-like abilities in reasoning and decision-making. Nevertheless, integrating these two technologies could lead to a substantial transformation in the sector. Despite both systems being state-of-the-art, their integration could streamline and accelerate processes.

The expansion of the Bitcoin system has led to the rising popularity and advancement of blockchain technology in recent years. Blockchain technology generates several interconnected data blocks through cryptographic processes. Crucial data encircles each Block to validate its authenticity and facilitate the subsequent generation of blocks.

Consequently, Blockchain operates as a distributed database, acquiring essential attributes such as immutability, privacy preservation, and decentralization that facilitate secure data sharing. Furthermore, it enhances openness and data integrity inside the information system, which accounts for its utilization in numerous key applications, including supply chains, industries, gaming systems, identity management, and food monitoring.

Furthermore, the electrical sector, the Internet of Vehicles, and the healthcare industry extensively utilize the advancements of blockchain technology. Implementing blockchains in the healthcare sector engenders a significant transformation. Patient data is typically straightforward to manage; however, handling unstructured data can sometimes require additional effort.

This medical data is compiled from several users and is accessed or modified by multiple individuals for significant objectives. Patient data must be managed safely, reliably, and safeguarded due to its critical importance. Consequently, when the blockchain system accommodates numerous users generating vast quantities of data, such as from the Internet of Things (IoT), it encounters particular challenges, as a substantial user base can impede the system's processing speed, leading to complications with blockchain scalability and authentication. The cybersecurity system employs various techniques, including the Elliptic Curve Integrated Encryption Scheme (ECIES), Convolutional Neural Network (CNN), Fuzzy Computing, Ring verification methodology, and deep

belief network combined with ResNet. Consequently, African Buffalo Optimization (ABO) [35], Whale Optimization[36], Ant Lion Optimization (ALO) [37], Improved Particle Swarm Optimization (IPSO) [38], Genetic Algorithm (GA) [39], and various other instances of meta-heuristic optimization have gained prominence in the enhancement of cybersecurity recently. Conventional healthcare systems' security and privacy safeguards are insufficient and susceptible to hostile assaults.

Moreover, traditional methods have been associated with a substantial rise in computational complexity and latency. This study introduces an innovative security enhancement method utilizing Blockchain for data sharing in Healthcare to mitigate cybersecurity issues.

Every medical institution employs distinct data storage technologies and protocols, each governed by stringent policies regulating the exchange and transfer of patient Information. The existing data collection process fails to ensure the integrity and reliability of patients' medical records.

Classical healthcare systems face numerous issues, including patient data storage and secure transmission across healthcare information networks. All players and stakeholders can swiftly and securely integrate healthcare data with a distributed blockchain platform. A significant challenge for the medical community is protecting patient data while ensuring its accessibility when required. This issue can be rectified, as data may be shared securely and unchanged due to blockchain technology's distributed and immutable nature.

Incorporating blockchain technology into healthcare systems may address the previously listed difficulties through diverse encryption methods, consensus mechanisms, and peer-to-peer networks.

Blockchain is a distributed, decentralized, peer-to-peer database network that allows numerous parties, including untrustworthy ones, to execute transactions without external interference while ensuring data integrity. It is a distributed ledger that executes transactions and generates verifiable informative entries that are permanently retained. Three essential concepts—peer-to-peer networks, public key cryptography, and distributed consensus—constitute blockchain technology's and its transactions' core.

The transaction data is encapsulated within the Block, which serves as a record and comprises the following Information.

- *The Block's alphanumeric identifier is hashed for recognition.*
- *The hash of the preceding Block of the current Block.*

3.8. Temporal resource

A solitary random integer is employed to modify the hash value.

In a blockchain network, a Merkle root represents the hash of all transactions constituting a block.

Transaction data include details on numerous transactions.

One of the fundamental aspects of Blockchain is its peer-to-peer network structure, allowing anyone to join without altering the data. Time mining is employed to illustrate the existence of records inside a designated time window and may also assist in identifying any unlawful alterations. Data is immutable because it cannot be altered once recorded on a blockchain.

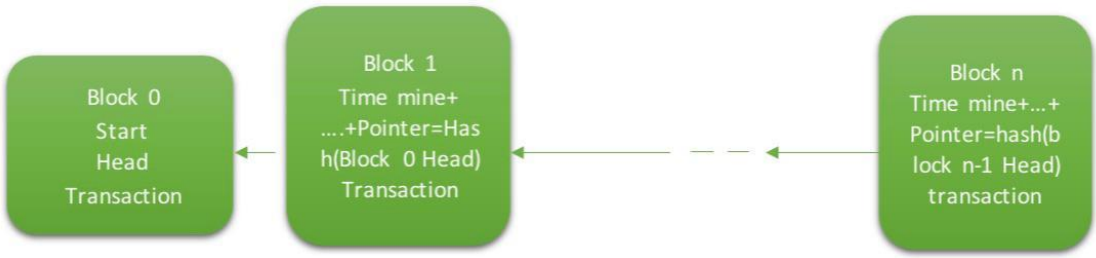


Figure 27. Blocs of Blockchain[33]

[33] https://epa.oszk.hu/04100/04186/00018/pdf/EPA04186_biztud_szemle_2022_ksz_099-108.pdf

The decentralized nature of blockchain technology prevents network failures. The complexity of establishing a revocation procedure, coupled with the public nature of Blockchain, imposes costs on other users, rendering transactions irreversible by the sender and, given the attributes of blockchain technology, safeguarding patient medical Information and ensuring its secure transfer when necessary is imperative.

What is hash rate, and why is it crucial to comprehend it to evaluate the security of the Blockchain?

The hash rate quantifies the computational capacity of a proof-of-work (PoW) cryptocurrency network[40]. The mining power of a blockchain network is utilized to evaluate its health, security, and mining difficulty.

A hash is a randomly generated alphanumeric code, and attempting to deduce it is referred to as hashing (or anything akin to it). The total number of guesses executed by computers on the network is recorded, and the hash rate signifies the number of guesses generated per second throughout the entire network.

3.8.1. Principal lesson

The hash rate measures the computational power within a blockchain network.

What is the frequency of assumptions making each second that influence the hash rate?

The average hash rate can be utilized to determine a blockchain network's security and mining difficulty.

Hash rates may vary, with the most prevalent blockchains experiencing an annual rise.

The frequency at which each computer attempts to solve the hash on a blockchain network is utilized to quantify hash rates. This is an essential phase in the proof-of-work (PoW) network's cryptocurrency mining procedure.

3.8.2. Operational Mechanism:

A blockchain network employs a hashing algorithm that randomly generates hash codes.

In the blockchain network, mining computers vie to ascertain the hash value.

The hash rate on the blockchain network quantifies the number of attempts made each second. When a miner forecasts a number that is less than or equal to the numerical value of the target hash, the hash is deemed "solved." The successful miner can append the subsequent Block to the Blockchain and get Bitcoin benefits, also known as "block rewards."

A blockchain network's hash rate escalates with the number of machines that connect and compute hashes (guesses) within the network. A PoW blockchain network with a substantial hash rate is more secure and robust because the probability of an attack is diminished.

3.8.3. What is the method for measuring hash rate?

The hash rate refers to the quantity of hashes (or guesses) executed on a blockchain network each second. It escalates with the network's expansion.

The hash rate is typically quantified in terahashes, equivalent to 1 trillion hashes per second, due to the several computers producing millions of guesses per second. The Bitcoin network's hash rate is quantified in terahashes per second.

To observe smaller networks, kilohashes per second (1,000/s), mega hashes per second (1,000,000/s), or gigahashes per second (1 billion/s) can be utilized[41].

3.8.4. What is the significance of the hash rate?

The hash rate is essential for assessing a blockchain network's overall security and miners' difficulties obtaining block rewards. The likelihood of a malicious attack on the network diminishes as the number of blockchain miners competing to mine blocks increases.

The hash rate additionally affects the mining difficulty of a specific blockchain. As the hash rate increases, certain blockchains make mining blocks more difficult. This suggests that individual miners may find competing in bitcoin networks with exceptionally high hash rates extraordinarily challenging.

Furthermore, a cryptocurrency's popularity may be assessed by its hash rates. A specific cryptocurrency network is more prone to growth and popularity when increased computational power is dedicated to it.

3.8.5. What is the hash rate of Proof of Work (PoW)?

As of October 2022, the Bitcoin network's hash rate is approximately 240,000,000 terahashes per second (TH/s). In May 2011, the network attained a hash rate of 1 TH/s for the first time, and it has subsequently increased each year you may find all the information's in Bitcoin Mining Network Stats[42].

3.8.6. What Occurs When the Hash Rate Fluctuates (Rises or Falls)?

The hash rate indicates miners' aggregate activity in a Proof of Work network. The implications of an increase in hash rate are as follows:

- Block mining necessitates more computational power.
- The electricity consumption escalates.
- As the network expands beyond the capacity of a single entity to manage, its security increases.
- Mining becomes more difficult as the hash rate increases, and most blockchain network algorithms exhibit a similar trend.

A decline in the hash rate of a PoW blockchain network frequently signifies:

There is a diminished number of miners competing for block rewards and incorporating new blocks.

When a consortium of miners controlling over 50% of the network's hash rate alters the Blockchain, its security diminishes, rendering it more vulnerable to a 51% attack.

Computers employed for mining consume less energy.

Block mining gets less arduous as mining difficulty diminishes.

Where can I access diverse cryptocurrency hash rates?

Observing the hash rates of prominent Proof of Work cryptocurrency blockchain networks in various places is feasible. The hash rates of various cryptocurrencies are quantified on platforms such as BitInfoCharts[43] and others. The following are some of the most popular PoW hash rates:

- Bitcoin
- Ethereum
- Ethereum Classic
- Dogecoin
- Litecoin
- Monero

The integration of advanced technologies such as Cyber-Physical Systems (CPS), Big Data, Cloud Computing, Machine Learning, and Blockchain with healthcare services has improved performance and efficiency through data-driven learning and system interconnection. Nonetheless, the extensive acquisition, dissemination, and retention of healthcare data has introduced complexity and significant risks. A major challenge confronting the healthcare sector is safeguarding sensitive data from hackers while ensuring privacy through authenticated access. Implementing Blockchain-based networks can significantly diminish the risks of healthcare systems and safeguard their data. Adopting blockchain-based networks may mitigate the risks of healthcare systems and protect their data.

Blockchain technology applications in Healthcare encompass secure medical data storage, log management, pharmaceutical supply chain management, and database administration and sharing [44]. The authors [45] investigate and delineate the research opportunities for integrating blockchain solutions with other advanced technologies, such as big data, algorithms, and IoT.

We examine blockchain-based solutions for the security challenges faced by healthcare facilities. In [46], the challenges faced in integrating blockchain technology into healthcare systems concerning security parameters such as stability, confidentiality,

security frameworks, and interoperability are examined. They acknowledge that challenges, including identifying data requirements and individual privacy concerns, accompany these technology benefits for healthcare security. In [47] we explore the potential applications of blockchain technology in medicine and argue that it can resolve challenges associated with diverse data types, such as electronic health records (EHRs). Addressing the advantages of blockchain technology not only in terms of reduced processing times, lower costs, and enhanced transparency but primarily in data security and privacy.

3.9. Advantages and disadvantages of blockchain security in the healthcare sector (specification).

Distributed ledger technology remains in use today for several reasons. The primary significance is its facilitation of the emergence of cryptocurrencies in recent years and the more straightforward utilization of non-cryptographic currencies. The impact of technology is considered to surpass that of cryptocurrencies. Consequently, students and experts in various fields continue to explore Blockchain's true potential.

With the advent of Health 4.0, the healthcare sector is entering a new epoch of innovation. Integrating advanced technologies such as Big Data, Cloud Computing, Machine Learning, Cyber-Physical Systems (CPS), and Blockchain with healthcare services has enhanced performance and efficiency via data-driven learning and system interconnectivity[48].

Nonetheless, the extensive gathering, exchange, and backup of healthcare data has heightened complexity and introduced significant hazards. Protecting sensitive data from cyberattacks while maintaining privacy through verified access is a significant concern in Healthcare. Consequently, we are deploying blockchain-based networks that can substantially reduce vulnerabilities in healthcare systems and safeguard patient data. This essay addresses the following inquiries to enhance readers' understanding of how blockchains might safeguard healthcare data: What data is utilized, when it is necessary, why it is desired, and who demands it. We identify and examine the technological constraints and legal challenges of implementing blockchain-based medical data security to establish a framework for prospective research subjects or instructional guidance.

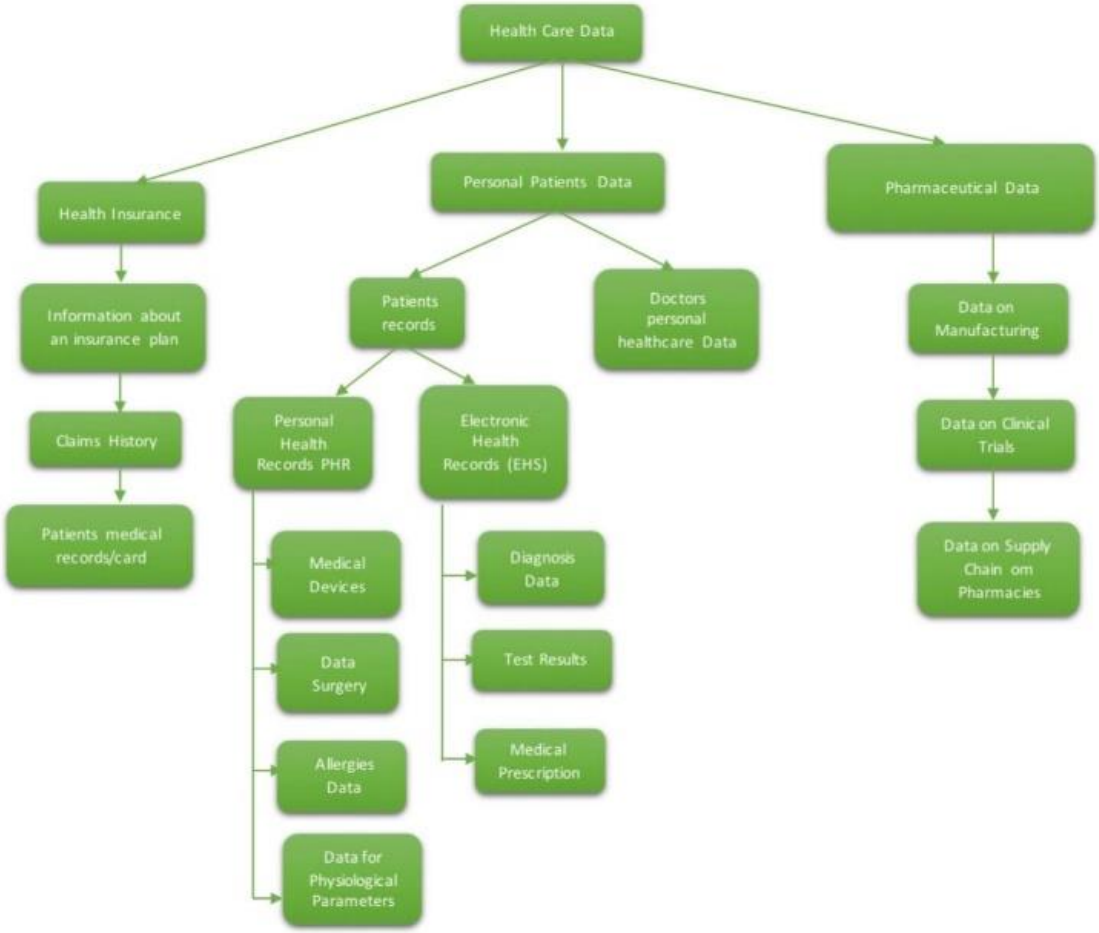


Figure 28. Where the blockchain can be applied in healthcare[34]

So, based on the figure, we can use the health care data that are put in the chain first in health insurance. The companies can first provide the history of the insured patient or the medical records that are public or confirmed by the patient, so that the insurance company can access them. This way, we can provide real-time medical records, allowing the insurance company to make a decision more quickly.

Another significant data record is Personal Patient Data. Based on the records, the patient can access their data as "Personal Health Records PHR," so in this way, the patient can always have Information about their medical record in real-time. Sometimes, the patients do not remember their allergies, or if something happens, the doctor can access the data

[34] https://epa.oszk.hu/04100/04186/00018/pdf/EPA04186_biztud_szemle_2022_ksz_099-108.pdf

in the chain inside the hospital to see the patient's allergies, so that they can have the best medical care. Moreover, when the doctor decides, the patient can see or access the surgery date if needed. So he does not have to go to the hospital. This way, we do not have confusion or misunderstandings. For the patient records, we have to put the doctor records as well, since the doctor can be a patient, too, and all the above can be used in the doctor records as well.

Healthcare data is also needed in the pharmaceutical industry, although most data is focused on manufacturing. So, based on the records of medicine used by the patients, the manufacturers can produce enough medicine so they do not have missing medicine or more than is needed. Of course, the data from medical trials would be essential, as the manufacturer must provide the necessary medical care if the trial is successful. Last but not least is "Data on the Supply Chain," which enables the pharmacy chain to have all the records on the supply of data from all distributors.

All the Information stored on the Blockchain can be accessed by the parties involved. Of course, they have to be a trusted link on the chain, and they should have access depending on the Information needed. Therefore, the doctor can access all patient records, history, and data in real-time; the patient can access their data in real-time; and all other parties, including those from the hospital, should have access to the data on medicines or trials conducted within the hospital. Of course, all the records the third parties take will not include the patient's name. In this way, we can protect the patient and give records to the needed companies so we can do more scientific research or probabilities.

3.10. Technical hurdles to blockchain adoption in the healthcare industry

A functional limitation of blockchain technology is its lack of Scalability for extensive networks. Storing such a substantial volume of data at each node is challenging. The authors propose keeping only specific data, like metadata, hash values, and pointers, on the Blockchain while retaining other data on servers to mitigate this issue. Scalability is merely one issue; the confidentiality of healthcare data constitutes another. Every node in a blockchain maintains a copy of the ledger as it operates on a distributed network. Nonetheless, disseminating copies of a patient's medical diagnosis reports across the network is not conducive to the patient's welfare.

The apprehension regarding data privacy is another rationale for implementing a hybrid data storage solution utilizing Blockchain technology within the healthcare sector. Although not all data is disseminated across the network, every participant can access the Blockchain's transaction data associated with each node's ID. Consequently, the Blockchain is incapable of ensuring the confidentiality of node activities. Alongside blockchain-based encryption, as discussed in the preceding section, alternative encryption methods safeguard user privacy. Contemporary blockchain-based systems include various access control measures designed to address data privacy concerns. No mechanism exists to enforce these norms inside the network without employing functionalities external to the Blockchain's characteristics, despite their integration within the system via block storage. Different consensus algorithms employed in Blockchain possess particular limits in addition to overarching functional constraints. The many consensus algorithms utilized in blockchain technology possess specific limitations besides general functioning constraints. These constraints are universal and equally pertinent to Blockchain applications in Healthcare. Due to the computational resource demands of proof of work, most individual patients and small hospitals cannot pay them. Even in permissioned blockchains, the demand for computational resources undermines the principle of participant equality. Network congestion arises in the PBFT consensus employed by the Hyperledger blockchain due to the extensive volume of messages that must be exchanged across the nodes. Patients increasingly convey personal health information gathered via cellphones and medical IoT devices.

Smart contracts facilitate the implementation of functionalities such as access control, privacy, recording, change, and viewing of healthcare data. Smart contracts significantly facilitate work automation. Nonetheless, certain limitations exist regarding smart contracts. Exert a direct influence on the efficacy of healthcare data security. Once a smart contract's code is recorded on the Blockchain, anyone cannot modify it. Consequently, prior to deployment, developers must identify vulnerabilities. Each validating node executes these contracts upon request to perform an action for transaction validation. The accessibility of all data by each node presents privacy problems. Consequently, when developing a smart contract, it is imperative to exercise caution in ascertaining the volume of data and the encryption keys to provide.

3.11. Regulatory challenges of Blockchain for healthcare data security.

Among these, privacy concerns are significant. Blockchain's immutable nature prevents the deletion of historical data if a patient or organization opts to exit the network. This contravenes the "right to be forgotten" framework established under privacy rights in most nations.

Healthcare data storage systems on the Blockchain remain unstandardized. Companies employ numerous advanced systems based on their requirements. Healthcare enterprises utilizing Blockchain possess distinct data storage formats, encryption techniques, and consensus algorithms. Hospitals and other healthcare organizations encounter difficulties in communication due to interoperability issues among the blockchains. The necessity to transfer their data between chains poses a challenge for patients. Consequently, standard operating procedures for blockchain operations are essential.

In the healthcare sector, where sensitive patient data is at stake, the requirement for cryptographic verification and majority consent before adding new blockchain blocks fosters transparency and collective responsibility. It provides patients with several advantages regarding the regulation of access to and utilization of their data. By alleviating the bottlenecks associated with the system's centralized operation, it also streamlines the processes for physicians, healthcare organizations, and medical research institutions to obtain relevant Information. Blockchain obviates the necessity for a trusted intermediary and distributes the responsibility for data security among all participants via individual encryption. To comprehensively secure, safeguard privacy, and assure accountability for relevant data, healthcare organizations currently emphasize the decentralization of systemic operations. To attain the same objective, peer-to-peer networks utilizing blockchain technology are widely employed. Nonetheless, none of the proposed blockchain-based healthcare networks are entirely decentralized. The administrative nodes of these systems, which disrupt them, necessitate research to attain complete decentralization and total transparency. Healthcare blockchain solutions necessitate a sustainable mechanism for generating and distributing incentives to miners and validators to uphold the network. In the healthcare sector, it has become challenging to maintain all data on the Blockchain. Moreover, data privacy holds similar significance.

Consequently, only the metadata and hash values are stored on the blockchain instead of all healthcare data.

Under these conditions, additional data encryption is applied in conjunction with the encryption provided by the Blockchain to ensure data privacy. Blockchain-based networks can substantially enhance data security for future healthcare systems; nevertheless, continuous research on scalability and encryption techniques is essential. Alongside technological challenges, there are legislative concerns around healthcare data ownership and the necessity for a standardized inter-organizational operational framework. The Structure and functioning of Blockchain require a technological redesign specifically customized to the data types, organizational hierarchies, and security considerations within the healthcare business.

3.11.1. What is hash rate, and why is it crucial to comprehend it to evaluate the security of the Blockchain?

The hash rate quantifies the computational capability of a proof-of-work (PoW) cryptocurrency network. The mining power of a blockchain network is utilized to evaluate its health, security, and mining difficulty.

A hash is a randomly generated alphanumeric code, and the act of attempting to deduce it is referred to as hashing. The total number of guesses executed by computers on the network is quantified, whereas the hash rate reflects the number of guesses generated per second throughout the entire network.

3.11.2. Blockchain Defense Technology for Individual Node Defense

Defense through deployment on an alternative node is the predominant method for blockchain safeguarding. When an individual node employs its defense mechanisms—primarily cryptography, encryption, hashing, digital signatures, authentication, and key management technologies—it is referred to as "single-node independent defense." This approach offers the benefit of high portability, allowing defense technologies developed on a single node to be readily transferred to other nodes. The security assurance of this

strategy mostly relies on the robustness of the individual node. This section examines the single-node defense technology, along with its present development state and focal areas.

3.12. Cryptography

Cryptography offers substantial protection for data availability, confidentiality, and integrity. Blockchain technology frequently employs cryptography to ensure security and reliability, safeguarding transactions and blockchain data[49].

Data can be encrypted and converted into ciphertext to maintain privacy and confidentiality. Blockchain can utilize cryptography to secure user identities and transaction data, thereby protecting user privacy and preventing fraud.

Traditional text search queries necessitate scanning the entire Blockchain, which is laborious and may expose confidential Information. An attribute-based keyword search approach is preferable in this instance. Encrypted blockchains may be rapidly queried without disclosing any personal data. Fuzzy matching can be utilized by users locally for search queries, after which the corresponding results can be uploaded to the Blockchain and authenticated by smart contracts. Encrypting the data and conducting a fuzzy search for several keywords is an alternate method that can be utilized. Using the smart contract, the uploaded matches will be analyzed, the Blockchain will be scanned, and access to data that is appropriately protected will be provided. By using the appropriate key to decrypt the data, users can obtain plaintext results that are in accordance with the parameters of their search requirements.

Maintaining the confidentiality of the client is of the utmost importance when dealing with sensitive materials like photographs. These articles make use of encryption to ensure that the image can only be accessed by authorized users and to protect the image's confidentiality. Furthermore, the technology of Blockchain is utilized in order to monitor encrypted images and tales. The qualities of Blockchain, which include decentralization, immutability, and diffusion, have the potential to ensure the security and precision of encrypted data. For the purpose of carrying out encryption and decryption procedures in environments with restricted resources, the study makes use of a lightweight authentication approach.

From the point of view of the encryption model, a model that is suitable for deployment across a large number of nodes needs to be trained in order to make it possible for each node to carry out the function that has been assigned to it.

Equity, security, and reliability must be guaranteed during training to enhance the model's credibility. Attribute-based encryption technology is employed to protect the training data, while a smart contract governs communication between nodes to assure the fairness of the training process.

Investigating the potential vulnerabilities of single-node defensive technologies is a field that requires additional scrutiny. This strategy enables nodes to operate independently and mobile, although it jeopardizes the entire blockchain network if the security of a single node is breached.

3.13. The hashing algorithm

The hashing algorithm converts data of arbitrary length into fixed-length digests. Blockchain technology utilizes hashing algorithms to ensure consistency and integrity. The blocks in the Blockchain encompass a hash value derived from a hashing method applied to all transaction data within that Block[50]. Upon creation, a block's hash value is disseminated around the network, allowing other nodes to assess its integrity and immutability. The Bitcoin hashing algorithm authenticates the precision and uniformity of each Block's proof-of-work[51].

As blockchain technology advances, a growing number of transactions will be documented on the Blockchain. Consequently, hashing algorithms must be faster and more efficient in managing the increasing amount of data. Enhancing the efficiency of hashing algorithms is still prevalent. The field-programmable gate array (FPGA) is employed to construct the approach, and an optimization of the hash algorithm utilizing the parallel residual carry adder is provided. Experimental results indicate that the proposed hashing method surpasses conventional hashing algorithms in performance and space efficiency, hence enhancing the effectiveness and efficiency of blockchain applications.

Hashing techniques that are resistant to quantum computing could be included into blockchain technology. There is a possibility that quantum computing will make brute-force attacks possible by utilizing hashing methods. Increasing the security of blockchain networks could be accomplished by conducting research on hashing algorithms that are resistant to quantum mistakes [52]. The hashing algorithms used by blockchains requires electricity. In light of the large amount of computational power that is required for blockchain mining and verification, it is necessary to reevaluate the energy consumption of hashing algorithms. The blockchain technology can be made more environmentally friendly with the implementation of energy-efficient hashing algorithms and blockchain protocols. I find it fascinating to investigate the interoperability of blockchain networks and the various hashing algorithms.

Data and transaction sharing across specialized blockchain networks will gain significance. The acceptance and efficiency of Blockchain may improve through standardized hashing algorithms that enhance interoperability among blockchain networks.

3.14. Electronic signature

Digital signatures function as a means of document authentication. Blockchain technology enables digital signatures to authenticate transactions, mitigate fraud, and avert double-spending. Digital signatures unequivocally identify the initiator of a transaction and detect any alterations to its information, preventing impersonation and identity fraud; they can also serve to verify users. In asymmetric cryptography, the public and private keys facilitate digital signatures by hashing the original material and encrypting it with the private key, resulting in digital signatures[53]. The recipient verifies the validity of the digital signature using the public key. A blockchain member may digitally authenticate transactions with their private key, while other nodes can verify these digital signatures utilizing the public key. Digital signatures protect against blockchain threats, including transaction forgery and manipulation. A blockchain-based authentication system that safeguards cloud services from malicious attacks.

3.15. Verification of identity

Authentication is a process for verifying a user's identity. Blockchain authentication is achievable by using a user's public and private keys to validate their identity and authenticity[54]. To safeguard users' digital assets and private information, building more reliable and secure technologies and solutions is imperative. Blockchain authentication constitutes a significant security concern. Building more reliable and secure technologies and solutions is imperative to safeguard users' digital assets and private information. Blockchain authentication is a significant security concern. Assume that hackers successfully acquire the user's private key. Consequently, they may utilize it to execute transactions and access digital assets under the user's identity, potentially resulting in significant financial losses and security concerns.

A multi-factor authentication framework utilizing random terminal selection and decentralized identification (DID) is essential for enhancing identity verification security[55]. The system employs various randomly chosen authentication methods to ensure security and leverages blockchain technology to store and authenticate user identity data. This method can enhance the security and effectiveness of authentication. A blockchain-based transaction authentication method resistant to quantum assaults is optimal to enhance security, including both traditional and quantum encryption. This strategy can enhance the security of transaction authentication and offer robust protection against quantum computing attacks.

3.16. Management of Key’s

Key management offers a secure method for the preservation of encryption keys and passwords. Blockchain key management facilitates the secure retention of private keys, thereby averting loss and unauthorized disclosure. Scholars are employing blockchain technology to develop innovative solutions or improve current ones that tackle certain security, privacy, and efficiency challenges.

3.17. Collaborative multi-node defensive Technology

Multi-node collaborative defense technology establishes a distributed defensive network to enhance blockchain security. Multi-node collaborative security tools leverage the decentralized and immutable characteristics of Blockchain to identify and prevent many forms of threats. The method mitigates the effects of network attacks on systems while augmenting defensive capabilities and response times.

In the domain of multi-node collaborative defense, strength resides in collaboration. Although each node is capable of self-defense, the ultimate efficacy of the defensive system is achieved through collaborative efforts among the nodes. The efficacy of this strategy depends on the security of individual nodes and the collaboration of the system. To guarantee system security, coordinated and validated nodes can detect and eliminate compromised or attacked nodes.

Multi-node collaborative defense surpasses single-node independent defense in security efficacy. The former necessitates coordination and verification, whereas the latter depends exclusively on node security. The capacity to synchronize and verify among nodes renders multi-node collaborative protection a more dependable and secure alternative.

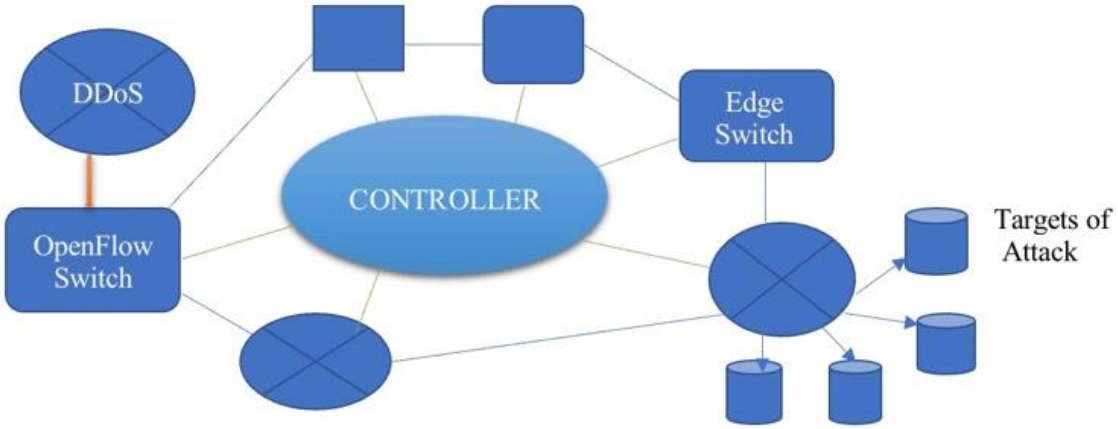


Figure 29. Schematic diagram for the multi-node collaborative defensive paradigm.[35]

Conventional distributed denial-of-service (DDoS) protections are insufficient to mitigate extensive attacks[56]. Consequently, it has been established that incorporating defensive measures is superior to augmenting the defensive capabilities of individual systems. Conventional centralized protection systems can lack requisite hardware and software capabilities. A collaborative, multi-domain DDoS mitigation system offers protective services built upon the current distributed architecture.

Cybersecurity has expanded significantly over the past two decades due to the Internet's numerous straightforward yet potent attack routes, such as distributed denial-of-service (DDoS) attacks[57]. DDoS attackers have numerous new opportunities to exploit the decentralized characteristics of fast-developing collaborative environments such as cloud computing, software-defined networking, and the Internet of Things. By compromising devices, attackers can create vast networks of bots to execute large-scale attacks covertly. DDoS prevention must be effective and efficient. [58]The author examines DDoS threat evaluations and novel security strategies across several domains.

The interactive dashboards of a blockchain-based collaborative defense platform display the current threat mitigation status, enabling security analysts to respond to attacks individually or collectively. BloSS is a cooperative, multi-domain DDoS prevention

[35] https://www.researchgate.net/figure/The-schematic-diagram-of-the-multi-node-collaborative-defense-model_fig2_374549569

system constructed on the Blockchain, wherein each autonomous system (AS) joins a defensive consortium. [59]The operational deployment of BloSS is now automated for DDoS mitigation. However, it lacks interactivity and aesthetic appeal. Cybersecurity professionals can now utilize a security dashboard management system that offers a comprehensive overview of all attack-related Information.

Human decision-makers, such as security analysts, are essential in utilizing this dashboard to assess the severity of the threat and determine the optimal course of action. This governance dashboard effectively diminishes the operational intricacy of blockchain-based cooperative defense, underscoring the significance of their experience and discernment in the cybersecurity procedure.

Nodes of the Collaborative Intrusion Detection System (CIDS) provide essential detection and control data for cooperative defense. Software-defined networking (SDN) serves as a vital platform for Collaborative Intrusion Detection Systems (CIDS)[60] applications, providing network controllers for multi-autonomous system networks to safeguard against insider threats and to inhibit the dissemination of erroneous and malicious detection signatures to other participating controllers; however, CIDS research remains deficient in robust trust management and the integrity protection of collaborative defenses within SDN controllers.

The implementation of SIs is problematic owing to the substantial requirements of current DDoS mitigation technologies on bandwidth and processing capabilities. The implementation of a distributed collaborative ingress defense (DCED) architecture, founded on blockchain technology, is essential for protecting SIs against DDoS attacks[61]. This advanced system, comprising distributed detection digest handlers, digest virtual aggregation, and ingress control, represents a crucial advancement in cybersecurity, emphasizing the necessity and significance of its implementation.

4. DEVELOPING A BLOCKCHAIN FOR PATIENT RECORD MANAGEMENT SYSTEMS (PRM)

Utilizing Blockchain to establish an autonomous and transparent patient data management system. We are incorporating blockchain technology into healthcare devices

to enhance the accuracy and privacy of patient data. Integrating blockchain technology can enhance security and transparency in the storage and processing of patient data within hospital IT systems. At the Python application level, we can establish specific security mechanisms to safeguard sensitive patient data within the hospital IT system.

4.1. Why Python?

Employing Python to create a blockchain-based patient record management system presents numerous benefits, particularly in a healthcare setting where security, Scalability, and swift growth are essential. Herein is the rationale for Python's distinction:

1. Clarity and Comprehensibility

The clarity of Python's syntax facilitates rapid prototyping and enhances collaboration among developers, including those lacking extensive blockchain knowledge.

In Healthcare, where interdisciplinary teams (physicians, developers, administrators) collaborate, Python facilitates a clearer comprehension of the codebase for all participants.

2. Abundant Libraries and Frameworks

Python possesses robust libraries for blockchain development, including pycryptodome (for cryptographic functions), Flask (for RESTful APIs), and web3.py (for Ethereum interface).

These technologies facilitate operations such as encryption, consensus mechanism execution, and smart contract integration.

3. Robust Support for Data Management

Patient records frequently encompass both structured and unstructured data, including text, photographs, and laboratory findings.

Python is proficient in data processing using libraries such as pandas, NumPy, and OpenCV, facilitating the management, analysis, and integration of medical data on the Blockchain.

4.Cross-Platform and Open Source

Python is an open-source language that operates on all main platforms, hence reducing development expenses and enhancing accessibility for hospitals or clinics with constrained resources.

5. Accelerated Prototyping

Rapidly construct and evaluate blockchain systems (e.g., permissioned blockchains) designed to comply with patient privacy standards such as HIPAA or GDPR.

6. Community and Documentation

Python possesses a substantial and dynamic community. Regardless of whether you are employing proof-of-authority consensus or interfacing with EMR systems, someone likely has addressed a comparable issue.

Architecture and a fundamental code snippet for a blockchain-based Patient Record Management System utilizing Python

- A basic blockchain structure
- Adding patient records as transactions
- Flask API to interact with the Blockchain

4.1.1. Architecture Overview

[User Interface]

|

[Flask API Server]

|

[Blockchain Ledger] -- Stores hashed patient records// Maintains encrypted patient records

|

[Data Storage / IPFS / External DB] -- (Optional) for large files like scans

Overview of Architecture

A blockchain-based patient record management system guarantees safe, immutable, and decentralized storage of medical records, while upholding patient privacy and access control. **The structure comprises:**

***1.Blockchain Layer*:**

• Type: Private or permissioned blockchain (e.g., Hyperledger Fabric or Ethereum-based).

• Purpose: Preserves encrypted patient records and access logs as immutable transactions.

• Consensus Mechanism: Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) to enhance efficiency in a permissioned network.

• Smart Contracts: Oversee record generation, access control, and modifications (e.g., via Solidity or Python-based chaincode).

***2. Data Preservation*:**

• On-Chain: Metadata (e.g., record ID, patient ID, hash of the record, access rights) to ensure integrity and auditability.

• Off-Chain: Encrypted patient records are maintained in a secure database (e.g., IPFS or a centralized encrypted database) to enhance blockchain efficiency.

• Encryption: AES-256 for data encryption; public-private key pairs for access management.

***3. Application Layer*:**

• Frontend: A web or mobile application facilitating interaction between patients and healthcare providers within the system.

• Backend: Python-based APIs (such as Flask or FastAPI) for interfacing with the blockchain and off-chain storage.

• Identity Management: Utilization of decentralized identifiers (DIDs) or role-based access control (RBAC) for patients, physicians, and administrators.

4. Access Control:

• Patients possess ownership of their records and manage access permissions through smart contracts.

Multi-signature wallets or cryptographic signatures guarantee secure access.

5. Interoperability:

• Complies with standards such as HL7 FHIR to ensure compatibility with current healthcare systems.

• Application Programming Interfaces for integration with hospitals and clinics.

6. Security:

• Comprehensive end-to-end encryption for data both in transit and at rest.

• Blockchain audit logs for all record access and alterations.

• Optional zero-knowledge proofs for privacy-preserving inquiries.

Essential Python Code Snippets

The following are concise code snippets illustrating essential components utilizing Python. This example ("silvana1") employs a fundamental Ethereum-based blockchain utilizing a local test network (e.g., Ganache) and Web3.py for interaction, in conjunction with AES encryption for off-chain storage. For a production system, one would integrate with a more sophisticated blockchain such as Hyperledger or a tailored solution.

4.1.2. Smart Contract (Solidity) for Record Administration

This contract governs record metadata and access control. Utilize a tool such as Remix or Truffle for deployment.

// **SPDX-License-Identifier: MIT**[62]
pragma solidity ^0.8.0;

contract PatientRecord {
struct Record {

```
string recordId;
string patientId;
string recordHash; // Hash of encrypted record
address[] authorized; // List of authorized addresses
}

mapping(string => Record) private records;
mapping(address => string) private patientToId;

event RecordAdded(string recordId, string patientId);
event AccessGranted(string recordId, address authorized);

function addRecord(string memory _recordId, string memory _patientId, string memory
_recordHash) public {
require(bytes(patientToId[msg.sender]).length != 0, "Patient not registered");
records[_recordId] = Record(_recordId, _patientId, _recordHash, new address[](0));
records[_recordId].authorized.push(msg.sender);
emit RecordAdded(_recordId, _patientId);
}

function grantAccess(string memory _recordId, address _authorized) public {
require(keccak256(bytes(records[_recordId].patientId)) ==
keccak256(bytes(patientToId[msg.sender])), "Not patient");
records[_recordId].authorized.push(_authorized);
emit AccessGranted(_recordId, _authorized);
}

function getRecord(string memory _recordId) public view returns (string memory,
string memory, address[] memory) {
require(isAuthorized(_recordId, msg.sender), "Not authorized");
Record memory record = records[_recordId];
return (record.recordId, record.recordHash, record.authorized);
```

```
}

function registerPatient(string memory _patientId) public {
patientToId[msg.sender] = _patientId;
}

function isAuthorized(string memory _recordId, address _user) private view returns
(bool) {
for (uint i = 0; i < records[_recordId].authorized.length; i++) {
if (records[_recordId].authorized[i] == _user) return true;
}
return false;
}
}
```

4.1.3. Python Backend (Web3.py for Blockchain Engagement)

This Flask-based API interfaces with the smart contract and manages off-chain storage.

```
from flask import Flask, request, jsonify
from web3 import Web3
from cryptography.fernet import Fernet
import hashlib
import json

app = Flask(__name__)

# Connect to Ethereum node (e.g., Ganache)
w3 = Web3(Web3.HTTPProvider('http://127.0.0.1:7545'))
w3.eth.default_account = w3.eth.accounts[0]
```

```
# Load smart contract
with open('PatientRecord.json') as f:
contract_data = json.load(f)
contract_abi = contract_data['abi']
contract_address = '0xYourContractAddress' # Replace with deployed contract address
contract = w3.eth.contract(address=contract_address, abi=contract_abi)

# Encryption setup
key = Fernet.generate_key()
cipher = Fernet(key)

# Simulated off-chain storage (replace with IPFS or database)
offchain_storage = {}

@app.route('/register_patient', methods=['POST'])
def register_patient():
data = request.json
patient_id = data['patient_id']
tx_hash = contract.functions.registerPatient(patient_id).transact()
w3.eth.wait_for_transaction_receipt(tx_hash)
return jsonify({"message": "Patient registered", "patient_id": patient_id})

@app.route('/add_record', methods=['POST'])
def add_record():
data = request.json
record_id = data['record_id']
patient_id = data['patient_id']
record_data = data['record_data']

# Encrypt record
encrypted_record = cipher.encrypt(record_data.encode())
record_hash = hashlib.sha256(encrypted_record).hexdigest()
```

```
# Store encrypted record off-chain
offchain_storage[record_id] = encrypted_record

# Store metadata on-chain
tx_hash = contract.functions.addRecord(record_id, patient_id, record_hash).transact()
w3.eth.wait_for_transaction_receipt(tx_hash)

return jsonify({"message": "Record added", "record_id": record_id})

@app.route('/grant_access', methods=['POST'])
def grant_access():
data = request.json
record_id = data['record_id']
authorized_address = data['authorized_address']
tx_hash = contract.functions.grantAccess(record_id, authorized_address).transact()
w3.eth.wait_for_transaction_receipt(tx_hash)
return jsonify({"message": "Access granted"})

@app.route('/get_record/<record_id>', methods=['GET'])
def get_record(record_id):
record_id, record_hash, authorized = contract.functions.getRecord(record_id).call()

# Verify record integrity
encrypted_record = offchain_storage.get(record_id)
if not encrypted_record:
return jsonify({"error": "Record not found"}), 404

if hashlib.sha256(encrypted_record).hexdigest() != record_hash:
return jsonify({"error": "Record tampered"}), 400

# Decrypt record
```

```
decrypted_record = cipher.decrypt(encrypted_record).decode()
return jsonify({
"record_id": record_id,
"record_data": decrypted_record,
"authorized": authorized
})

if __name__ == '__main__':
app.run(debug=True)
```

4.1.4. Encryption for Off-Chain Storage

The aforementioned code employs cryptography. Fernet for AES encryption. Ensure the key is securely held, such as in a key management system, during manufacturing.

1. Establish Blockchain:

• Implement the Solidity contract utilizing Remix or Truffle on a local Ethereum node (e.g., Ganache).
• Revise the contract_address within the Python code.

2. Install Dependencies:

Install Flask, Web3, and Cryptography using pip.

3. Execute Flask API:

execute python app.py

4. Evaluate Endpoints:

• Register a patient: POST /register_patient with {"patient_id": "P001"}.
• Create a record: POST /add_record with {"record_id": "R001", "patient_id": "P001", "record_data": "Patient diagnosis: Influenza"}.
• Provide access: POST /grant_access with {"record_id": "R001", "authorized_address": "0xDoctorAddress"}.

• Fetch record: GET /get_record/R001.

4.1.5. Essential Factors

• ***Scalability***: Utilize IPFS or a distributed database for off-chain storage to accommodate extensive medical records.
• ***Privacy:*** Employ zero-knowledge proofs or homomorphic encryption for enhanced privacy.
• ***Interoperability:*** Integrate using FHIR APIs to ensure compatibility with hospital systems.
• ***Security:*** Employ hardware security modules (HSMs) for key management and provide secure multi-party computation for access control.
• ***Performance***: Enhance gas efficiency in smart contracts and use batch transactions for improved efficacy.

Incorporating IPFS (Inter Planetary File System) into a blockchain-based patient record management system improves scalability and decentralization by storing extensive encrypted patient records off-chain while preserving their integrity and accessibility. IPFS is a peer-to-peer protocol designed for the storage and dissemination of files within a distributed file system, wherein files are identified by their cryptographic hash (Content Identifier, or CID). I will elucidate the integration method, its advantages, and furnish Python code snippets to enhance the previously discussed system.

4.2. What are the advantages of integrating IPFS?

Scalability: Blockchain storage is costly and inefficient for substantial data, such as

medical records (e.g., image files, PDFs). IPFS retains these off-chain, with only metadata (e.g., CID, hash) recorded on the blockchain.
Decentralization: IPFS disseminates data among nodes, diminishing dependence on centralized servers.
Integrity: Files are identified by their hash, guaranteeing secure storage against tampering.
Availability: IPFS guarantees that records remain accessible as long as they are hosted by any node inside the network.
Cost Efficiency: Storing substantial files on IPFS is more economical than on-chain storage.

4.2.1. Architecture for IPFS Integration

The integration alters the Data Storage layer of the prior architecture:
On-Chain: Archive the IPFS CID, record ID, patient ID, and access rights within the blockchain through the smart contract.
Utilize IPFS for the storage of encrypted patient records off-chain. The CID is a distinctive hash associated with the file.

Procedure:

Encrypt the patient record utilizing AES-256.
Upload the encrypted record to IPFS to obtain a CID.
Record the CID and metadata on the blockchain.
To obtain, query the blockchain for the CID, retrieve the file from IPFS, and decrypt it.
Access Control: The blockchain smart contract regulates access to the CID, while encryption guarantees that only authorized individuals can decrypt the file.

Procedure for IPFS Integration: Establish IPFS.

Operate a local IPFS node or utilize a hosted service such as Infura's IPFS gateway.
Install the IPFS daemon or utilize a Python module such as ipfshttpclient to engage with

IPFS.

Encrypt and Upload Documentation:

Utilize a symmetric key, such as Fernet, to encrypt the patient record.
Upload the encrypted file to IPFS and obtain the CID.

Preserve Metadata on Blockchain:

Revise the smart contract to retain the CID in lieu of a generic record hash.
Document the CID in the blockchain upon the addition of a patient record.

Obtain Records:

Access the blockchain to retrieve the CID and permitted users.
Utilize the CID to retrieve the encrypted file from IPFS.

Decrypt the file for permitted users.

Revised Code Excerpts (Python with IPFS)
I will enhance the existing Flask-based Python backend by including IPFS through the ipfshttpclient library. The smart contract stays fundamentally unchanged, with the recordHash field now understood as the IPFS CID.

1. Install Dependencies

Install the necessary Python libraries for IPFS:
Install the following packages: ipfshttpclient, cryptography, flask, web3 using pip.
Verify if a local IPFS node is operational (ipfs daemon) or utilize a remote IPFS API (e.g., Infura).

2. Altered Python Backend (Flask integrated with IPFS)

This modifies the prior Flask API to provide IPFS storage and retrieval.

from flask import Flask, request, jsonify

```
from web3 import Web3

from cryptography.fernet import Fernet

import ipfshttpclient

import json

app = Flask(__name__)

# Connect to Ethereum node (e.g., Ganache)

w3 = Web3(Web3.HTTPProvider('http://127.0.0.1:7545'))

w3.eth.default_account = w3.eth.accounts[0]


# Load smart contract

with open('PatientRecord.json') as f:

    contract_data = json.load(f)

contract_abi = contract_data['abi']

contract_address = '0xYourContractAddress'  # Replace with deployed contract address

contract = w3.eth.contract(address=contract_address, abi=contract_abi)

# Connect to IPFS

ipfs_client = ipfshttpclient.connect('/ip4/127.0.0.1/tcp/5001')  # Local IPFS node

# Encryption setup

key = Fernet.generate_key()

cipher = Fernet(key)

@app.route('/register_patient', methods=['POST'])
```

```
def register_patient():
    data = request.json
    patient_id = data['patient_id']
    tx_hash = contract.functions.registerPatient(patient_id).transact()
    w3.eth.wait_for_transaction_receipt(tx_hash)
    return jsonify({"message": "Patient registered", "patient_id": patient_id})
@app.route('/add_record', methods=['POST'])
def add_record():
    data = request.json
    record_id = data['record_id']
    patient_id = data['patient_id']
    record_data = data['record_data']

    # Encrypt record
    encrypted_record = cipher.encrypt(record_data.encode())

    # Upload encrypted record to IPFS
    ipfs_result = ipfs_client.add_bytes(encrypted_record)
    ipfs_cid = ipfs_result  # CID of the uploaded file

    # Store metadata on-chain (CID as recordHash)
```

```
    tx_hash = contract.functions.addRecord(record_id, patient_id, ipfs_cid).transact()
    w3.eth.wait_for_transaction_receipt(tx_hash)

    return jsonify({"message": "Record added", "record_id": record_id, "ipfs_cid": ipfs_cid})

@app.route('/grant_access', methods=['POST'])
def grant_access():
    data = request.json
    record_id = data['record_id']
    authorized_address = data['authorized_address']
    tx_hash = contract.functions.grantAccess(record_id, authorized_address).transact()
    w3.eth.wait_for_transaction_receipt(tx_hash)
    return jsonify({"message": "Access granted"})

@app.route('/get_record/', methods=['GET'])
def get_record(record_id):
    try:
        # Query blockchain for record metadata
        record_id, ipfs_cid, authorized = contract.functions.getRecord(record_id).call()
```

```
        # Fetch encrypted record from IPFS
        encrypted_record = ipfs_client.cat(ipfs_cid)

        # Decrypt record
        decrypted_record = cipher.decrypt(encrypted_record).decode()

        return jsonify({
            "record_id": record_id,
            "record_data": decrypted_record,
            "ipfs_cid": ipfs_cid,
            "authorized": authorized
        })
    except Exception as e:
        return jsonify({"error": str(e)}), 400

if __name__ == '__main__':
    app.run(debug=True)
```

4.3. Smart Contract (Unaltered)

The Solidity smart contract from the prior response remains unchanged, as it already accommodates the storage of a recordHash, which is now utilized as the IPFS CID. Interpret the recordHash field as the CID when engaging with the contract.

Initiating the System with IPFS Activate IPFS Node:

Install IPFS: Adhere to the guidelines provided at ipfs.io.
Execute the daemon:
IPFS daemon Deploy Smart Contract:
Utilize Remix or Truffle to deploy the PatientRecord contract on a local Ethereum node, such as Ganache.
Revise the contract_address in the Python code.
Execute Flask API:
Execute python app.py
Testing Endpoints:
Register a patient: POST /register_patient with {"patient_id": "P001"}.
Insert a record: POST /add_record with {"record_id": "R001", "patient_id": "P001", "record_data": "Diagnosis: Influenza"}.
This uploads the encrypted data to IPFS and records the CID on the blockchain.
Authorize access: POST /grant_access with {"record_id": "R001", "authorized_address": "0xDoctorAddress"}.
Obtain record: GET /get_record/R001.
This obtains the CID from the blockchain, acquires the file from IPFS, then decrypts it.
Essential Factors for IPFS Integration Management of IPFS Nodes:
Operate a local IPFS node for testing purposes; however, for production, evaluate hosted services (e.g., Infura, Pinata) or establish a private IPFS cluster for enhanced reliability.
Pin files to guarantee persistence (e.g., via ipfs_client.pin.add(ipfs_cid)).

Execution:

IPFS retrieval may be sluggish if files are unpinned or if node density is low. Utilize pinning services or a specialized IPFS cluster.
Store commonly accessed records locally to minimize latency.

Safety:

Encryption is essential due to the default public nature of IPFS. The aforementioned code employs AES-256 (Fernet); however, it is imperative to handle the encryption key securely (e.g., with a key management system).

Utilize private IPFS networks for confidential data to limit access to authorized nodes.

Data Accessibility:

Guarantee that files are affixed by many nodes to avert data loss in the case of a node becoming down.
Assess the health and connectivity of the IPFS node.

Adherence:

In healthcare, adhere to regulations such as HIPAA or GDPR. The public nature of IPFS necessitates robust encryption and access control to safeguard patient data.
Record access attempts on the blockchain for audit purposes.

Management of Errors:

Manage IPFS connection failures or absent CIDs with poise (e.g., implement retry mechanisms, utilize fallback storage).

Verify CID integrity by contrasting the hash of the obtained file with the CID.

Advantages of IPFS in This Framework:

Decentralized Storage: Mitigates single points of failure in contrast to centralized databases.
Tamper-Proof: CIDs guarantee data integrity, as any alteration in the file produces a distinct CID.
Scalability: Efficiently manages extensive medical files (e.g., MRIs, X-rays). Interoperability: IPFS CIDs facilitate sharing across systems, allowing cross-institutional access.

Possible Improvements

Private IPFS Network: Limit IPFS nodes to sanctioned healthcare providers to bolster privacy.
IPFS Pinning Services: Utilize services such as Pinata to guarantee file permanence.
File Sharding: Distribute extensive files across IPFS for expedited retrieval.

Hybrid Storage: Integrate IPFS with a centralized encrypted database for essential records necessitating minimal latency.

Decentralized storage solutions

Decentralized storage solutions are essential for a blockchain-based patient record management system, as they provide secure, scalable, and robust off-chain storage of extensive encrypted medical information while preserving data integrity and accessibility. I will elucidate essential decentralized storage options pertinent to this use case, their connection with the aforementioned system, and factors for deployment. I will also present a concise comparison and updated Python code snippets to illustrate integration beyond IPFS, emphasizing alternatives like as Filecoin, Arweave, and Storj.

4.4. Summary of Decentralized Storage Solutions

Decentralized storage systems allocate data among a network of nodes, hence removing dependence on centralized servers. They employ cryptographic methods to guarantee data integrity and availability. This patient record management system employs technologies that store encrypted medical documents off-chain, while metadata (such as content hashes or identifiers) is retained on the blockchain.

1. InterPlanetary File System (IPFS)

A peer-to-peer protocol for the storage and dissemination of files, identified by their cryptographic hash (CID).
Principal Attributes:
Content-addressed storage guarantees data integrity.
Free and open-source, lacking inherent incentivization for storage.

Necessitates pinning to guarantee data persistence.

Application: Optimal for the decentralized storage of encrypted medical records, with Content Identifiers (CIDs) recorded on the blockchain.

Advantages:

Extensively utilized, featuring comprehensive tools (e.g., ipfshttpclient).
Absence of storage expenses for self-hosted nodes.

Disadvantages:

Lack of intrinsic motivation for prolonged preservation.
Requires pinning services (e.g., Pinata, Infura) for data permanence.
Integration: Previously illustrated in the prior response. Utilizes ipfshttpclient for the

upload and retrieval of encrypted records.

2. Filecoin Description:

A decentralized storage network constructed on IPFS, with a marketplace where customers compensate for data storage and miners are motivated to offer storage services.
Principal Attributes:
Integrates with IPFS, employing CIDs for content addressing.
Incentivized storage guarantees data persistence via storage agreements.
Facilitates retrieval agreements for expedited access.

Use Case: Appropriate for the prolonged preservation of patient records, guaranteeing accessibility via compensated storage agreements. (See algorithm figure 1).

Advantages:

Inherent economic motivations for data retention.
Effortless incorporation with IPFS workflows.

Disadvantages:

Mandates payment in FIL (Filecoin's token), hence escalating expenses.
More intricate configuration than IPFS alone.
Integration: Utilize libraries like as pyfilecoin or hosted services (e.g., Filecoin’s Lotus API, Web3.Storage) to upload encrypted records and save CIDs on the blockchain.

3. Arweave

A decentralized storage protocol dedicated to permanent data retention ("permaweb"), wherein users incur a singular price for everlasting storage.
Principal Attributes:
Blockweave technology guarantees the perpetual storage of data.

Content referenced by transaction identifiers.
Inherent support for data immutability.

Use Case: Optimal for unchangeable patient records that require perpetual accessibility (e.g., essential medical histories).

Advantages:
Single payment for perpetual storage.
Emphasis on data persistence.

Disadvantages:
Elevated initial expenses in comparison to IPFS or Filecoin.
Reduced adaptability for dynamic data modifications.
Integration: Utilize the Arweave Python module to upload encrypted records and archive transaction IDs on the blockchain.

4. Storj
A decentralized cloud storage platform that encrypts and fragments data across a worldwide network of nodes.
Principal Attributes:
Client-side encryption and data sharding for enhanced privacy and redundancy.
Usage-based paradigm predicated on storage capacity and bandwidth utilization.
Optimal efficiency for retrieval.
Use Case: Appropriate for high-performance retrieval of patient records, including imaging files and real-time clinical data.
Advantages:

Expedited access facilitated by sharding and redundancy.
Robust privacy using client-side encryption.

Disadvantages:
Continuing expenses for storage and bandwidth.

Less integrated with blockchain ecosystems than IPFS/Filecoin.
Integration: Utilize the storj-python package or Storj's API to upload encrypted data and maintain access metadata on the blockchain.

4.5. Comparison of Decentralized Storage Solutions

StorjSegmented, usage-basedCompensate for storage and bandwidthElevated (superfluity)ElevatedOptimal performance, frequent accessibility
For a patient record management system, utilizing IPFS alongside a pinning service (such as Pinata) or Filecoin is typically the optimal initial choice, owing to its compatibility with blockchain ecosystems and their equilibrium of cost and data persistence. Arweave is optimal for enduring records.

Table 5. Comparison of Decentralized Storage Solutions

Solution	**Storage Model**	**Cost**	**Persistence**	**Performance**	**Best Use Case**
IPFS	Peer-to-peer, content-addressed	Free (self-hosted), pinning services cost	Requires pinning	Moderate	General-purpose, cost-sensitive systems
Filecoin	Incentivized, IPFS-based	Pay-per-deal (FIL)	High (via storage deals)	Moderate	Long-term storage with guaranteed availability
Arweave	Permanent, one-time payment	Upfront fee (AR)	Permanent	Moderate	Immutable, critical records
Storj	Sharded, pay-per-use	Pay for storage/bandwidth	High (redundancy)	High	High-performance,

Solution	Storage Model	Cost	Persistence	Performance	Best Use Case
					frequent access

For a patient record management system, utilizing IPFS with a pinning service (e.g., Pinata) or Filecoin is typically the optimal initial choice, owing to its connection with blockchain ecosystems and their equilibrium of cost and data persistence. Arweave is optimal for immutable records, whereas Storj is appropriate for applications requiring rapid access.

4.6. Illustration of Integration: Filecoin

We will enhance the existing Python Flask backend to incorporate Filecoin with Web3.Storage[36], a Filecoin-based service that facilitates storage and retrieval. This substitutes the IPFS-specific code, while the blockchain interaction (Ethereum smart contract) stays intact.

1. Install Dependencies

Execute the command: pip install web3-storage cryptography, Flask, Web3 Register for a Web3.Storage account to obtain an API token: web3.storage.

2. Enhanced Flask Backend with Filecoin (Web3.Storage)

[36] https://storacha.network/

This code transmits encrypted medical records to Filecoin over Web3.Storage and records the CID on the blockchain.

```
from flask import Flask, request, jsonify
from web3 import Web3
from cryptography.fernet import Fernet
from web3storage import Web3Storage
import json
import os
app = Flask(__name__)
# Connect to Ethereum node (e.g., Ganache)
w3 = Web3(Web3.HTTPProvider('http://127.0.0.1:7545'))
w3.eth.default_account = w3.eth.accounts[0]
# Load smart contract
with open('PatientRecord.json') as f:
    contract_data = json.load(f)
contract_abi = contract_data['abi']
contract_address = '0xYourContractAddress'  # Replace with deployed contract address
contract = w3.eth.contract(address=contract_address, abi=contract_abi)
```

```
# Connect to Web3.Storage (Filecoin)

web3_storage = Web3Storage(api_token='YOUR_WEB3_STORAGE_API_TOKEN')
# Replace with your token

# Encryption setup

key = Fernet.generate_key()

cipher = Fernet(key)

@app.route('/register_patient', methods=['POST'])

def register_patient():

    data = request.json

    patient_id = data['patient_id']

    tx_hash = contract.functions.registerPatient(patient_id).transact()

    w3.eth.wait_for_transaction_receipt(tx_hash)

    return jsonify({"message": "Patient registered", "patient_id": patient_id})

@app.route('/add_record', methods=['POST'])

def add_record():

    data = request.json

    record_id = data['record_id']

    patient_id = data['patient_id']

    record_data = data['record_data']

    # Encrypt record

    encrypted_record = cipher.encrypt(record_data.encode())
```

```
    # Save encrypted record to a temporary file
    temp_file = f"{record_id}.bin"
    with open(temp_file, 'wb') as f:
        f.write(encrypted_record)
    # Upload to Web3.Storage (Filecoin)
    with open(temp_file, 'rb') as f:
        cid = web3_storage.upload(f)  # Returns CID
    # Clean up temporary file
    os.remove(temp_file)
    # Store metadata on-chain (CID as recordHash)
    tx_hash = contract.functions.addRecord(record_id, patient_id, cid).transact()
    w3.eth.wait_for_transaction_receipt(tx_hash)
    return jsonify({"message": "Record added", "record_id": record_id, "filecoin_cid": cid})
@app.route('/grant_access', methods=['POST'])
def grant_access():
    data = request.json
    record_id = data['record_id']
    authorized_address = data['authorized_address']
    tx_hash = contract.functions.grantAccess(record_id, authorized_address).transact()
```

```
    w3.eth.wait_for_transaction_receipt(tx_hash)
    return jsonify({"message": "Access granted"})
@app.route('/get_record/', methods=['GET'])
def get_record(record_id):
    try:
        # Query blockchain for record metadata
        record_id, filecoin_cid, authorized = contract.functions.getRecord(record_id).call()
        # Fetch encrypted record from Web3.Storage
        encrypted_record = web3_storage.get(filecoin_cid)  # Fetch file content
        # Decrypt record
        decrypted_record = cipher.decrypt(encrypted_record).decode()
        return jsonify({
            "record_id": record_id,
            "record_data": decrypted_record,
            "filecoin_cid": filecoin_cid,
            "authorized": authorized
        })
    except Exception as e:
        return jsonify({"error": str(e)}), 400

if __name__ == '__main__':
```

app.run(debug=True)

3. Operating the System with Filecoin: Configure Web3.Storage:

Establish an account at web3.storage.
Acquire an API token and modify the api_token in the code.
Implement Smart Contract:
Deploy the PatientRecord contract (same to the previous version) utilizing Remix or Truffle.
Revise the contract_address in the Python code.
Execute Flask API:
Execute python app.py
Testing Endpoints:
Register a patient: POST /register_patient with {"patient_id": "P001"}.
Insert a record: POST /add_record with {"record_id": "R001", "patient_id": "P001", "record_data": "Diagnosis: Influenza"}.
This transmits the encrypted data to Filecoin and registers the CID on the blockchain.
Authorize access: POST /grant_access with {"record_id": "R001", "authorized_address": "0xDoctorAddress"}.
Obtain record: GET /get_record/R001.
This obtains the CID from the blockchain, acquires the file from Filecoin, then decrypts it.

4.7. Integration Illustration: Arweave (Concise)

To utilize Arweave, employ the arweave Python module to upload encrypted records and save transaction IDs on the blockchain. Below is a segment for the add_record endpoint:
import Wallet, Transaction from arweave

Initialize Arweave wallet (needs AR tokens).

```
arweave_wallet = Wallet('path_to_your_arweave_keyfile.json')

@app.route('/add_record', methods=['POST'])

define add_record():

data equals request.json

record_id = data.get('record_id')

patient_id = data['patient_id']

record_data = data['record_data']


Encrypt the record

encrypted_record = cipher.encrypt(record_data.encode())


Upload to Arweave

tx = Transaction(arweave_wallet, data=encrypted_record)

tx.add_tag('Content-Type', 'application/octet-stream')

tx.sign()

transmit.send()

arweave_transaction_id = transaction.id


Store metadata on-chain using the transaction ID as the record hash.

transaction_hash = contract.functions.addRecord(record_identifier, patient_identifier, arweave_transaction_id).transact()
```

w3.eth.wait_for_transaction_receipt(transaction_hash)

return jsonify({"message": "Record successfully added", "record_id": record_id, "arweave_txid": arweave_txid})

Utilize the Arweave library to obtain the transaction data by its ID and subsequently decrypt it. Arweave necessitates a wallet funded with AR, and expenses are incurred in advance for permanent storage.

4.8. Essential Factors for Decentralized Storage

4.8.1. Financial Oversight:

IPFS: Self-hosting is free, whereas pinning services (e.g., Pinata) incur subscription fees.

Filecoin: Transaction-based, necessitating FIL tokens. Allocate funds for storage and retrieval.

Arweave: A singular upfront payment in AR tokens, increased for extensive datasets.

Storj: Utilizes a pay-per-use model, incurring expenses for storage and bandwidth.

Data Retention:

IPFS: Necessitates pinning to prevent data loss.

Filecoin: Storage agreements guarantee continuity for the duration of the contract.

Arweave: Inherently permanent, optimal for unalterable records.

Storj: Redundancy guarantees availability; nonetheless, continuous payments are required

4.8.2. Execution:

IPFS/Filecoin: Retrieval speed is moderate, enhanced with pinning or retrieval agreements.

Arweave exhibits reduced speed for substantial files owing to its blockweave architecture.

Storj: Accelerated performance attributed to sharding and global node dispersion.

4.8.3. Safety:

Consistently encrypt data on the client-side (e.g., AES-256) prior to uploading, given that these systems are public or semi-public.

Employ secure key management solutions (e.g., AWS KMS, HashiCorp Vault) for encryption keys.

Preserve access logs on the blockchain for verifiability.

4.8.4. Adherence:

Guarantee adherence to healthcare regulations (e.g., HIPAA, GDPR) by encrypting data and limiting access with blockchain smart contracts.

The persistence of Arweave may hinder the implementation of GDPR's "right to be forgotten."

4.8.5. Hybrid Methodology:

Integrate solutions (e.g., IPFS for ephemeral storage, Arweave for enduring records) to optimize cost and durability.

Utilize a centralized encrypted database for rapid access to commonly utilized records, supplemented by backups on decentralized storage.

4.9. Suggestions for Patient Record Administration

Preferred Option: Filecoin (via Web3.Storage) due to its equilibrium of expense, durability, and interoperability with IPFS. It guarantees sustained availability via incentive storage agreements.

Alternative Option: IPFS utilizing a pinning service (e.g., Pinata) for budget-conscious implementations, particularly in the development phase.

Niche Application: Arweave for essential, unchanging records (e.g., birth certificates, surgical histories) that must stay perpetually accessible.

High-Performance Requirements: Storj for systems necessitating rapid retrieval, such as real-time clinical data access.

Subsequent Actions

Private Networks: Establish private IPFS or Filecoin clusters for sensitive medical data, limited to approved nodes.

Cost Optimization: Assess storage and retrieval expenses, particularly for Filecoin and Storj, and implement caching for frequently requested data.

Interoperability: Integrate with FHIR APIs to guarantee interoperability with hospital systems, while keeping FHIR-compliant records on decentralized storage.

Integrating a database into a blockchain-based patient record management system

Integrating a database into a blockchain-based patient record management system is crucial for effective data management, particularly for managing metadata, user profiles, access logs, or frequently accessed data that does not require storage on the blockchain or decentralized storage solutions such as IPFS/Filecoin. A database can enhance blockchain and decentralized storage by delivering rapid query performance, structured

data management, and facilitating operational workflows, all while guaranteeing security and adherence to healthcare regulations (e.g., HIPAA, GDPR)[63].

We will elucidate the function of a database within the system, propose appropriate database alternatives, delineate their integration with the current blockchain and IPFS/Filecoin configuration, and provide updated Python code snippets to illustrate database integration utilizing PostgreSQL as a case study[64]. We will also examine hybrid methodologies that integrate centralized databases with decentralized storage solutions.

The Function of a Database within the System

In a blockchain-based patient record management system, the database functions as an off-chain operational layer to manage data that does not necessitate the immutability or decentralization of the blockchain, nor the extensive storage capabilities of IPFS/Filecoin. Its primary functions encompass:

Metadata Repository:

Maintain metadata regarding patient records (e.g., record IDs, patient IDs, IPFS/Filecoin CIDs, encryption keys, or access permissions) for expedited retrieval.

Store blockchain data in a cache to minimize on-chain query expenses and latency.

Administration of Users:

Administer user profiles (e.g., patients, physicians, administrators) containing information such as names, contact data, or public keys.

Manage authentication and role-based access control (RBAC) for system users.

Access Records:

Maintain comprehensive access logs (e.g., identity of the individual accessing a record, timestamp, and actions performed) for auditing purposes, in conjunction with blockchain-based audit trails.

Facilitate rapid retrieval of access history for compliance documentation.

Storage and Organization of Data:

Cache frequently accessed patient records or decrypted data, ensuring stringent access constraints, to enhance performance.

Catalog information for optimized search and retrieval.

Operational Information:

Preserve system setups, API keys, or ephemeral session data.

Facilitate workflows such as appointment booking or alerts that do not require blockchain immutability.

Hybrid Storage:

Serve as the principal repository for low-latency access to essential records, with redundancies on IPFS/Filecoin/Arweave.

Facilitate adherence to legislation mandating data destruction (e.g., GDPR) by maintaining changeable data off-chain.

Database Alternatives

The selection of a database is contingent upon the system's prerequisites for scalability, security, performance, and compliance. The following are appropriate alternatives for a patient record management system:

1. PostgreSQL (Relational Database Management System)

An open-source, SQL-compliant relational database characterized by comprehensive security features.

Principal Attributes:

Robust data consistency and adherence to ACID principles.

Facilitates encryption both at rest and in transit (e.g., using SSL/TLS).

Enhanced indexing and querying for metadata and log data.

Extensions such as pgcrypto for the encryption of sensitive data fields.

Application: Optimal for organized information, user administration, and access records.

Advantages:

Developed, extensively utilized, and complies with HIPAA when appropriately configured.

Superb assistance for intricate queries and joins.

Disadvantages:

Centralized, necessitating stringent security protocols.

Scaling necessitates meticulous design, such as sharding and replication.

2. MongoDB (NoSQL Database)

A document-oriented NoSQL database designed for flexible, semi-structured data.

Principal Attributes:

Schema-free architecture for managing various medical record formats.

Integrated encryption and role-based access management.

Horizontal scaling through sharding.

Application*:* Appropriate for the storage of FHIR-compliant JSON documents or dynamic metadata.

Advantages:

Adaptable schema for the progression of healthcare data.

Exhibits scalability for extensive datasets.

Disadvantages:

Inferior consistency relative to relational databases.

Demands meticulous indexing for optimal performance.

3. CockroachDB (Distributed SQL Database)

A distributed, cloud-native SQL database engineered for scalability and robustness.

Essential Attributes:

Distributed architecture for enhanced availability.

Robust consistency and SQL compatibility.

Integrated encryption and geographic segmentation.

***Application*:** Optimally suited for international healthcare systems requiring high availability and minimal latency access.

Advantages:

Scales horizontally with minimal configuration required.

Resistant to node failures.

Disadvantages:

More intricate configuration than PostgreSQL.

Increased operational expenses.

4. SQLite (Compact Relational Database)

Embedded, serverless SQL database designed for small-scale or edge implementations.

Principal Attributes:

Lightweight and readily deployable.

Facilitates encryption using extensions (e.g., SQLCipher).

Monolithic storage.

Application: Appropriate for prototype or edge devices in the healthcare sector (e.g., mobile applications).

Advantages:

Basic configuration for development.

Minimal resource prerequisites.

Disadvantages:

Inappropriate for high-concurrency or large-scale systems.

Restricted scalability.

5. DynamoDB (Managed NoSQL Database)

AWS-managed NoSQL database featuring serverless scalability.

Essential Attributes:

Completely administered, featuring automatic scalability.

Data encryption in a dormant state and meticulous access regulation.

Optimized low-latency performance for key-value searches.

Application: Appropriate for cloud-based systems exhibiting fluctuating workloads.

Advantages:

No maintenance required and exceptional scalability.

Seamlessly integrates with AWS security mechanisms, such as KMS.

Disadvantages:

Vendor dependency with AWS.

Increased expenses for extensive utilization.

4.9.1. Recommendation:

PostgreSQL is the optimal selection for the majority of patient record management systems owing to its maturity, HIPAA compliance, robust security features, and capability to support structured healthcare data. CockroachDB or DynamoDB may be favored for cloud-native or extremely scalable solutions. MongoDB is appropriate for adaptable, FHIR-oriented workflows.

4.10. Architecture for Database Integration

The database interfaces with the current blockchain and IPFS/Filecoin layers as outlined below:

Blockchain Layer:

Stores unalterable metadata (e.g., record ID, patient ID, IPFS/Filecoin CID, access rights) and audit trails through the smart contract.

Guarantees data integrity and decentralized access governance.

Decentralized Storage (IPFS/Filecoin):

Stores encrypted medical records (e.g., clinical reports, imaging files).

CIDs are recorded on the blockchain and may be cached in the database for expedited retrieval.

Database Layer:

Retains operating data:

Users: Profiles of patients and providers (e.g., identifiers, names, public keys).

Metadata Cache: Record identifiers, CIDs, and patient identifiers for expedited inquiries.

Access Logs: Comprehensive records of data access (e.g., timestamp, user, action).

Encryption Keys: Keys securely maintained for the decryption of records (e.g., utilizing pgcrypto).

Facilitates rapid searching and indexing for operational processes.

Synchronizes with the blockchain to maintain consistency (e.g., caching CIDs subsequent to blockchain transactions).

Application Layer:

The Flask API interfaces with the database for user administration, metadata inquiries, and logging activities.

Interrogates the blockchain for immutable data and utilizes IPFS/Filecoin for encrypted records.

Implements access control with blockchain smart contracts and database role-based access control (RBAC).

Safety:

Encrypt sensitive fields within the database (e.g., with pgcrypto in PostgreSQL).

Employ TLS for database connections and implement safe key management for encryption keys.

Conduct an audit of all database access through blockchain logs.

4.10.1. Revised Code Excerpts (PostgreSQL Integration)

I enhance the existing Flask-based Python backend by incorporating PostgreSQL for the storage of user profiles, metadata, and access logs. The blockchain and Filecoin (Web3.Storage) elements are unchanged; however, the database caches CIDs and manages operational data.

1. Install Dependencies

Install the following packages: psycopg2-binary, web3-storage, cryptography, flask, and web3 using pip.

Install and configure PostgreSQL:

Install PostgreSQL by adhering to the guidelines provided at postgresql.org.

Establish a database (e.g., patient_records).

Activate pgcrypto for encryption purposes:

INSTALL EXTENSION pgcrypto;

Two. PostgreSQL Database Schema

Establish tables for users, document information, and log access records:

CREATE TABLE users (

user_id SERIAL PRIMARY KEY,

patient_id VARCHAR(50) UNIQUE NOT NULL,

name VARCHAR(100);

public_key TEXT,

role VARCHAR(20) CONSTRAINT role_check CHECK (role IN ('patient', 'doctor', 'admin'))

created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP

);

CREATE TABLE record_metadata (

record_id VARCHAR(50) CONSTRAINT PRIMARY KEY,

patient_id VARCHAR(50) REFERENCES users(patient_id);

filecoin_cid TEXT NOT NULL,

encrypted_key BYTEA, -- Encrypted key for the decryption of records

created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP

);

CREATE TABLE access_logs (

log_id SERIAL PRIMARY KEY,

record_id VARCHAR(50) REFERENCES record_metadata(record_id);

user_id INT REFERENCES users(user_id);

action VARCHAR(50);

timestamp TIMESTAMP DEFAULT CURRENT_TIMESTAMP

);

3. Enhanced Flask Backend utilizing PostgreSQL

This code incorporates PostgreSQL for user administration, metadata caching, and access logging, while maintaining interfaces with blockchain and Filecoin.

import Flask from the flask module, along with request and jsonify

import Web3 from web3

import Fernet from cryptography.fernet

import Web3Storage from web3storage

utilize psycopg2

import json

import os

import RealDictCursor from psycopg2.extras

application = Flask(__name__)

Establish a connection to an Ethereum node (e.g., Ganache).

w3 = Web3(Web3.HTTPProvider('http://127.0.0.1:7545'))

w3.eth.default_account = w3.eth.accounts[0];

Load the smart contract.

open('PatientRecord.json') as f:

contract_data = json.load(file)

contract_abi = contract_data['abi']

contract_address = '0xYourContractAddress' # Substitute with the deployed contract address

contract = w3.eth.contract(address=contract_address, abi=contract_abi)

Establish a connection to Web3.Storage (Filecoin)

web3_storage = Web3Storage(api_token='YOUR_WEB3_STORAGE_API_TOKEN') # Substitute with your token

Establish a connection to PostgreSQL

```
db_conn = psycopg2.connect(

database_name='patient_records',

user = 'your_username',

password='your_password',

host = 'localhost',

port = '5432'


db_conn.configure_session(autocommit=True)

db_cursor = db_conn.cursor(cursor_factory=RealDictCursor)
```

Encryption Configuration

```
key = Fernet.generate_key()

cipher equals Fernet(key)


app.route('/register_patient', methods=['POST'])

define register_patient():

data equals request.json

patient_id = data['patient_id']

identifier = data['name']
```

public_key = data.retrieve('public_key')

Register on the blockchain

transaction_hash = contract.functions.registerPatient(patient_id).transact()

w3.eth.wait_for_transaction_receipt(transaction_hash)

Store in the database

db_cursor.execute(INSERT INTO users (patient_id, name, public_key, role)

VALUES (?, ?, ?, ?)

RETRIEVING user_id""",

(patient_id, name, public_key, 'patient')

user_id = db_cursor.fetchone()['user_id']

return jsonify({"message": "Patient successfully registered", "patient_id": patient_id, "user_id": user_id})

app.route('/add_record', methods=['POST'])

define add_record():

data equals request.json

record_id = data['record_id']

patient_id = data['patient_id']

record_data = data['record_data']

```
*Encrypt the record*

encrypted_record = cipher.encrypt(record_data.encode())

*Store the encrypted record in a temporary file.*

temp_file = f"{record_id}.bin"

Utilizing open(temp_file, 'wb') as f:

f.write(encrypted_record)

*Upload to Filecoin*

Utilizing open(temp_file, 'rb') as f:

cid = web3_storage.upload(file)

*Eliminate transient file*

os.remove(temporary_file)

*Store metadata on the blockchain.*

transaction_hash = contract.functions.addRecord(record_id, patient_id, cid).transact()

w3.eth.wait_for_transaction_receipt(transaction_hash)

*Store metadata in the database, encrypting the key with pgcrypto.*

db_cursor.execute("""

INSERT INTO record_metadata (record_id, patient_id, filecoin_cid, encrypted_key)
```

VALUES (%s, %s, %s, pgp_sym_encrypt(%s, %s))""",

(record_id, patient_id, cid, key.decode(), 'secure_key_password') # Substitute with a secure key password

Log activity

db_cursor.execute(INSERT INTO access_logs (record_id, user_id, action)

SELECT %s, user_id, %s FROM users WHERE patient_id = %s""",

(record_id, 'record_created', patient_id))

return jsonify({"message": "Record successfully added", "record_id": record_id, "filecoin_cid": cid})

app.route('/grant_access', methods=['POST'])

define grant_access():

data equals request.json

record_id = data['record_id']

authorized_address = data['authorized_address']

Authorize access on the blockchain

transaction_hash = contract.functions.grantAccess(record_id, authorized_address).transact()

w3.eth.wait_for_transaction_receipt(transaction_hash)

Record action in database

db_cursor.execute("""

INSERT INTO access_logs (record_id, user_id, action)

SELECT %s, user_id, %s FROM users WHERE public_key = %s""

(record_id, 'access_granted', permitted_address)

return jsonify({"message": "Access authorized"})

@app.route('/get_record/', methods=['GET'])

fun retrieve_record(record_id):

attempt:

Retrieve metadata from the database.

db_cursor.execute(SELECT filecoin_cid, pgp_sym_decrypt(encrypted_key, %s)

AS decryption_key

SELECT * FROM record_metadata WHERE record_id = %s""('your_key_password', record_id)

metadata = db_cursor.fetchone()

in the absence of metadata:

return jsonify({"error": "Record not located"}), 404

filecoin_cid = metadata['filecoin_cid']

decryption_key = metadata['decryption_key']

Authenticate blockchain authorization

record_id, cid, authorized = contract.functions.getRecord(record_id).execute()

if cid is not equal to filecoin_cid:

return jsonify({"error": "Metadata discrepancy"}), 400

Retrieve encrypted record from Filecoin

encrypted_record = web3_storage.retrieve(filecoin_cid)

Decrypt the record

record_cipher = Fernet(decryption_key)

decrypted_record = record_cipher.decrypt(encrypted_record).decode()

Access log

db_cursor.execute("""INSERT INTO access_logs (record_id, user_id, action)

SELECT %s, user_id, %s FROM users WHERE public_key = %s""",(record_id, 'record_accessed', w3.eth.default_account)

return jsonify({

"record_id": record_id,

"record_data": decrypted_record,

"filecoin_cid": filecoin_cid,

"authorized": sanctioned

})

except Exception as e:

return jsonify({"error": str(e)}), 400

if __name__ == '__main__':app.run(debug=True)

4.10.2. 4. Operating the System with PostgreSQL

Configure PostgreSQL:

Install PostgreSQL and establish the patient_records database.

Execute the aforementioned SQL schema to establish tables.

Revise the database connection parameters (your_username, your_password, your_key_password) within the code.

Establish Web3.Storage:

Acquire an API token from web3.storage and modify the code accordingly.

Implement Smart Contract:

Utilize Remix or Truffle to deploy the PatientRecord contract.

Revise the contract_address within the code.

Execute Flask API:

Execute python app.py

Testing Endpoints:

To register a patient, execute a POST request to /register_patient with the following payload: {"patient_id": "P001", "name": "John Doe", "public_key": "0xPatientAddress"}.

Submit a record: POST /add_record with {"record_id": "R001", "patient_id": "P001", "record_data": "Patient diagnosis: Flu"}.

Stores metadata in PostgreSQL, content identifier on blockchain, and encrypted records on Filecoin.

Authorize access: POST /grant_access with {"record_id": "R001", "authorized_address": "0xDoctorAddress"}.

Obtain record: GET /get_record/R001.

Interrogates PostgreSQL for metadata, utilizes blockchain for authorization, and employs Filecoin for record-keeping.

4.10.3. Essential Factors for Database Integration

Safety:

Utilize pgcrypto or a comparable tool to encrypt sensitive fields, such as encryption keys.

Implement TLS for database connections and limit access to permitted IP addresses.

Establish Role-Based Access Control (RBAC) within the database and synchronize it with blockchain access controls.

Utilize a secure key management system (e.g., AWS KMS) for the storage of encryption keys in a production environment.

Uniformity:

Verify that database metadata (e.g., CIDs) corresponds with blockchain data by synchronizing following each blockchain transaction.

Utilize database triggers or background processes to identify and rectify discrepancies.

Performance:

Index commonly queried fields (e.g., record_id, patient_id) for expedited retrieval.

Store decrypted records in memory (e.g., Redis) for high-traffic systems, implementing stringent expiration controls.

Scalability:

Implement database replication, such as PostgreSQL streaming replication, to ensure high availability.

For global systems, consider utilizing distributed databases such as CockroachDB to minimize latency.

Adherence:

Guarantee HIPAA/GDPR compliance with the encryption of data both at rest and in transit.

Record all access in the database and blockchain for audit purposes.

Facilitate data erasure demands (e.g., GDPR's "right to be forgotten") by storing modifiable data in the database rather than on immutable blockchain/Arweave.

Hybrid Storage:

Preserve essential, frequently accessed records in the database for minimal latency access.

Ensure all records are backed up to IPFS/Filecoin for redundancy and decentralization.

Utilize Arweave for enduring, immutable documentation (e.g., birth certificates).

Advantages of Database Integration

Efficiency: Rapid retrieval of metadata and logs in comparison to blockchain or IPFS/Filecoin.

Flexibility: Accommodates intricate queries, user administration, and operational processes.

Compliance: Facilitates changeable data storage to meet regulatory mandates (e.g., data deletion).

Cost Efficiency: Minimizes blockchain queries using off-chain metadata caching.

Auditability: Comprehensive access logs within the database enhance blockchain audit trails.

Possible Improvements

Distributed Database: Substitute PostgreSQL with CockroachDB to achieve worldwide scalability and resilience.

FHIR Integration: Store FHIR-compliant JSON records in MongoDB or PostgreSQL's JSONB fields for interoperability.

Implement a caching layer utilizing Redis to store decrypted records or frequently requested metadata.

Backup Strategy:

Regularly archive database contents to Filecoin or Arweave for redundancy.

This integration offers a resilient, scalable, and compliant solution that amalgamates blockchain, decentralized storage, and a database.

Establishing a distributed database for a blockchain-based patient record management system improves scalability, resilience, and low-latency access across geographically scattered nodes, rendering it optimal for global healthcare systems. A distributed database guarantees high availability, fault tolerance, and consistent data access, while enhancing blockchain technology (for immutable metadata and access control) and decentralized storage solutions (e.g., Filecoin for encrypted medical records). I will elucidate the configuration procedure with CockroachDB, a distributed SQL database that provides robust consistency, scalability, and compatibility with PostgreSQL clients. I will combine it with the current Ethereum blockchain and Filecoin (Web3.Storage) configuration, supply Python code samples, and address essential considerations.

4.10.4. What are the Advantages of Utilizing a Distributed Database?

A distributed database such as CockroachDB is engineered to accommodate the requirements of a patient record management system by:

Scalability: Achieve horizontal scaling by incorporating additional nodes to accommodate heightened demand.

High Availability: Duplicate data across nodes to provide access despite potential node failures.

Geo-Distribution: Position nodes in various regions to ensure low-latency access (e.g., for global hospitals).

Robust Consistency: Safeguard data integrity for essential healthcare information (e.g., patient metadata, access logs).

SQL Compatibility: Facilitate intricate queries and interaction with current tools over the PostgreSQL wire protocol.

Ensure encryption and audits are activated for HIPAA/GDPR compliance.

CockroachDB is especially appropriate because to its distributed architecture, tolerance to node failures, and capacity to manage healthcare workloads with robust consistency.

Architecture of Distributed Databases

The distributed database interfaces with the current system in the following manner:

BLOCKCHAIN LAYER:

Stores unalterable metadata (e.g., record ID, patient ID, Filecoin CID, access rights) using the Ethereum smart contract.

Implements decentralized access control and audit capabilities.

Decentralized Storage (Filecoin):

Stores encrypted patient records, including medical reports and imaging files.

CIDs are preserved on the blockchain and kept in the distributed database cache.

Distributed Database (CockroachDB):

Objective: Oversees operational data, encompassing:

Users: Profiles of patients and providers (e.g., identifiers, names, public keys, roles).

Metadata Cache: Record Identifiers, Patient Identifiers, Filecoin Content Identifiers, and Encrypted Keys.

Access Logs: Comprehensive records of data access for auditing purposes.

Data is replicated among various nodes (e.g., in distinct regions) to ensure high availability and minimal latency.

Consistency: Guarantees robust consistency for metadata and logs, synchronizing with blockchain data.

APPLICATION LAYER:

The Flask API interfaces with CockroachDB for user administration, metadata inquiries, and logging activities.

Interrogates the blockchain for immutable information and Filecoin for encrypted documentation.

Implements access control with blockchain smart contracts and database role-based access control (RBAC).

SAFETY:

Utilize CockroachDB's encryption capabilities to secure sensitive information, such as encryption keys.

Employ TLS for database connections and implement secure key management.

Record all access on the blockchain and in CockroachDB for auditing purposes.

Procedure for Configuring CockroachDB

This is a comprehensive guide for establishing a CockroachDB cluster for the patient record management system.

1. Install CockroachDB.

Download and install CockroachDB by adhering to the instructions provided at cockroachlabs.com.

Alternatively, choose a managed service such as CockroachDB Cloud for simplified installation and upkeep.

2. Initiate a CockroachDB Cluster

For a multi-node cluster (e.g., three nodes for fault tolerance), execute the following on distinct machines or containers:

Node 1 (located at node1.silvana1.com):

initiate cockroach

--unsecured \

--store=node1

--listen-addr=node1.silvana1.com:26257

--http-addr=node1.silvana1.com:8080

--
join=node1.silvana1.com:26257,node2.silvana1.com:26257,node3.silvana1.com:26257

Node 2 (located at node2.silvana1.com):

initiate cockroach

--unconfident

--store=node2

--listen-addr=node2.silvana1.com:26257

--http-addr=node2.silvana1.com:8080

--
join=node1.silvana1.com:26257,node2.silvana1.com:26257,node3.silvana1.com:26257

Node 3 (located at node3.silvana1.com):

initiate cockroach

--unsecured \

--store=node3

--listen-addr=node3.silvana1.com:26257

--http-addr=node3.silvana1.com:8080

--
join=node1.silvana1.com:26257,node2.silvana1.com:26257,node3.silvana1.com:26257

Initiate the Cluster (execute on any node):

cockroach initialize --insecure --host=node1.silvana1.com:26257

Observations:

Substitute --insecure with certificate-based authentication for production (see to CockroachDB documentation for SSL/TLS configuration).

Utilize --locality flags to designate regions (e.g., --locality=region=us-east) for geographical distribution.

To conduct testing, initiate several nodes locally utilizing distinct ports (e.g., 26257, 26258, 26259).

3.Establish Database and Schema

Establish a connection to the cluster via the CockroachDB SQL client:

cockroach sql --insecure --host=node1.silvana1.com:26257

Establish the database and its corresponding tables:

```
ESTABLISH DATABASE patient_records;

CONFIGURE DATABASE = patient_records;

CREATE TABLE users (

user_id SERIAL PRIMARY KEY,

patient_id STRING UNIQUE NOT NULL,

name STRING,

public_key VARCHAR,

role STRING CHECK (role IN ('patient', 'doctor', 'administrator'))

created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP

);


CREATE TABLE record_metadata (

record_id STRING PRIMARY KEY,

patient_id STRING REFERENCES users(patient_id);

filecoin_cid STRING NOT NULL,

encrypted_key BYTES, -- Encrypted key for the decoding of records

created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP

);
```

```
CREATE TABLE access_logs (
log_id SERIAL PRIMARY KEY,
record_id STRING REFERENCES record_metadata(record_id);
user_id INT64 REFERENCES users(user_id);
action STRING,
timestamp TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

Activate encryption for sensitive fields (CockroachDB offers column-level encryption).

Implement application-level encryption for encrypted_key (managed in Python)

Performance Indices:

```
CREATE INDEX ON record_metadata (patient_id);
CREATE INDEX ON access_logs (record_id, timestamp);
```

Four. Configure Geo-Partitioning (Optional)

Partition data by area in global systems to minimize latency.

```
ALTER TABLE record_metadata PARTITION BY LIST (patient_id);
PARTITION us_values VALUES IN ('P001', 'P002') WITH (locality = 'region=us-east'),
PARTITION eu_values VALUES IN ('P003', 'P004') WITH (locality = 'region=eu-west')
);
```

Allocate nodes to regions utilizing --locality at the initiation of node startup.

Revised Code Excerpts (CockroachDB Integration)

I enhance the prior Flask-based Python backend to utilize CockroachDB in place of PostgreSQL, incorporating integration with the Ethereum blockchain and Filecoin (Web3.Storage). The PostgreSQL-compatible driver of CockroachDB (psycopg2) necessitates minimum code modifications.

1. Install Dependencies

Install the following packages: psycopg2-binary, web3-storage, cryptography, flask, and web3 using pip.

Verify that CockroachDB is operational and reachable.

2. Enhanced Flask Backend utilizing CockroachDB

This code employs CockroachDB for user administration, metadata caching, and access logging, while preserving interactions with blockchain and Filecoin.

import Flask from the flask module, along with request and jsonify

import Web3 from web3

import Fernet from cryptography.fernet

import Web3Storage from web3storage

utilize psycopg2

import json

import os

import RealDictCursor from psycopg2.extras

import hashes from cryptography.hazmat.primitives

import PBKDF2HMAC from cryptography.hazmat.primitives.kdf.pbkdf2

application = Flask(__name__)

Establish a connection to an Ethereum node (e.g., Ganache).

w3 = Web3(Web3.HTTPProvider('http://127.0.0.1:7545'))

w3.eth.default_account = w3.eth.accounts[0];

Load the smart contract.

open('PatientRecord.json') as f:

contract_data = json.load(file)

contract_abi = contract_data['abi']

contract_address = '0xYourContractAddress' # Substitute with the deployed contract address

contract = w3.eth.contract(address=contract_address, abi=contract_abi)

Establish a connection to Web3.Storage (Filecoin)

web3_storage = Web3Storage(api_token='YOUR_WEB3_STORAGE_API_TOKEN') # Substitute with your token

Establish a connection to CockroachDB

db_conn = psycopg2.connect(

database_name='patient_records',

user = 'your_username',

password='your_password',

host='node1.silvana1.com',

Alternatively, use localhost for testing

port = '26257',sslmode='disable'

Utilize 'require' with SSL in a production environment

db_conn.configure_session(autocommit=True)

db_cursor = db_conn.cursor(cursor_factory=RealDictCursor)

Encryption Configuration

key = Fernet.generate_key()

cipher = Fernet(key)

Key encryption for database storage with PBKDF2 for key derivation.

def encrypt_key(key, password):

kdf = PBKDF2HMAC(

algorithm = hashes.SHA256(),

length equals 32,

salt = b'salt_', # Employ a secure random salt in production

iterations equals 100,000,

key_der = kdf.derive(password.encode())

f = Fernet(Fernet.generate_key().decode()) # Simplified;

employ appropriate key derivation

return f.encrypt(key)

```
def decrypt_key(encrypted_key, password):

kdf = PBKDF2HMAC(

algorithm = hashes.SHA256(),

length equals 32.

salt = b'salt_', # Corresponds to the salt utilized in encryption

iterations = 100,000;

key_der = kdf.derive(password.encode())

f = Fernet(Fernet.generate_key().decode()) # Simplified; employ appropriate key derivation

return f.decrypt(encrypted_key)

app.route('/register_patient', methods=['POST'])

define register_patient():

data equals request.json

patient_id = data['patient_id']

identifier = data['name']

public_key = data.retrieve('public_key')
```

Register on the blockchain

```
transaction_hash = contract.functions.registerPatient(patient_id).transact()

w3.eth.wait_for_transaction_receipt(transaction_hash)
```

Store in CockroachDB

db_cursor.execute(""" INSERT INTO users (patient_id, name, public_key, role)

VALUES (?, ?, ?, ?)

RETURNING user identifier """,(patient_id, name, public_key, 'patient')

user_id = db_cursor.fetchone()['user_id']

return jsonify({"message": "Patient successfully registered", "patient_id": patient_id, "user_id": user_id})

@app.route('/add_record', methods=['POST'])

define add_record():

data equals request.json

record_id = data['record_id']

patient_id = data['patient_id']

record_data = data['record_data']

Encrypt the record

encrypted_record = cipher.encrypt(record_data.encode())

Store the encrypted record in a temporary file.

temporary_file = f"{record_id}.bin"

Utilizing the 'with' statement, open the temporary file in write-binary mode as 'f':

f.write(encrypted_record)

Upload to Filecoin

Utilizing open(temp_file, 'rb') as f:

cid = web3_storage.upload(file)

Eliminate transient file

os.remove(temporary_file)

Store metadata on the blockchain.

transaction_hash = contract.functions.addRecord(record_identifier, patient_identifier, content_identifier).transact()

w3.eth.wait_for_transaction_receipt(transaction_hash)

Encrypt the key for database storage.

encrypted_key = encrypt_key(key, 'secure_password') # Substitute with a robust password

Store metadata in CockroachDB.

db_cursor.execute(INSERT INTO record_metadata (record_id, patient_id, filecoin_cid, encrypted_key)

VALUES (?, ?, ?, ?)""(record_id, patient_id, cid, encrypted_key)

Log activity

db_cursor.execute(

INSERT INTO access_logs (record_id, user_id, action)

SELECT %s, user_id, %s FROM users WHERE patient_id = %s

"""

(record_id, 'record_created', patient_id)

return jsonify({"message": "Record successfully added", "record_id": record_id, "filecoin_cid": cid})

app.route('/grant_access', methods=['POST'])

def grant_access():

data equals request.json

record_id = data['record_id']

authorized_address = data['authorized_address']

Authorize access on the blockchain

transaction_hash = contract.functions.grantAccess(record_id, authorized_address).transact()

w3.eth.wait_for_transaction_receipt(transaction_hash)

Log activity in CockroachDB

db_cursor.execute("""INSERT INTO access_logs (record_id, user_id, action)

SELECT %s, user_id, %s FROM users WHERE public_key = %s""",(record_id, 'access_granted', authorized_address)

return jsonify({"message": "Access permitted"})

@app.route('/get_record/', methods=['GET'])

define get_record(record_id):

attempt:

Query CockroachDB for metadata.

db_cursor.execute("""SELECT filecoin_cid, encrypted_key

SELECT * FROM record_metadata WHERE record_id = %s

""",(record_id,))

metadata = db_cursor.fetchone()

in the absence of metadata:

return jsonify({"error": "Record not located"}), 404

filecoin_cid = metadata['filecoin_cid']

encrypted_key = metadata['encrypted_key']

Decrypt the key

decryption_key = decrypt_key(encrypted_key, 'secure_password') # Substitute with a safe password

Authenticate blockchain authorization

record_id, cid, authorized = contract.functions.getRecord(record_id).execute()

if cid is not equal to filecoin_cid:

return jsonify({"error": "Metadata discrepancy"}), 400

Retrieve encrypted record from Filecoin

encrypted_record = web3_storage.retrieve(filecoin_cid)

Decrypt the record

record_cipher = Fernet(decryption_key)

decrypted_record = record_cipher.decrypt(encrypted_record).decode()

Access log

db_cursor.execute("""INSERT INTO access_logs (record_id, user_id, action)

SELECT %s, user_id, %s FROM users WHERE public_key = %s""",

(record_id, 'record_accessed', w3.eth.default_account))

return jsonify({

"record_id": record_id,

"record_data": decrypted_record,

"filecoin_cid": filecoin_cid,

"authorized": sanctioned

})

except Exception as e:

return jsonify({"error": str(e)}), 400

if __name__ == '__main__':

app.run(debug=True)

3. Operating the System with CockroachDB

Establish CockroachDB Cluster:

Adhere to the aforementioned steps to initiate a 3-node cluster (or utilize CockroachDB Cloud).

Establish the patient_records database and its corresponding tables utilizing the SQL schema.

Establish Web3.Storage*:*

Acquire an API token from web3.storage and modify the code accordingly.

Implement Smart Contract:

Utilize Remix or Truffle to deploy the PatientRecord contract.

Revise the contract_address within the code.

Execute Flask API:

Execute python app.py

Testing Endpoints:

To register a patient, execute a POST request to /register_patient with the following payload: {"patient_id": "P001", "name": "John Doe", "public_key": "0xPatientAddress"}.

Submit a record*:* POST /add_record with {"record_id": "R001", "patient_id": "P001", "record_data": "Patient diagnosis: Influenza"}.

Stores metadata in CockroachDB, content identifier on the blockchain, and an encrypted record on Filecoin.

Authorize access*:* POST /grant_access with {"record_id": "R001", "authorized_address": "0xDoctorAddress"}.

Obtain record: GET /get_record/R001.

Interrogates CockroachDB for metadata, utilizes blockchain for authorization, and employs Filecoin for record-keeping.

Essential Factors for CockroachDB Configuration

Safety:

Activate SSL/TLS for CockroachDB connections by substituting sslmode='disable' with sslmode='require'.

Utilize application-level encryption (as demonstrated) or CockroachDB's encryption-at-rest to secure sensitive fields (e.g., encrypted_key).

Implement Role-Based Access Control (RBAC) in CockroachDB and synchronize it with blockchain access controls.

Utilize a secure key management system (e.g., AWS KMS) for the storage of encryption keys in production environments.

Uniformity:

CockroachDB inherently offers robust consistency, guaranteeing that metadata aligns with blockchain data.

Synchronize database metadata with the blockchain subsequent to each transaction (as demonstrated in the code).

Utilize CockroachDB's change data capture (CDC) to oversee and rectify inconsistencies.

Scalability:

Incorporate nodes into the cluster to accommodate heightened demand (e.g., cockroach start with --join).

Implement geo-partitioning to position data nearer to users (e.g., regions in the US and EU).

Assess cluster health with CockroachDB's administrative interface (http://node1.silvana1.com:8080).

Efficiency:

Index commonly queried fields (e.g., record_id, patient_id) for expedited retrieval.

Store cache metadata in memory (e.g., Redis) for high-traffic systems, implementing stringent expiration controls.

Enhance SQL queries to reduce latency (e.g., eliminate superfluous joins).

Enhanced Availability:

Deploy a minimum of three nodes to withstand the failure of one node (CockroachDB employs Raft consensus).

Duplicate data across regions for catastrophe recovery (e.g., us-east, us-west, eu-west).

Utilize CockroachDB's automated rebalancing to achieve equitable load distribution.

Adherence:

Guarantee HIPAA/GDPR compliance with the encryption of data both at rest and in transit.

Document all access in CockroachDB and blockchain for audit purposes (as illustrated).

Facilitate GDPR's "right to be forgotten" by storing modifiable data in CockroachDB rather than on the immutable blockchain or Arweave.

Financial Oversight:

CockroachDB Cloud streamlines management; nonetheless, expenses are determined by the number of nodes and storage utilized.

Self-hosted clusters are economical yet necessitate infrastructure upkeep.

Enhance storage efficiency by retaining solely operational data in CockroachDB and substantial records in Filecoin.

Advantages of CockroachDB in This System

- Global Scalability: Manages extensive, geographically dispersed healthcare systems.

- Resilience: Endures node or regional failures without data loss.
- Low Latency: Geo-partitioning guarantees rapid access for users globally.
- SQL Compatibility: Utilizes established PostgreSQL tools and proficiency.
- Compliance: Facilitates encryption and auditing in accordance with healthcare legislation.

Possible Improvements

Multi-Region Deployment: Implement nodes across many cloud providers (e.g., AWS, GCP, Azure) to ensure redundancy.

Change Data Capture: Employ CockroachDB's CDC to transmit metadata alterations to a monitoring system for instantaneous analytics.

FHIR Integration: Preserve FHIR-compliant JSON records within CockroachDB's JSONB fields for enhanced compatibility.

Implement a caching layer by incorporating Redis to cache decrypted records or metadata, synchronized with CockroachDB.

Integrate CockroachDB with Prometheus/Grafana for the purpose of monitoring cluster performance.

Alternative Distributed Database Systems

If CockroachDB does not meet the requirements, consider:

YugabyteDB:

Distributed SQL database exhibiting interoperability with PostgreSQL.

Robust consistency and geographical distribution.

Open-source, emphasizing high-performance tasks.

Use case: Comparable to CockroachDB, although potentially provides superior performance for write-intensive applications.

Spanner (Google Cloud):

Administered a globally distributed SQL database ensuring robust consistency.

Optimally suited for enterprise-level healthcare systems.

Disadvantages: Vendor lock-in and elevated expenses.

DynamoDB (Amazon Web Services):

Administered NoSQL database utilizing global tables for dissemination.

Appropriate for key-value information and log entries.

Disadvantages: Restricted query flexibility in comparison to SQL.

Recommendation: Opt for CockroachDB due to its equilibrium of SQL compatibility, robust consistency, and open-source accessibility. Utilize YugabyteDB for write-intensive systems or DynamoDB for serverless, NoSQL-oriented implementations.

Executing the System

The supplied code smoothly integrates CockroachDB with the current blockchain and Filecoin configuration. To enhance system scalability:

Increase the number of CockroachDB nodes as necessary (e.g., cockroach start --join).

Establish geo-partitioning to facilitate low-latency access in designated locations.

Track blockchain gas fees and Filecoin storage/retrieval expenses to enhance cost efficiency.

Table 6. Summary of Additions

Feature	Tool / Concept
Smart contracts	Custom Python logic
Data encryption	AES (with PyCryptodome)
File handling	IPFS (off-chain storage)

GitHub project architecture for a blockchain-based patient record management system utilizing Python, Flask, encryption, and IPFS.

patient-chain/

├── app/

│ ├── __init__.py

│ ├── blockchain.py

│ ├── encryption.py

│ ├── ipfs_handler.py

│ ├── smart_contract.py

│ └── routes.py

├── static/

│ └── uploads/ # Store temp encrypted files before IPFS

├── templates/

│ └── index.html # Optional: Web UI

├── run.py

├── requirements.txt

└── README.md

These are some of the security measures at the database level. Maintaining patient data secure and adhering to security practices at the database infrastructure level is essential. At the physical infrastructure level, the security of the hospital IT system includes measures to protect the hardware and the physical environment where the equipment and servers are stored and operated.

4.11. The optimal database for medical information

Specific requirements, such as scalability, performance, security, compliance (for example, HIPAA or GDPR), interoperability (for example, FHIR), and integration with blockchain and decentralized storage (for example, Filecoin), [65]are taken into consideration when selecting the most suitable database for a blockchain-based patient record management system in the healthcare industry. I have analyze the top database options, with a particular emphasis on distributed and traditional databases, based on the requirements that are special to the healthcare industry, analyze their applicability, and then make a recommendation for the most suitable solution for the system.

Table 7. Comparison of Databases for Healthcare

Database	**Type**	**Security**	**Scalability**	**Performance**	**Consistency**	**Interoperability**	**Availability**	**Cost**	**Best Use Case**
CockroachDB	Distributed SQL	HIPAA-compliant, encryption, RBAC	Horizontal (nodes)	Fast with indexing	Strong	FHIR JSONB, SQL	High (multi-region)	Moderate (self-hosted or Cloud)	Global, compliant systems
PostgreSQL	Relational SQL	HIPAA-compliant, pgcrypto, TLS	Vertical, limited horizontal	Fast for structured data	Strong	FHIR JSONB, SQL	Moderate (replication)	Low (open-source)	Regional, cost-sensitive systems
YugabyteDB	Distributed SQL	HIPAA-compliant, encryption	Horizontal (sharding)	High for writes	Strong	FHIR JSON, SQL/YCQL	High (multi-region)	Low (open-source)	Write-heavy, global systems

Database	Type	Security	Scalability	Performance	Consistency	Interoperability	Availability	Cost	Best Use Case
MongoDB	NoSQL Document	HIPAA-compliant (Atlas)	Horizontal (sharding)	Fast for JSON	Tunable	FHIR JSON	High (replication)	Moderate (Atlas)	FHIR-focused, flexible schema
DynamoDB	Managed NoSQL	HIPAA-compliant, AWS KMS	Serverless	Fast for key-value	Strong/Eventual	FHIR JSON, limited	High (global tables)	High (AWS)	Cloud-native, low-maintenance
Spanner	Distributed SQL	HIPAA-compliant, encryption	Horizontal (unlimited)	Fast with indexing	Strong	FHIR JSON, SQL	High (global)	High (GCP)	Enterprise, global systems

Recommendation: CockroachDB

CockroachDB is the optimal database for a blockchain-based patient record management system in healthcare, considering the necessities for a distributed architecture and compatibility with Ethereum and Filecoin.

Table 8. Comparison: Blockchain vs. Traditional Systems

Feature	Blockchain	Traditional(e.g.,Centralized Database)
Security	Decentralized, immutable, cryptographic	Centralized, vulnerable to breaches

Feature	Blockchain	Traditional(e.g.,Centralized Database)
Privacy	Patient-controlled access via smart contracts	Admin-controlled, less patient agency
Interoperability	Unified ledger for cross-system access	Siloed systems, complex integration
Auditability	Immutable audit trails	Mutable logs, risk of tampering
Trust	Decentralized trust via consensus	Relies on trusted intermediaries
Resilience	Distributed, fault-tolerant	Single point of failure
Cost	Higher (gas fees, setup)	Lower (standard infrastructure)
Performance	Slower for transactions	Faster for queries

In conclusion, blockchain demonstrates superiority in security, privacy, interoperability, and trust, rendering it well-suited for the delicate and collaborative aspects of healthcare, although its elevated price and complexity.

5. THE EXPERIMENT:

The experimet has taken place in Albania. One of the users is Rudens Qose that is my brother who alowed me to put into motion my thesis. The place is FiBank in Albania.

The sistem of FiBank is protected by several layers like:

- SIEM(ManageEngine)
- ADaudit (ManageEngine)

- ADManager(ManageEngine)
- Data Security(ManageEngine)
- Email Exchange monitoring (ManageEngine)
- DLP(Symantec data loss prevention)
- Sophos antivirus (XDR/MDR)
- CloudFlare (WAF, DNS)
- Vsphere
- Veeam
- Digicert (digital certificates)
- CA (certa) (microsoft certificate authority)
- Next gen firewall (nexus cisco) (fmc)
- Sophos firewall (sg firewall)
- Sophos email security gateway.

All this programs where conected to secure the Bank data and systems. As you can see in the photos below for one month there have been 26 Malicus emails, 25 viruses, 6 unscannable viruses 105 malicus url, 1 impersonation, 676 spam,1688 Bulk, 380 authenification faliure, 17 data control so in total 8646 potenial threads identified.

I have taken just one moth in consideration but I have seen the system for 1 year in this timet he bank has had many threads and many problems. This is a regular month so I did not want to take into consideration a month with too many threads since the difference in the system when implementin the new data protection it will make a difference.

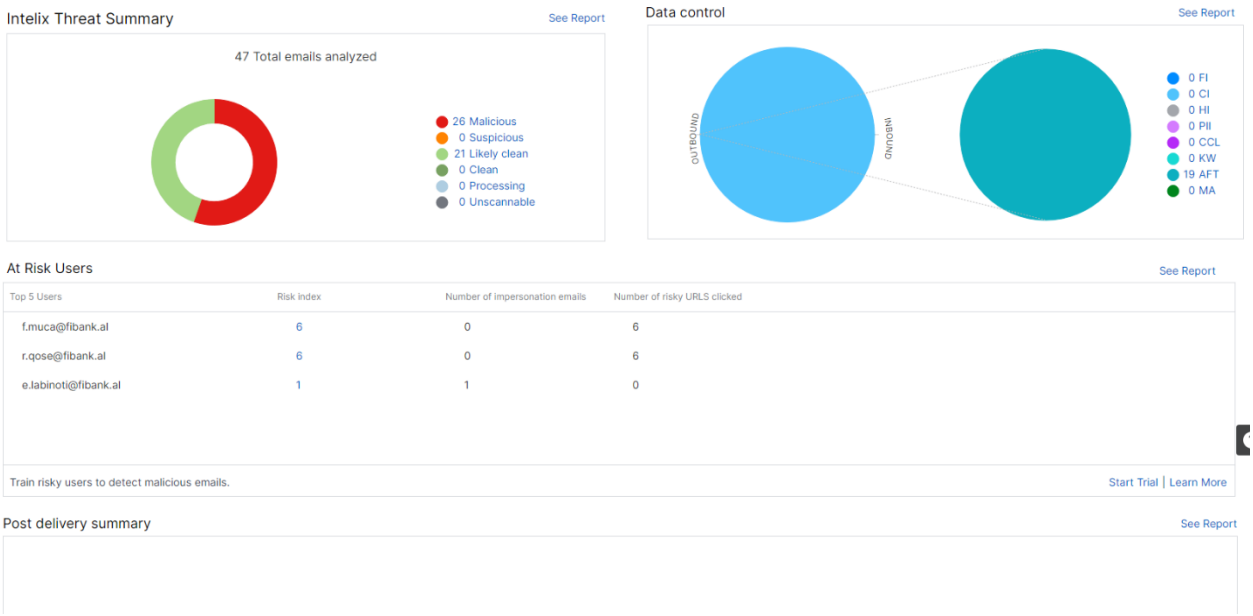


Figure 30. Intelix Threat Summary 2023[37]

[37] https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/LogsReports/Reports/IntelixThreatSummary/index.html

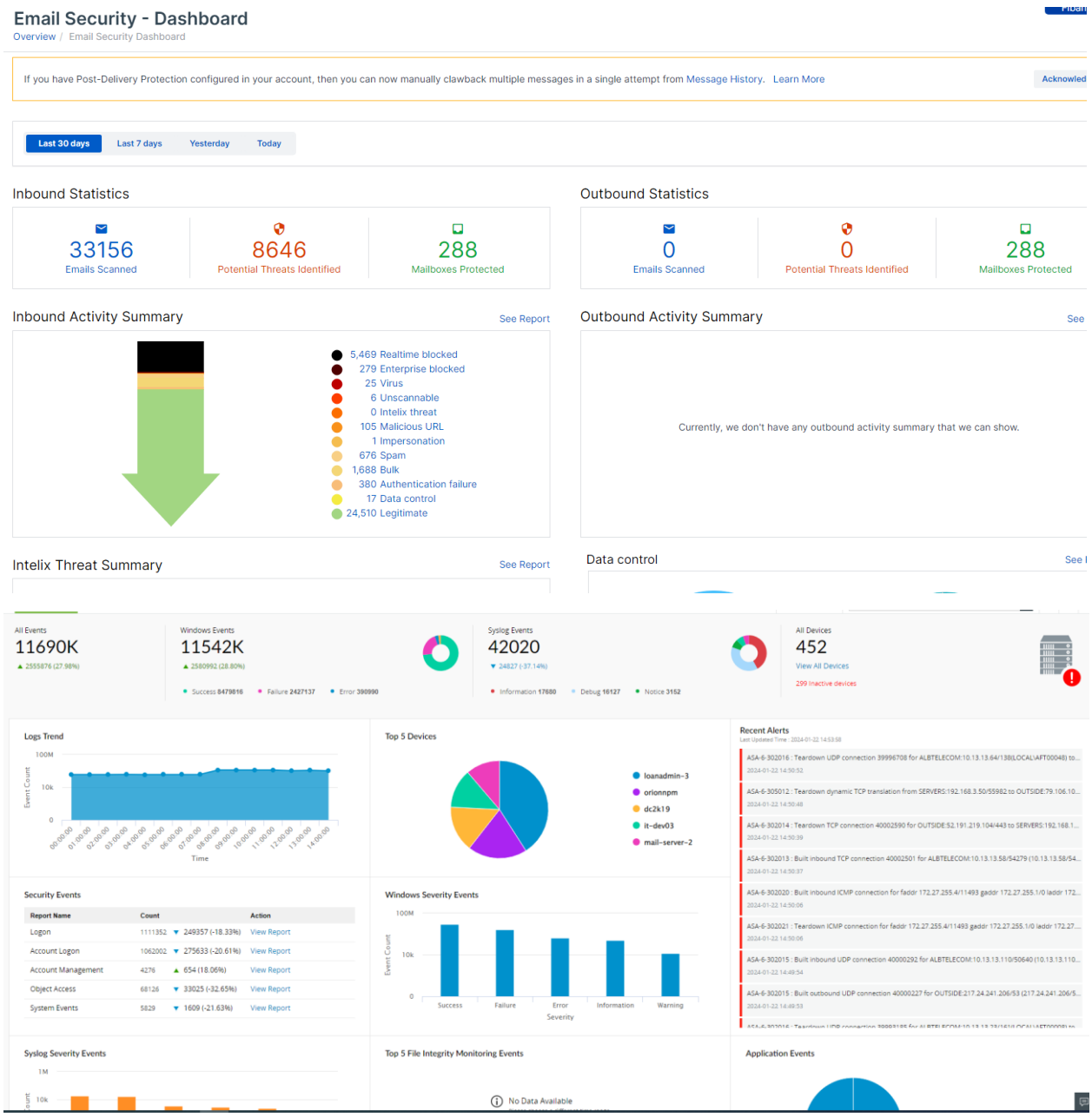


Figure 31. Email Security Dashboard 2023[38]

[38] https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EmailSecurity/EmailDashboard/index.html

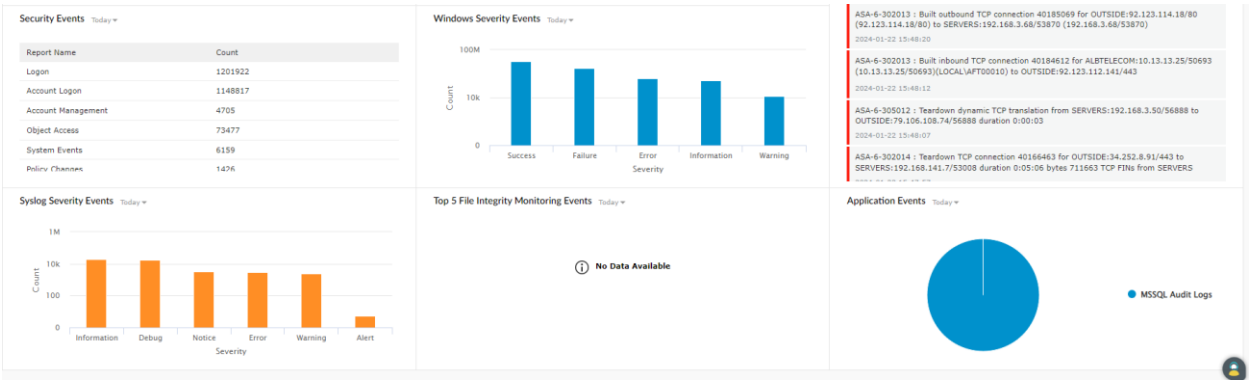


Figure 32. Windows Security Events 2023[39]

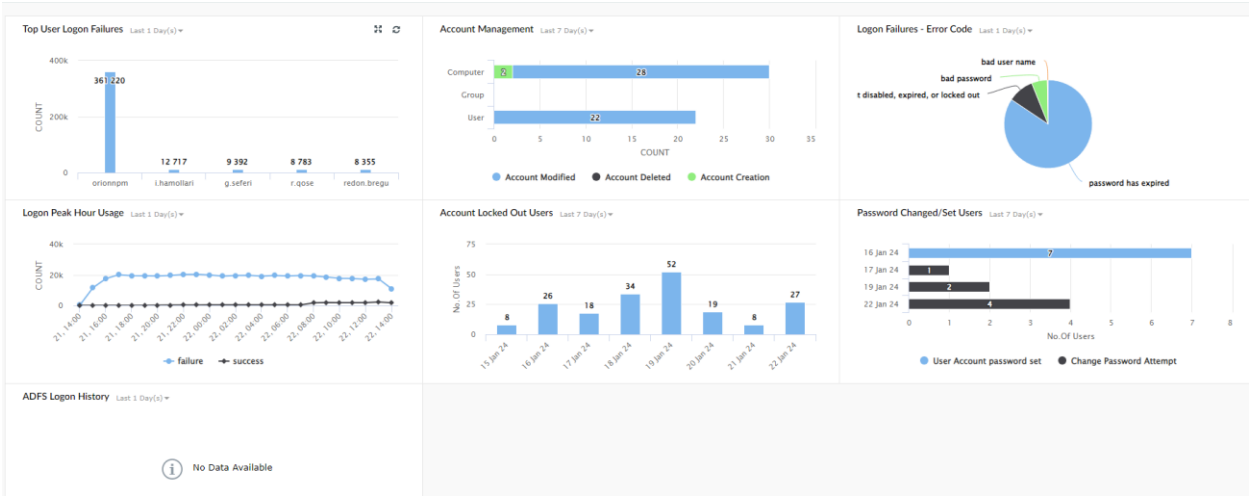


Figure 33.Top Users Filatures 2023[40]

[39] https://support.sophos.com/support/s/article/KBA-000009156?language=en_US

[40] https://support.sophos.com/support/s/article/KBA-000009156?language=en_US

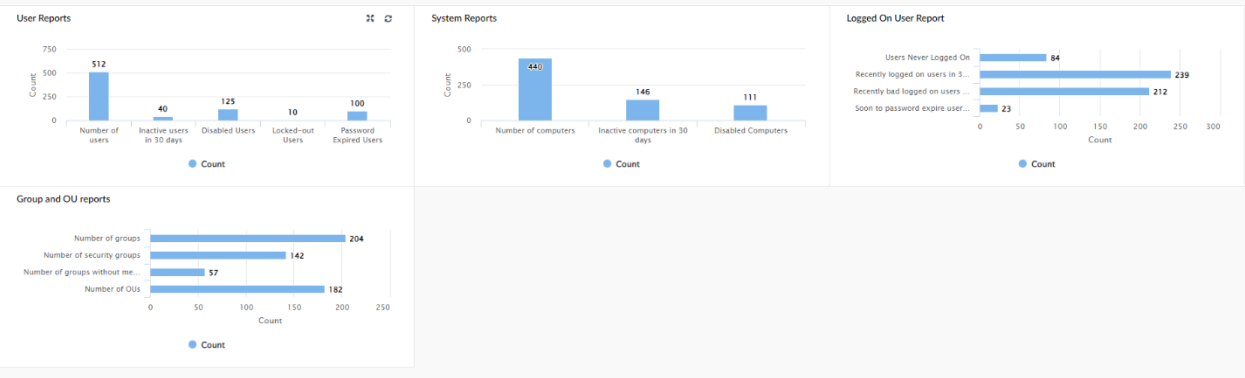


Figure 34. Rapports 2023[41]

Following the implementation of the new program, we observe an enhancement in security despite the presence of numerous threats. The DoS assault was more challenging to control with other systems; however, after we included the data into the chain, it became easier to safeguard it.

Only individuals with the authority to input additional data into the chain are those who establish new bank accounts; their information is recorded in the chain and verified by the employee upon completion of the process. Subsequent to confirmation, each transaction executed by the user is recorded in the chain and validated by the bank.

The cybersecurity team oversees the blocks, with each deal executed by the bank recorded in a separate block on the chain. Certainly, we possess the block for the creditors and other items. No one can delete any information from the system; if data is incorrectly recorded, it can be rectified by adding new information, but it cannot be wiped.

According to the latest statistics from the official Bank of Albania, the only bank that experienced no system issues last year was FiBank. Incorporating data into Blockchain serves as a safeguard, ensuring continuous system functionality. If a block, such as one containing new bank accounts, is compromised, the system triggers an alert and requires a key from three bank representatives. Initially, from the head of security; then, from the head of IT; and finally, from the director of the bank. The other systems will remain

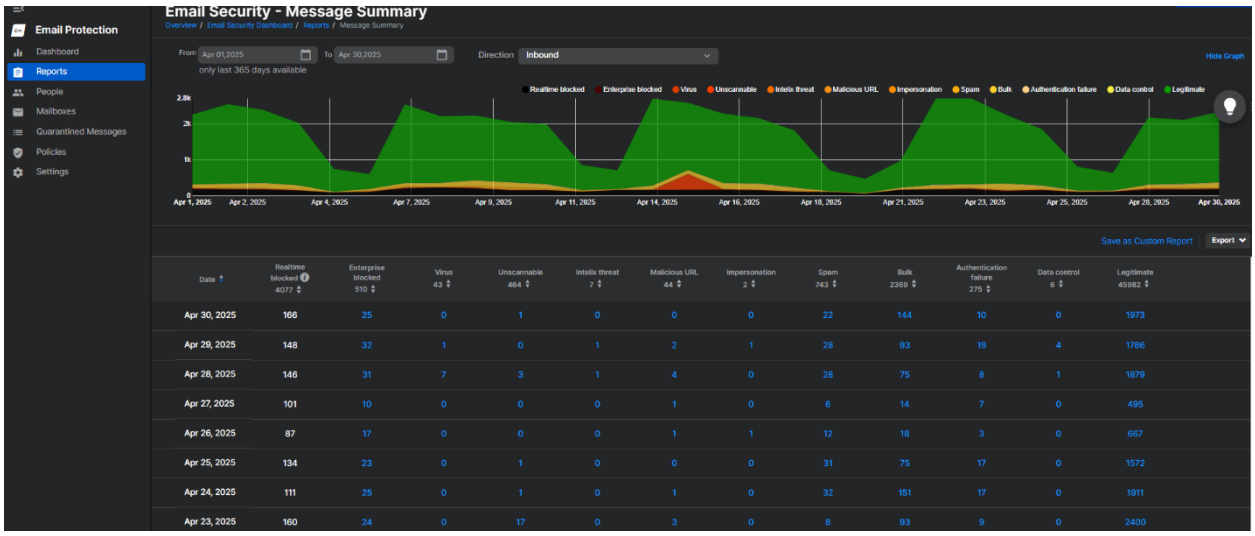
[41] https://support.sophos.com/support/s/article/KBA-000009156?language=en_US

secure, but the compromised block can be paused or taken offline for five minutes due to the significant threat, after which one can re-login using the three passkeys.

We conducted a run, and everything functions flawlessly; but, due to the necessity of including confidential data, I am unable to provide all the images or screenshots.

The new programs that where put into the protectiveness of the systems created where:

A new DPL and Vunerability Management Plus (Manage Engine).



Date	Realtime blocked 4077	Enterprise blocked 510	Virus 43	Unscannable 464	Intelix threat 7	Malicious URL 44	Impersonation 2	Spam 743	Bulk 2369	Authentication failure 275	Data control 6	Legitimate 45982
Apr 30, 2025	166	25	0	1	0	0	0	22	144	10	0	1973
Apr 29, 2025	148	32	1	0	1	2	1	28	93	19	4	1786
Apr 28, 2025	146	31	7	3	1	4	0	28	75	8	1	1879
Apr 27, 2025	101	10	0	0	0	1	0	6	14	7	0	495
Apr 26, 2025	87	17	0	0	0	1	1	12	18	3	0	667
Apr 25, 2025	134	23	0	1	0	0	0	31	75	17	0	1572
Apr 24, 2025	111	25	0	1	0	1	0	32	151	17	0	1911
Apr 23, 2025	160	24	0	17	0	3	0	8	93	9	0	2400

Figure 35.Security Summary 2025[42]

When we draw a parallel with the patient doctor system, we can argue that it is the same thing working as the doctor enters the diagnosis into the system, which is not subject to change, and the medications that the patient ought to take. The patient has the data stored in his system, and he is able to access them in order to view the history. It is also possible for the patient to give access to a doctor with a key if he is in danger of losing his life. Any doctor who is attending the patient can access the medical information. Everyone, including a physician, is unable to remove something from a patient's medical record. If

[42] https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/LogsReports/Reports/EmailMessagesReport/index.html

there is a mistake that has been made, he has the ability to write a note to explain the situation; nevertheless, no record can be wiped, just like the bank system.

5.1. Constraints/Limitations of Blockchain in Healthcare

Although blockchain has considerable advantages, it is not a universal remedy.

Efficiency and Expandability:

Blockchain transactions, such as those on Ethereum, exhibit greater latency and higher costs compared to conventional databases.
Mitigation: Employ a permissioned blockchain (e.g., Hyperledger) or layer-2 solutions (e.g., Optimism) to facilitate expedited and cost-effective transactions. Utilize Filecoin for off-chain storage of substantial data, as implemented in your system.

Expense:

Transaction fees on public blockchains such as Ethereum can be substantial.
Mitigation: Employ a private or permissioned blockchain or enhance smart contract interactions (e.g., batch transactions).

Intricacy:

Integrating blockchain necessitates proficiency in smart contracts, cryptography, and consensus algorithms.
Mitigation: Utilize frameworks such as Web3.py (as implemented in your system) and managed services (e.g., Infura for Ethereum).

Regulatory Obstacles:

The immutable nature of blockchain data contradicts the GDPR's "right to be forgotten."
Mitigation: Store mutable data in CockroachDB and immutable metadata (e.g., hashes, CIDs) on the blockchain, as executed.

Obstacles to Adoption:

Healthcare practitioners may oppose the adoption of blockchain owing to outdated systems or insufficient competence.
Mitigation: Incorporate standards such as FHIR and offer user-friendly APIs (e.g., Flask within your system).

6. CONCLUSIONS

In conclusion, blockchain demonstrates superiority in security, privacy, interoperability, and trust, rendering it well-suited for the delicate and collaborative aspects of healthcare, although its elevated price and complexity. Practical Advantages in the System Security:

Ethereum guarantees immutable metadata and access control, safeguarding against illegal access or manipulation.

Patient Control: Patients utilize smart contracts to confer or withdraw access, hence augmenting privacy and confidence.

Interoperability: Blockchain integrates Filecoin records with CockroachDB metadata, facilitating worldwide access to FHIR-compliant data.

Compliance: Immutable blockchain records and mutable CockroachDB data adhere to HIPAA and GDPR standards.

Efficiency: Smart contracts automate access control, hence diminishing administrative burdens.

Resilience: The decentralized blockchain and Filecoin, in conjunction with CockroachDB’s distributed architecture, guarantee continuous availability.

Blockchain revolutionizes healthcare by offering security, patient autonomy, interoperability, auditability, trust, fraud mitigation, compliance, and resilience, thereby tackling significant industry challenges. In your system, Ethereum's smart contracts guarantee immutable metadata, decentralized access control, and auditability, effectively enhancing Filecoin's storage and CockroachDB's distributed operational data management. Notwithstanding problems such as expense and intricacy, the advantages of blockchain surpass its limitations for sensitive, collaborative healthcare applications.

At the end, we are not reiterating the advantages and disadvantages of blockchain in the area of security in general or in medicine in particular, as we have already listed them in the text. Still, we can say that regardless of the cost, the benefits in the area of security are unimaginable if the system is built correctly. Hospitals, in this case, as well as other fields such as the army or government sites for large tenders, can use this system through contracts, which not only preserves anonymity but will also be much fairer.

6.1. Suggestions for the System

Within the context of the healthcare system, to maximize the benefits of blockchain technology:

Improve the effectiveness of expenditures:

Please take advantage of a permissioned blockchain, such as Hyperledger Fabric, or an Ethereum layer-2 solution, such as Polygon, in order to reduce the amount of gas fees they incur.

Reduce the amount of data that is stored on the blockchain by saving only metadata and CIDs, while using Filecoin for substantial records.

Improve Levels of Confidentiality:

For the purpose of providing privacy-preserving queries on the blockchain, zero-knowledge proofs, such as zk-SNARKs, should be utilized.

CockroachDB should not be used for the storage of encryption keys; instead, a secure key management system (such as Amazon Web Services KMS) should be utilized.

Improve Your Productivity:

CockroachDB should be used to store blockchain metadata in order to improve query speed.

For the purpose of reducing latency, smart contracts should make use of batch transactions.

Adherence is Guaranteed in:

For the sake of auditing, it is important to document every access to the blockchain and CockroachDB.

Ensure compliance with the General Data Protection Regulation (GDPR) by eliminating mutable data from CockroachDB, such as user profiles, while maintaining immutable hashes on the blockchain.

The ability to interoperate:

It is possible to store JSON that is compliant with FHIR in the JSONB fields of CockroachDB or in Filecoin, along with information that is related to the blockchain.

Ensure that electronic health records from the hospital are integrated.

REFERENCE:

[1] G. Tripathi, M. A. Ahad, and G. Casalino, “A comprehensive review of blockchain technology: Underlying principles and historical background with future

challenges," *Decision Analytics Journal*, vol. 9, p. 100344, Dec. 2023, doi: 10.1016/j.dajour.2023.100344.

[2] M. Thanasi-Boçe and J. Hoxha, "Blockchain for Sustainable Development: A Systematic Review," *Sustainability*, vol. 17, no. 11, p. 4848, May 2025, doi: 10.3390/su17114848.

[3] O. José de Oliveira, F. Francisco da Silva, F. Juliani, L. César Ferreira Motta Barbosa, and T. Vieira Nunhes, "Bibliometric Method for Mapping the State-of-the-Art and Identifying Research Gaps and Trends in Literature: An Essential Instrument to Support the Development of Scientific Projects," in *Scientometrics Recent Advances*, 2019. doi: 10.5772/intechopen.85856.

[4] T. Hodge, "Application of Big Data Analytics to Support Homeland Security Investigations Targeting Human Smuggling Networks," *Homeland Security Affairs*, 2018.

[5] M. Yıldız and T. Karakuş Yılmaz, "Bibliometric Analysis in Scientific Research Using R: A Review of Scopus and Web of Science Databases," *Journal of Data Applications*, vol. 0, no. 2, pp. 31–46, Jun. 2024, doi: 10.26650/JODA.1462396.

[6] J. Mingers and L. Leydesdorff, "A review of theory and practice in scientometrics," *Eur J Oper Res*, vol. 246, no. 1, pp. 1–19, Oct. 2015, doi: 10.1016/j.ejor.2015.04.002.

[7] Eugene Garfield, "Citation Indexes for Science A New Dimension in Documentation through Association of Ideas," *Science (1979)*, vol. 122, pp. 108–111, 1995.

[8] D. J. Solla Price's, *Networks of Scientific Papers*, 149(3683)., vol. 149. Science, 1965.

[9] L. Billard and E. Diday, *Symbolic Data Analysis*. Wiley, 2006. doi: 10.1002/9780470090183.

[10] J. LIN, E. KEOGH, S. LONARDI, J. LANKFORD, and D. NYSTROM, "VizTreeA Tool for Visually Mining and Monitoring Massive Time Series Databases," in *Proceedings 2004 VLDB Conference*, Elsevier, 2004, pp. 1269–1272. doi: 10.1016/B978-012088469-8/50124-8.

[11] M. E. J. Newman, "The Structure and Function of Complex Networks.," *SIAM Review 45*, vol. 2, pp. 167–256, 2003.

[12] S. Tabassum, F. S. F. Pereira, S. Fernandes, and J. Gama, "Social network analysis: An overview," *WIREs Data Mining and Knowledge Discovery*, vol. 8, no. 5, Sep. 2018, doi: 10.1002/widm.1256.

[13] S. Fortunato, "Community detection in graphs," *Phys Rep*, vol. 486, no. 3–5, pp. 75–174, Feb. 2010, doi: 10.1016/j.physrep.2009.11.002.

[14] A. Clauset, M. E. J. Newman, and C. Moore, "Finding community structure in very large networks," *Phys Rev E*, vol. 70, no. 6, p. 066111, Dec. 2004, doi: 10.1103/PhysRevE.70.066111.

[15] C. Drago, "Exploring the Community Structure of Complex Networks," *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.2833789.

[16] C. Drago and A. Gatto, "An interval-valued composite indicator for energy efficiency and green entrepreneurship," *Bus Strategy Environ*, vol. 31, no. 5, pp. 2107–2126, Jul. 2022, doi: 10.1002/bse.3010.

[17] C. Lauro and F. Gioia, "Dependence and Interdependence Analysis for Interval-Valued Variables," in *Data Science and Classification*, Springer Berlin Heidelberg, pp. 171–183. doi: 10.1007/3-540-34416-0_19.

[18] M. Vichi and H. A. L. Kiers, "Factorial k-means analysis for two-way data," *Comput Stat Data Anal*, vol. 37, no. 1, pp. 49–64, Jul. 2001, doi: 10.1016/S0167-9473(00)00064-5.

[19] V. Kanade, R. Levi, Z. Lotker, F. Mallmann-Trenn, and C. Mathieu, "Distance in the Forest Fire Model How far are you from Eve?," in *Proceedings of the Twenty-*

Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, Philadelphia, PA: Society for Industrial and Applied Mathematics, Jan. 2016, pp. 1602–1620. doi: 10.1137/1.9781611974331.ch109.

[20] A.-L. Barabási and R. Albert, "Emergence of Scaling in Random Networks," *Science (1979)*, vol. 286, no. 5439, pp. 509–512, Oct. 1999, doi: 10.1126/science.286.5439.509.

[21] N. Almohanna and K. Alhulwah, "<i>NK</i>-Labeling of Graphs," *American Journal of Computational Mathematics*, vol. 14, no. 04, pp. 391–400, 2024, doi: 10.4236/ajcm.2024.144020.

[22] F. Emmert-Streib and M. Dehmer, "Data-Driven Computational Social Network Science: Predictive and Inferential Models for Web-Enabled Scientific Discoveries," *Front Big Data*, vol. 4, Apr. 2021, doi: 10.3389/fdata.2021.591749.

[23] Z. Halim, M. Waqas, A. R. Baig, and A. Rashid, "Efficient clustering of large uncertain graphs using neighborhood information," *International Journal of Approximate Reasoning*, vol. 90, pp. 274–291, Nov. 2017, doi: 10.1016/j.ijar.2017.07.013.

[24] P. Pons and M. Latapy, "Computing Communities in Large Networks Using Random Walks," *J Graph Algorithms Appl*, vol. 10, no. 2, pp. 191–218, 2006, doi: 10.7155/jgaa.00124.

[25] H.-H. Bock and E. Diday, Eds., *Analysis of Symbolic Data*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000. doi: 10.1007/978-3-642-57155-8.

[26] M. Aria and C. Cuccurullo, "bibliometrix : An R-tool for comprehensive science mapping analysis," *J Informetr*, vol. 11, no. 4, pp. 959–975, Nov. 2017, doi: 10.1016/j.joi.2017.08.007.

[27] S. Wasserman and K. Faust, *Social Network Analysis*. Cambridge University Press, 1994. doi: 10.1017/CBO9780511815478.

[28] M. A. Javed, M. S. Younis, S. Latif, J. Qadir, and A. Baig, “Community detection in networks: A multidisciplinary review,” *Journal of Network and Computer Applications*, vol. 108, pp. 87–111, Apr. 2018, doi: 10.1016/j.jnca.2018.02.011.

[29] M. Magnaghi, A. Ghezzi, and A. Rangone, “5G is not just another G: A review of the 5G business model and ecosystem challenges,” *Technol Forecast Soc Change*, vol. 215, p. 124121, Jun. 2025, doi: 10.1016/j.techfore.2025.124121.

[30] A. Manoj Athreya *et al.*, “Peer-to-Peer Distributed Storage Using InterPlanetary File System,” 2021, pp. 711–721. doi: 10.1007/978-981-15-3514-7_54.

[31] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, “Decentralized Applications: The Blockchain-Empowered Software System,” *IEEE Access*, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[32] P. Krawiec, R. Janowski, J. Mongay Batalla, E. Andrukiewicz, W. Latoszek, and C. X. Mavromoustakis, “On providing multi-level security assurance based on Common Criteria for O-RAN mobile network equipment. A test case: O-RAN Distributed Unit,” *Comput Secur*, vol. 150, p. 104271, Mar. 2025, doi: 10.1016/j.cose.2024.104271.

[33] K. A. Tychola, K. Voulgaridis, and T. Lagkas, “Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies,” *Drones*, vol. 8, no. 6, p. 219, May 2024, doi: 10.3390/drones8060219.

[34] M. Š. Mathias Cormann, “Better Regulation Practices across the European Union 2022,” OECD.

[35] J. B. Odili, M. N. M. Kahar, and S. Anwar, “African Buffalo Optimization: A Swarm-Intelligence Technique,” *Procedia Comput Sci*, vol. 76, pp. 443–448, 2015, doi: 10.1016/j.procs.2015.12.291.

[36] S. Mirjalili and A. Lewis, “The Whale Optimization Algorithm,” *Advances in Engineering Software*, vol. 95, pp. 51–67, May 2016, doi: 10.1016/j.advengsoft.2016.01.008.

[37] S. Mirjalili, “The Ant Lion Optimizer,” *Advances in Engineering Software*, vol. 83, pp. 80–98, May 2015, doi: 10.1016/j.advengsoft.2015.01.010.

[38] N. N. Srinidhi, S. M. Dilip Kumar, and K. R. Venugopal, “Network optimizations in the Internet of Things: A review,” *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 1–21, Feb. 2019, doi: 10.1016/j.jestch.2018.09.003.

[39] A. Sircar, K. Yadav, K. Rayavarapu, N. Bist, and H. Oza, “Application of machine learning and artificial intelligence in oil and gas industry,” *Petroleum Research*, vol. 6, no. 4, pp. 379–391, Dec. 2021, doi: 10.1016/j.ptlrs.2021.05.009.

[40] S.-N. Li, Z. Yang, and C. J. Tessone, “Proof-of-Work cryptocurrency mining: a statistical approach to fairness,” in *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, IEEE, Aug. 2020, pp. 156–161. doi: 10.1109/ICCCWorkshops49972.2020.9209934.

[41] bit2me Academy, “What is the Hash Rate?,” bit2me Academy.

[42] Bitcoin Mining Network Stats, “Bitcoin Mining Network Stats,” Bitcoin Mining Network Stats.

[43] https://bitinfocharts.com/, “https://bitinfocharts.com/,” https://bitinfocharts.com/.

[44] P. Kanade, R. K A, Kavya D, and S. Kanade, “Block Chain Application in Healthcare Data Management,” *International Journal of Advanced Networking and Applications*, vol. 15, no. 03, pp. 5952–5958, 2023, doi: 10.35444/IJANA.2023.15305.

[45] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, “Blockchain Application in Healthcare Systems: A Review,” *Systems*, vol. 11, no. 1, p. 38, Jan. 2023, doi: 10.3390/systems11010038.

[46] T. Richard, “Blockchain in Healthcare: Ensuring Data Security and Integrity,” *Research Output Journal of Public Health and Medicine*, vol. 4, no. 2, pp. 12–17, Nov. 2024, doi: 10.59298/ROJPHM/2024/421217.

[47] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, “Blockchain technology applications in healthcare: An overview,” *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.

[48] A. K. Tyagi, S. U. Aswathy, G. Aghila, and N. Sreenath, “AARIN: Affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology,” *International Journal of Intelligent Networks*, vol. 2, pp. 175–183, 2021, doi: 10.1016/j.ijin.2021.09.007.

[49] Y. Li, R. Bi, N. Jiang, F. Li, M. Wang, and X. Jing, “Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks,” *Electronics (Basel)*, vol. 13, no. 12, p. 2372, Jun. 2024, doi: 10.3390/electronics13122372.

[50] C. Roberto Martinez Martinez, “Blockchain Mining: Understanding Its Difficulty in Terms of Hashing Algorithm Efficiency,” in *Blockchain - Pioneering the Web3 Infrastructure for an Intelligent Future*, IntechOpen, 2024. doi: 10.5772/intechopen.1005350.

[51] L. Theodorakopoulos, A. Theodoropoulou, and C. Halkiopoulos, “Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology: A Comprehensive Review,” *Applied Sciences*, vol. 14, no. 16, p. 7007, Aug. 2024, doi: 10.3390/app14167007.

[52] K. Schärer and M. Comuzzi, “The quantum threat to blockchain: summary and timeline analysis,” *Quantum Mach Intell*, vol. 5, no. 1, p. 19, Jun. 2023, doi: 10.1007/s42484-023-00105-4.

[53] Md. Sagar Hossen, T. Tabassum, Md. Ashiqul Islam, R. Karim, L. S. Rumi, and A. A. Kobita, “Digital Signature Authentication Using Asymmetric Key Cryptography with Different Byte Number,” 2021, pp. 845–851. doi: 10.1007/978-981-15-5258-8_78.

[54] A. Alabdulatif, “Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users,” *Information*, vol. 16, no. 3, p. 219, Mar. 2025, doi: 10.3390/info16030219.

[55] P. T. Tran-Truong *et al.*, “A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis,” *Journal of Systems Architecture*, vol. 162, p. 103402, May 2025, doi: 10.1016/j.sysarc.2025.103402.

[56] N. Jayakrishna and N. N. Prasanth, “Detection and mitigation of distributed denial of service attacks in vehicular ad hoc network using a spatiotemporal deep learning and reinforcement learning approach,” *Results in Engineering*, vol. 26, p. 104839, Jun. 2025, doi: 10.1016/j.rineng.2025.104839.

[57] M. Merkebaiuly, “Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods,” *InterConf*, no. 43(193), pp. 494–508, Mar. 2024, doi: 10.51582/interconf.19-20.03.2024.048.

[58] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, “Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques,” *Sensors*, vol. 24, no. 11, p. 3571, Jun. 2024, doi: 10.3390/s24113571.

[59] B. Rodrigues, E. Scheid, C. Killer, M. Franco, and B. Stiller, “Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks,” *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 953–989, Oct. 2020, doi: 10.1007/s10922-020-09559-4.

[60] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, “Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4519–4530, Jul. 2021, doi: 10.1109/TITS.2020.3027390.

[61] X. Li *et al.*, “Blockchain Security Threats and Collaborative Defense: A Literature Review,” *Computers, Materials & Continua*, vol. 76, no. 3, pp. 2597–2629, 2023, doi: 10.32604/cmc.2023.040596.

[62] MIT, “https://bscscan.com/verifyContract-solc?a=0xaEC1A244c043106bA4a1CF1A4D51C0ECE8002c3E&c=v0.8.22%2bcommit.4fc1097e&lictype=3”.

[63] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, “Blockchain for healthcare systems: Architecture, security challenges, trends and future directions,” *Journal of Network and Computer Applications*, vol. 215, p. 103633, Jun. 2023, doi: 10.1016/j.jnca.2023.103633.

[64] N. Sangeeta and S. Y. Nam, “Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability,” *Electronics (Basel)*, vol. 12, no. 7, p. 1545, Mar. 2023, doi: 10.3390/electronics12071545.

[65] S. Schmeelk, M. Kanabar, K. Peterson, and J. Pathak, “Electronic health records and blockchain interoperability requirements: a scoping review,” *JAMIA Open*, vol. 5, no. 3, Jul. 2022, doi: 10.1093/jamiaopen/ooac068.

ANNEXES

Below you will find the database extracted from WoS (Web of Science) with all the information needed to conduct the literature research.

Publication	Authors	Book Auth	Book Edito	Book Grou	Author Full	Book Auth	Group Auth	Article Title	Source Title	Book Serie	Book Serie	Language	Document	Conference	Conference	Conference	Conference	Conference	Author Key	Keywords	Abstract	Addresses	Affiliations	Reprint Ad	Email Addr	Researche	ORCIDs	Funding O	Funding N	Funding Te	Cited Refe	Cited Refe	Times Cite	Times Cite	180 Day U	Since 2013	Publisher	Publisher C	Publisher A	ISSN	eISSN	ISBN
J	Alkatheiri, I				Alkatheiri, I			Blockchain	ELECTRONI			English	Article						blockchain	SECURITY	The Intern	[Alkatheiri,	University c	Alkatheiri,	msalkather	Alkatheiri, I	Alghamdi,	University c	University c	This work w		47	7	7	1	15	MDPI	BASEL	ST ALBAN	2079-9292		
C	Alexander,			IEEE	Alexander,			Cybersecu	2019 IEEE	IEEE Sout		English	Proceeding	IEEE Sout	APR 11-14	Huntsville,	IEEE		blockchain	SECURITY	Blockchain	[Alexander	Mississippi	Alexander,	tech.health							32	3	3	5	39	IEEE	NEW YORI	345 E 47T	1091-0050		978-
J	Pokharel, E				Pokharel, E			blockHealth	INFORMAT			English	Article						blockchain	CHALLENC	The COVID	[Pokharel,	Rochester	Kshetri, N (	bishwoprak		Kshetri, Na					38	0	0	0	0	MDPI	BASEL	MDPI AG, (		2078-2489	
C	Wang, LD;			IEEE	Wang, Lido			Big Data, C	2019 IEEE	IEEE Sout		English	Proceeding	IEEE Sout	APR 11-14	Huntsville,	IEEE		big data; c	ARTIFICIA	Today, Big	[Wang, Lid	Mississippi	Wang, LD	lidong@ise							37	5	5	3	16	IEEE	NEW YORI	345 E 47T	1558-058X		978-
J	Alajlan, R;				Alajlan, Ra			Cybersecu	APPLIED S			English	Review						cybersecur	THINGS IC	The Intern	[Alajlan, Ra		Alajlan, R;	22300097			King Faisa	King Faisa	This work w		56	22	22	7	42	MDPI	BASEL	ST ALBAN		2076-3417	
C	Quasim, MT		Paul, S; Ve		Quasim, Mc			A Blockcha	2020 INTEI			English	Proceeding	Internation	JUL 02-04,	NE Hill Univ	IEEE,IEEE	NE Hill Univ	IoT; Blockc		The world's	[Quasim, M	University c	Quasim, M	mtabrez@u	Algarni, Fa	Quasim, M					26	11	11	3	7	IEEE	NEW YORI	345 E 47T			978-
J	Islam, MS;				Islam, Md.			Blockchain	CMES-CON			English	Review						Blockchain	SOFTWAR	Blockchain	[Islam, Md.	Universiti M	Islam, MS (	msi.ice.ru@	Ajra, Husni	Ajra, Husni	Institute fo	Institute fo	The author		393	5	5	4	52	TECH SCIE	HENDERS	871 CORO	1526-1492	1526-1506	
J	Miriam, DDI				Miriam, D. I			Secured C	INTELLIGE			English	Article						Healthcare	AUTHENTI	Blockchain	[Miriam, D.	Majmaah U	Robin, CRI	crrenerobin	ROBIN, RE	Dahiya, De					36	10	10	1	21	TECH SCIE	HENDERS	871 CORO	1079-8587	2326-005X	
J	Lakhan, A;				Lakhan, Al			Blockchain	IEEE TRAN			English	Article						Blockchain	SCHEDULI	Cybersecu	[Lakhan, A	University c	Tiwari, P (c	abdullah.la	Kumar, Ne	Kumar, Ne	Ministry of	Ministry of	This work w		36	17	18	0	6	IEEE COM	LOS ALAM	10662 LOS	2327-4697		
J	Arafa, A; S				Arafa, Ahm			Emerging I	INFORMAT			English	Review						artificial inte		Emerging (	[Arafa, Ahr	National C	Arafa, A (c	ahmed011	Alsalamah,	Arafa, Ahm					90	1	1	11	28	MDPI	BASEL	ST ALBAN		2078-2489	
J	Almazroi, A				Almazroi, A			Innovative	NETWORK			English	Article						EffiIncepNe		Data mana	[Almazroi, /	University c	Almazroi, A	aalmazroi@	Almazroi, A	Almazroi, A					33	0	0	1	1	SPRINGER	Vienna	Prinz-Euge	2192-6662	2192-6670	
J	García, JA				Garcia, Jor			Securing C	JOURNAL (			English	Article						Cybersecu	HEALTH-C	The existe	[Garcia, Jo		García, JA	jggarcia@u							38	0	0	0	0	TRANS TE	Baech	Seestrasse	2296-9837	2296-9845	
C	Akarca, D;			IEEE	Akarca, D.;			Blockchain	PROCEEDI			English	Proceeding	10th Intern	JUN 05-07,	Leeds Bec	IEEE,Natl /	Leeds Bec	Blockchain		There have	[Akarca, D.	University c	Akarca, D (	danyal@m							13	9	11	0	10	IEEE	NEW YORI	345 E 47T			978-
C	Bornelus, E			ASSOC CC	Bornelus, E			Integrating	ACMSE 20			English	Proceeding	ACM South	APR 02-04	Tampa, FL	Assoc Com		Blockchain		As the hea	[Bornelus,	State Unive	Bornelus, E	bertony1.b	Francia, Gi		National Sc	National Sc	This work w		19	3	3	0	3	ASSOC CC	NEW YORI	1515 BRO.			978-
J	Waghe, PU				Waghe, Pr			Blockchain	INTERNATI			English	Article						Block Chai	HEALTH-C	Securing p	[Waghe, P	Yeshwantr	Waghe, PU		Prasad, Ar						20	1	1	3	3	SCIENCE &	WEST YOI	19 BOLLIN	2158-107X	2156-5570	
J	Waghe, PU				Waghe, Pr			Blockchain	INTERNATI			English	Article						Block Chai	HEALTH-C	Securing p	[Waghe, P	Yeshwantr	Waghe, PU		Godla, Sar						19	0	0	2	2	SCIENCE &	WEST YOI	19 BOLLIN	2158-107X	2156-5570	
J	Bhuyan, SS				Bhuyan, Sc			Transformi	JOURNAL (			English	Article						Cybersecu		The recent	[Bhuyan, S	Rutgers Ur	Bhuyan, S	bhuyanss@	Wyant, Dav	Kabir, Uma					75	50	66	4	40	SPRINGER	NEW YORI	ONE NEW	0148-5598	1573-689X	
C	Castillo, J; (			ASSOC CC	Castillo, Jo			MediLink: /	PROCEEDI			English	Proceeding	2024 Work	OCT 14-18	Salt Lake (	University c		blockchain;		The use of	[Castillo, Jc	University c	Castillo, J (	jorge.a.cas			National Sc	National Sc	We would l		41	0	0	0	0	ASSOC CC	NEW YORI	1601 Broa			979-
J	Szczepaniu				Szczepaniu			Cryptograp	INFORMAT			English	Article						Cybersecu	MEDICAL T	The idea o	[Szczepani	Warsaw Ur	Szczepanii	hubert_szc	Szczepanii	Szczepanii					50	1	1	3	13	ELSEVIER	NEW YORI	STE 800, 2	0020-0255	1872-6291	
J	Hazra, A; A				Hazra, Abh			Blockchain	IEEE CONS			English	Article						Blockchain	COMPUTIN	The blockc	[Hazra, Abl	Indian Inst	Hazra, A (c	abhishek.h	alkhayyat,	alkhayyat,					13	17	17	14	32	IEEE-INST	PISCATAV	445 HOES	2162-2248	2162-2256	
J	Selvarajan,				Selvarajan,			A quantum	SCIENTIFIC			English	Article							ARTIFICIA	Many resea	[Selvarajan	University c	Selvarajan	shitharths@	S, Shithart	selvarajan,					55	28	29	3	11	NATURE P	BERLIN	HEIDELBE	2045-2322		
J	Himdi, T				Himdi, Tarik			A Blockcha	ADVANCES			English	Article						AI security;		Cognitive c	[Himdi, Tar	Jeddah Int	Himdi, T (c	tarikhimdi@							30	0	0	0	0	Shimur Pul	New Moti N	Tc-1/7, TC-		2582-9793	
C	Latoni, A; Z			IEEE	Latoni, Ant			Enhancing	2024 IEEE			English	Proceeding	18th IEEE	NOV 15, 2(	Holtsville, N	Institute of				Cybersecu	[Latoni, An	City Univer	Latoni, A (c	Latoni1332	Zhang, Xia		Google Cy	Google Cy	Zhang is p		8	0	0	0	0	IEEE	NEW YORI	345 E 47T			979-
J	Kumari, KS				Kumari, K.			Synergizing	WATER RE			English	Article; Ear						cybersecur	RENEWAB	The introdu	[Kumari, K.	Velagapud	Kiyosov, S	kiyosov_sh	Kiyosov, S						20	0	0	3	8	IWA PUBL	LONDON	REPUBLIC	2709-6092	2709-6106	
J	Jadav, D; J				Jadav, Dha			A Trustwor	MATHEMA			English	Article						AI; LSTM;	ROBUST; /	Over the la	[Jadav, Dh	Nirma Univ	Gupta, R (c	rajesh.gupt	Tanwar, Su	Jadav, Nile	King Saud	King Saud	This work w		41	5	6	6	31	MDPI	BASEL	ST ALBAN		2227-7390	
J	Kumar, P; J				Kumar, Pra			Blockchain	SOFTWARI			English	Article						blockchain	INTRUSIOI	Artificial Int	[Kumar, Pr	Lappeenra	Kumar, P (	prabhat.ku	Kumar, Pra	Kumar, Pra	Research (	Research (	This work w		37	3	3	10	22	WILEY	HOBOKEN	111 RIVER	0038-0644	1097-024X	
C	Badidi, E; L			IEEE COM	Badidi, Ela			Toward a S	20TH INTE	Internation		English	Proceeding	20th Intern	MAY 06-09	Montreal, C	IEEE		Cybersecu		Modern he	[Badidi, Ela	United Ara	Badidi, E (c	ebadidi@u	Lamaazi, H						23	0	0	0	1	IEEE COM	LOS ALAM	10662 LOS	2639-2313		979-
C	Aich, S; Sir			IEEE	Aich, Satya			Protecting	2022 24TH	Internation		English	Proceeding	24th Intern	FEB 13-16	ELECTR N	Global IT R		Artificial inte		For decade	[Aich, Saty	Inje Univer	Kim, HC (c	satyabrata	Kumar, Sa		Ministry of	Ministry of	This resea		16	2	2	0	13	IEEE	NEW YORI	345 E 47T	1738-9445		979-
C	Sadri, S; SI			IEEE	Sadri, Sam			Blockchain	2022 24TH	Internation		English	Proceeding	24th Intern	FEB 13-16	ELECTR N	Global IT R		Supply cha		To support	[Sadri, San	University c	Sadri, S (c	samin.sadr	sadri, soma		Natural Sci	Natural Sci	This resea		23	0	0	0	3	IEEE	NEW YORI	345 E 47T	1738-9445		979-
J	Sharma, N;				Sharma, N			Emerging a	MULTIMED			English	Article; Ear						Artificial inte	DEEP; BLC	The term a	[Sharma, N	Chitkara U	Sharma, N	neha.1129	Sharma, N	Jindal, Nee					93	5	5	6	24	SPRINGER	DORDREC	VAN GODE	1380-7501	1573-7721	
J	Kumar, A; /				Kumar, Aja			Cutting-Ed	MATHEMA			English	Article						Healthcare	CLOUD; SI	Healthcare	[Kumar, Aj	National In	Khan, SB (	ajay.kumar	Abhishek,	Alzahrani,	King Saud	King Saud	The author		43	0	0	1	1	MDPI	BASEL	ST ALBAN		2227-7390	
J	Olawale, O				Olawale, O			Cybersecu	IEEE ACCE			English	Article						Artificial inte	INTRUSIOI	The Intern	[Olawale, (	Near East	Ebadinezh	sahar.ebac	Ebadinezh	Ebadinezh					62	1	1	7	7	IEEE-INST	PISCATAV	445 HOES	2169-3536		
C	Yeasmin, S			IEEE	Yeasmin, S			Unblocking	2019 INTE			English	Proceeding	Internation	NOV 19-21	Ras Al Kha			Blockchain		Technolog	[Yeasmin,	Al-Yamama	Yeasmin, S	20162219	Yeasmin, S	Yeasmin, S					25	10	10	1	6	IEEE	NEW YORI	345 E 47T			978-
J	Rao, AR; C				Rao, A. Ra			Perspective	INTERNET			English	Article						Internet-of	SMART CC	The space	[Rao, A. Ra	Fairleigh D	Rao, AR (c	ravirao@fd		Clarke, Dai					107	36	37	0	11	ELSEVIER	AMSTERD	RADARWE	2543-1536	2542-6605	
J	Ali, A; Al-rir				Ali, Aitizaz;			HealthLock	SENSORS			English	Article						blockchain		The swift a	[Ali, Aitizaz	UNITAR In	Alsubaei, F	aitizaz.ali@	Al-rimy, Ba	Alsubaei, F	Deputyship	Deputyship	The resear		43	34	34	7	29	MDPI	BASEL	ST ALBAN		1424-8220	
J	Alsemmear				Alsemmear			Resilient S	ELECTRONI			English	Article						tri-layered r	NETWORK	The growth	[Alsemmea	King Abdu	Alsulami, A	ralsemmea	Alsulami, A	Alsulami, A	Deanship c	Deanship c	This projec		41	12	12	2	16	MDPI	BASEL	ST ALBAN	2079-9292		
J	Alamro, H;				Alamro, Ha			Modeling o	IEEE ACCE			English	Article						Deep learn		An IoT hea	[Alamro, Ha	Princess N	Hamza, MA	ma.hamza(	Marzouk, F	Aljameel, D	King Khalic	King Khalic	The author		28	9	9	3	33	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Chinaei, MI				Chinaei, Mc			Optimal Wi	IEEE INTEI			English	Article						Blockchain	DEVICES;	Verification	[Chinaei, M	University c	Gharakheil	m.chinaei@	Gharakheil	Sivaraman					50	23	25	1	10	IEEE-INST	PISCATAV	445 HOES	2327-4662		
J	Pirbhulal, S				Pirbhulal, S			IoT cyberse	INTERNATI			English	Article						Cybersecu	INTERNET	The 5th ge	[Pirbhulal,	Institute fo	Pirbhulal, S	sandeep@	Abie, Habt	Chockaling	SFI Norwe	SFI Norwe	This resea		164	2	2	8	11	SPRINGER	NEW YORI	ONE NEW	1615-5262	1615-5270	
C	Stodt, F; R		Ganascia,		Stodt, Fate			Blockchain	2024 8TH (			English	Proceeding	8th Cyber S	DEC 04-06	Paris, FRAI	Institute of		Blockchain		Modern he	[Stodt, Fat		Stodt, F (c				Federal Mi	Federal Mi	This resea		20	0	0	0	0	IEEE	NEW YORI	345 E 47T			979-
J	Elsayeh, M				Elsayeh, M			CYBERSE	BIOMEDIC			English	Article						Blockchain		The interne	[Elsayeh, M	Egyptian K	Ezzat, KA	kadry ezat	Elsayeh, M	Elsayeh, M					28	11	12	0	25	WORLD SC	SINGAPOI	5 TOH TUC	1016-2372	1793-7132	
J	Saxena, R;				Saxena, R			Semantic a	INTERNATI			English	Review						Blockchain	INDUSTRY	Integrating	[Saxena, F	Koneru La	Saxena, R	rashisaxen	Kumari, P I	Saxena, R					91	5	5	3	18	SPRINGER	NEW DELH	7TH FLOO	0975-6809	0976-4348	
J	Davis, DS				Davis, D.			Investigatin	MEDICAL F			English	Meeting Ab									[Davis, D.]	University c									0	0	0	1	1	WILEY	HOBOKEN	111 RIVER	0094-2405	2473-4209	
C	Koulianos,			ASSOC CC	Koulianos,			Towards E	17TH ACM			English	Proceeding	17th Intern	JUN 26-28,	Crete, GRE	ACM		Healthcare	SECURITY	The manag	[Koulianos		Koulianos,	akoulianos	Papadakis	Litke, Anto	European	European	The work d		20	0	0	0	0	ASSOC CC	NEW YORI	1601 Broa			979-
J	Nguyen, GI				Gia Nhu Ng			Secure blo	JOURNAL (			English	Article						Cyber-phys	ARCHITEC	Cyber-phys	[Gia Nhu N	Duy Tan U	Gupta, BB	nguyengia	Abd El-Lat	Gia Nhu, N	RUSA Pha	RUSA Pha	The work o		27	198	201	8	77	ACADEMIC	SAN DIEG	525 B ST,	0743-7315	1096-0848	
J	Sharma, A;				Sharma, A			A compreh	TRANSACT			English	Review							INFORMAT	Blockchain	[Sharma, A	Thapar Ins	Sharma, A	asharma_p	Kaur, Sanr	Singh, Mar					262	35	35	7	100	WILEY	HOBOKEN	111 RIVER	2161-3915		
J	Raimundo,				Raimundo,			Cybersecu	APPLIED S			English	Article						Internet of	NETWORK	Nowadays,	[Raimundo	Universida	Raimundo,	ricardo.rain	Raimundo,	Rosario, Al	GOYCOPF	GOYCOPF	We would l		70	31	31	8	41	MDPI	BASEL	MDPI AG, (		2076-3417	
B	Awotunde,		Imoize, AL		Awotunde,			Cybersecu	ARTIFICIA	IET Health		English	Article; Boo							INTERNET	Cybersecu	[Awotunde	University c	Awotunde,		Imoize, Ag						122	0	0	2	2	INST ENGI	STEVENA(	MICHAEL I			978-
C	Ahram, T; S			IEEE	Ahram, Tar			Blockchain	2017 IEEE			English	Proceeding	IEEE-Tech	JUN 08-10,	Santa Clar	IEEE,IEEE		Blockchain		Digital worl	[Ahram, Ta	State Unive	Ahram, T (		Ahram, Tai	Sargolzaei					14	245	266	9	85	IEEE	NEW YORI	345 E 47T			978-
C	Alfrhan, AA			IEEE	Alfrhan, Ais			CyberSecu	2019 2ND I			English	Proceeding	2nd Interna	MAY 01-03	Riyadh, SA	IEEE,IEEE		Cyber-Atta		The netwo	[Alfrhan, Ai	Qassim Un	Alfrhan, AA	39120034	AlHusain, F	khediri, sal					17	0	0	0	7	IEEE	NEW YORI	345 E 47T			978-
J	Segal, G; M				Segal, Gad			A blockcha	DIGITAL H			English	Review						Blockchain		Digital tran	[Segal, Ga	Chaim She	Segal, G (	gad.segal@		Segal, Gad					22	1	1	1	11	SAGE PUE	LONDON	1 OLIVERS	2055-2076		
J	Hasan, N; (				Hasan, Nal			pi-BLoM: a	INTERNATI			English	Article; Ear						Industrial Ic	FAILURE-I	The Indust	[Hasan, Na	Jamia Millia	Chaudhary	hasan.nab	Hasan, Na	Hasan, Na					42	0	0	1	1	SPRINGER	NEW DELH	7TH FLOO	0975-6809	0976-4348	
B	Ayodeji, AC		Imoize, AL		Ayodeji, Ar			Achieving (	ARTIFICIA	IET Health		English	Article; Boo								The challe	[Ayodeji, A		Ayodeji, AC								38	0	0	0	0	INST ENGI	STEVENA(	MICHAEL I			978-
C	Prashanth,		Kumar, A; (		Prashanth,			Blockchain	PROCEEDI	Lecture No		English	Proceeding	5th Interna	DEC 15-16	Hyderabad			Block Chai		Blockchain	[Prashanth	Vardhamar	Prashanth,	saiprashan	Karanti, Dr						14	0	0	0	0	SPRINGER	SINGAPOI	152 BEAC	1876-1100	1876-1119	978-
C	Das, D; Bai		Simmhan, '		Das, Deba			A Blockcha	2023 IEEE			English	Proceeding	23rd IEEE/	MAY 01-04	Bangalore,	IEEE,Asso		Blockchain		Cyber-Phy	[Das, Deba	Kalyani Un	Das, D (co	debashis.d	Dasgupta,	Das, Deba					24	1	1	0	4	IEEE COM	LOS ALAM	10662 LOS			979-
J	Singh, N; F				Singh, Nar			Towards ar	INTERNATI			English	Article						SCADA Sy		Peer-to-pe	[Singh, Na	Ramdeoba	Singh, N (c	singhn3@r	Tirpude, Ne						12	0	0	0	1	PERPETU	DELHI-6	5006, HAU	2229-4678	0976-5034	
J	Alatawi, MN				Alatawi, Mc			An Approa	INTERNATI			English	Article						ML; blockcl		This paper	[Alatawi, M	University c	Alatawi, MI	alatawimn(	ALATAWI,		Information	Information	& nbsp;Thi		23	1	1	2	6	WORLD SC	SINGAPOI	5 TOH TUC	0218-1940	1793-6403	
J	Tagliafico, /				Tagliafico,			Blockchain	RADIOLOG			English	Article						Blockchain	TECHNOL(	Blockchain	[Tagliafico,	University c	Tagliafico,	alberto.tag	Tagliafico,	rengo, mar					41	28	30	0	11	SPRINGER	MILAN	VIA DECEI	0033-8362	1826-6983	
J	Alfrhan, A;				Alfrhan, Ais			Comparativ	BLOCKCH/			English	Article						Lightweigh		Over the la	[Alfrhan, A	Qassim Un	Alfrhan, A	39120034	Moulahi, T	Alabdulatif					37	25	25	3	9	ELSEVIER	AMSTERD	RADARWE	2096-7209		
J	Sam, MFM;				Sam, Mohc			The Effecti	INTERNATI			English	Review						wearable d	CHALLENC	Wearable t	[Sam, Moh	University 1	Sam, MFM	mohd.fazli(	Abu Bakar	ISMAIL, AI	Universiti T	Universiti T	This work w		50	6	7	2	16	INT ASSO(	WIEN	KIRCHENG		2626-8493	
J	Ameen, AH				Ameen, Ay			Dimensions	JOURNAL (			English	Review						blockchain	HEALTH; N	The Intern	[Ameen, A	University c	Mohamme	aya21c100	Rashid, Ah	Hamid Ame					68	10	10	2	19	DE GRUYT	WARSAW	BOGUMIL/	0334-1860	2191-026X	
C	Mozumder,			IEEE	Mozumder,			Overview: '	2022 24TH	Internation		English	Proceeding	24th Intern	FEB 13-16	ELECTR N	Global IT R		Metaverse;		Metaverse	[Mozumder	Inje Univer	Kim, HC (c	arifulislamr	Islam Mozu	Mozumder,	Commercia	Commercia	This work w		15	148	156	6	235	IEEE	NEW YORI	345 E 47T	1738-9445		979-
J	Kruger, J; \				Kruger, Jor			The Utilizat	CURRENT			English	Review						Smart cont		Purpose of	[Kruger, Jo	Harvard Ur	Kruger, J (	Jordan@bl							21	0	0	0	0	SPRINGER	NEW YORI	ONE NEW	1531-3433	1534-3081	
J	Alharbi, S;				Alharbi, Sh			Integrating	SUSTAINA			English	Article						Internet of	INTRUSIOI	Recently, t	[Alharbi, SI	King Abdu	Alharbi, S (	smalharbe(	Attiah, Afra	Attiah, Afra	Deanship c	Deanship c	This projec		40	10	10	2	16	MDPI	BASEL	MDPI AG, (		2071-1050	
J	Lone, AN;				Lone, Aeja			A compreh	SECURITY			English	Article						CIA triad; c	INTRUSIOI	It has becc	[Lone, Aej	Aligarh Mu	Alam, M (c	mahfoozal	Alam, Dr. N	Alam, Dr. N					129	36	38	7	40	WILEY	HOBOKEN	111 RIVER	2475-6725		
J	Badri, S				Badri, Sah			HO-CER: H	ELECTRONI			English	Article						blockchain	SYSTEMS	The Intern	[Badri, Sah	King Abdu	Badri, S (c	skbadri@k	badri, saha	badri, saha					27	1	1	0	5	AMER INS	SPRINGFI	PO BOX 2		2688-1594	
C	Smith, KJ;			Assoc Info	Smith, Kan			Blockchain	AMCIS 201			English	Proceeding	23rd Ameri	2017	Boston, MA			Blockchain		Blockchain	[Smith, Kai	Virginia Co	Smith, KJ (	smithkj6@	Dhillon, Gu						15	0	0	1	1	ASSOC IN	ATLANTA	P.O. BOX			978-
J	Singh, AK;				Singh, A. K			A Survey o	ACM TRAN			English	Article						Smart heal	WIRELESS	With the re	[Singh, A. I	National In	Singh, AK	amit.singh	Lyu, Zhiha	Singh, Ami					122	66	69	3	51	ASSOC CC	NEW YORI	1601 Broa	1551-6857	1551-6865	
C	Bangui, H;		Fill, HG; Va		Bangui, Hir			Blockchain	PROCEEDI			English	Proceeding	17th Intern	JUL 11-13,	Lisbon, PO	INSTICC		Critical Infra	SMART CI	The widesp	[Bangui, H	Masaryk U	Bangui, H		Bangui, Hir		ERDF/ESF	ERDF/ESF	The work w		59	0	0	0	2	SCITEPRE	SETUBAL	AV D MAN			978-
J	Lakhan, A;				Lakhan, Al			Secure blo	INTERNET			English	Article						BIoMT; Cai		In today's	[Lakhan, A	University c	Mohamme	abdullah.la	Abdulkaree	Nedoma, J	European	European	This article		35	12	12	1	7	ELSEVIER	AMSTERD	RADARWE	2543-1536	2542-6605	
C	Baskaran, I		Anbar, M; /		Baskaran,			A Survey o	ADVANCES	Communica		English	Proceeding	1st Interna	JUL 30-AU	MALAYSIA	Univ Sains		Blockchain		Due to the	[Baskaran,	Universiti T	Baskaran,	hasventhra	Abdul Rah	Abdul Rah	Ministry of	Ministry of	The author		19	2	2	0	15	SPRINGER	SINGAPOI	152 BEAC	1865-0929	1865-0937	978-
J	Sharma, V;				Sharma, Vi			Digital twin	KNOWLED			English	Article						Cybersecu	INTRUSIOI	Digital twin	[Sharma, V	Delhi Tech	Sharma, K	vikassharm							66	1	1	5	5	SPRINGER	LONDON	236 GRAY	0219-1377	0219-3116	
C	Kadhum, A		Jaber, KM		Kadhum, A			Leveraging	2024 INTE			English	Proceeding	1st Interna	DEC 17-18	Amman, JC	Princess S		Internet of		The rapid c	[Kadhum, /	University c	Kadhum, A	ayatnadhu							38	0	0	0	0	IEEE	NEW YORI	345 E 47T			979-
J	Hakak, S; I				Hakak, Sac			Recent adv	INTERNATI			English	Article						blockchain	MACHINE	The rise of	[Hakak, Sa	University c	Hakak, S (	saqib.haka	Hakak, Sac	Bhattachar					101	15	15	1	38	INDERSCII	GENEVA	WORLD TF	1743-8225	1743-8233	
J	Gnanasun				Gnanasun			Blockchain	JOURNAL (			English	Article						Node Valid	INTERNET	Wireless se	[Gnanasur	Karpagam	Gnanasun	pgnanasur							26	0	0	3	3	IOS PRES	AMSTERD	NIEUWE H	1064-1246	1875-8967	
C	Sharma, CI			IEEE	Sharma, Cl			AI Anomaly	10TH INTE	IEEE Interr		English	Proceeding	10th IEEE	JUL 12-14,	Indian Inst	IEEE,IEEE	Indian Inst	Activity Re		Detecting a	[Sharma, C	Amrita Vish	Sharma, C	chrahulans	M R, Shinu						10	0	0	1	1	IEEE	NEW YORI	345 E 47T	2334-0940		979-
J	Zlatolas, LI				Zlatolas, Li			Data breac	CLUSTER (			English	Review						Data secur	ACCESS-C	The digitali	[Zlatolas, L	University c	Zlatolas, L	lili.nemeczl	Zlatolas, Li	Mwansa, G	Slovenian	Slovenian	The author		135	11	11	12	18	SPRINGER	NEW YORI	ONE NEW	1386-7857	1573-7543	
C	Safavi, S; I		Abidin, KA		Safavi, Sey			Cyber Vuln	PROCEEDI			English	Proceeding	Cyber Resi	NOV 13-15	Putrajaya,	Fac Inform		Cybersecu	SECURITY	Smart hom	[Safavi, Se	Universiti K	Safavi, S (	Safavi@tal	Safavi, Sey	Safavi, Sey	Universiti K	Universiti K	This resea		31	12	12	0	4	IEEE	NEW YORI	345 E 47T			978-
J	Gonçalves,				Goncalves,			User Reput	JOURNAL (			English	Review						reputation	SYSTEMA	User trust i	[Goncalves	Universida	Gonçalves	mjose@isc			European	European	This work w		45	4	4	0	0	MDPI	BASEL	MDPI AG, (		2624-800X	
J	Bensaid, R				Bensaid, R			SA-FLIDS:	PEERJ CO			English	Article						Intrusion de	PRIVACY	Smart heal	[Bensaid, F	Universite (	Maglaras, I	l.maglaras(	Ari, Ado/AF	Abba Ari, A					44	0	0	2	2	PEERJ INC	LONDON	341-345 O		2376-5992	
C	Craggs, B;			IEEE Comp	Craggs, Ba			Trust beyo	2019 IEEE			English	Proceeding	41st IEEE/	MAY 25-31	Montreal, C	IEEE,ACM		Blockchain	BITCOIN	Blockchain	[Craggs, B	University c	Craggs, B	barney.cra			UK Engine	UK Engine	This work h		54	17	17	0	12	IEEE COM	LOS ALAM	10662 LOS			978-
J	Khan, AA;				Khan, Abd			BDLT-IoMT	JOURNAL (			English	Article						Internet of		The integra	[Khan, Abc	Shenyang	Khan, AA (	abdullah.kl	Alsafyani, I	Baqasah, /	The author	The author	The author		42	4	4	5	5	SPRINGER	DORDREC	VAN GODE	0920-8542	1573-0484	
J	Anwar, M;				Anwar, Mas			BBAD: Blo	IEEE ACCE			English	Article						Smart heal		Cybersecu	[Anwar, Ma	Air Univers	Alabdullah	bialabdulla	Alabdullah	AlSagri, Ha	Princess N	Princess N	This work w		59	3	3	5	6	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Jabbar, R;				Jabbar, Ra			Blockchain	IEEE ACCE			English	Review						Blockchain	DISCHARC	The use of	[Jabbar, Ra	Qatar Univ	Jabbar, R (	rateb.jabba	Jabbar, Ra	Zaidan, Es	Qatar Natic	Qatar Natic	This work w		484	84	86	13	166	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Myrzashova				Myrzashova			Safeguardi	IEEE TRAN			English	Article						Medical se	INTELLIGE	Medical he	[Myrzashov	Chinese Ac	Alsamhi, S	rose5004@	Mohsen, G	Alsamhi, S	Natural Sci	Natural Sci	This work w		58	2	2	4	4	IEEE-INST	PISCATAV	445 HOES	2377-3782		
J	Liang, XP;				Liang, Xue			A novel fra	COMPUTEI			English	Article						Cloud secu	COMPUTIN	The rise in	[Liang, Xu	State Unive	Liang, XP	xuliang@fi	Liang, Xue						99	0	0	4	4	ELSEVIER	OXFORD	OXFORD F	0167-4048	1872-6208	
C	Kong, TS;			IEEE	Kong, Tae			Blockchain	2022 24TH	Internation		English	Proceeding	24th Intern	FEB 13-16	ELECTR N	Global IT R		Blockchain		Recently, b	[Joo, Moor	Inje Univer	Lee, TG (c	cmki@nate			Ministry of	Ministry of	This resea		14	3	3	0	4	IEEE	NEW YORI	345 E 47T	1738-9445		979-
J	Alharbi, S;				Alharbi, Sh			A Blockcha	IEEE INTEI			English	Article						Security; IF	IOT; IDS	Nowadays,	[Alharbi, SI	King Abdu	Alharbi, S (	smalharbe(	Mohaisen,	Alghazzaw					27	0	0	13	21	IEEE-INST	PISCATAV	445 HOES	2327-4662		
C	Ghimire, T;				Ghimire, Tu			Blockchain	MATERIAL			English	Proceeding	2nd Interna	SEP 17-18	Phagwara,	Lovely Pro		Industry 4;	2025 TUBE	ABSTR A (	[Ghimire, T	Vellore Ins	Selvaraj, S	senthilkum	Chadha, U	Chadha, U					87	37	42	4	19	ELSEVIER	AMSTERD	RADARWE	2214-7853		
C	Mohammad		Barnaghi, I		Mohammad			CUREX: se	2019 IEEE			English	Proceeding	19th IEEE/	OCT 13-17	Thessaloni	IEEE,WIC,		eHealth; C	SELECTIO	The Health	[Mohamma	University c	Mohamme	farnaz@un	Xenakis, C	M, Farnaz/	EU [H2020	EU(Europe	This resea		30	10	14	0	5	ASSOC CC	NEW YORI	1601 Broa			978-
J	Anderson,				Anderson,			Blockchain	DECISION			English	Article						Patient cor	DESIGN-S	With the in	[Anderson,	University c	Anderson,	ander556@	Anderson,	Anderson,	Miami Univ	Miami Univ	Funding Th		83	8	8	16	43	ELSEVIER	AMSTERD	RADARWE	0167-9236	1873-5797	
C	Cong, RC;		Moallem, A		Cong, Ruic			Secure Inte	HCI FOR C	Lecture No		English	Proceeding	4th Interna	JUN 26-JU	ELECTR N			Blockchain	FRAMEWC	In recent y	[Cong, Rui	Waseda Ui	Jin, Q (com	carriecon@	Asaeda, H	Jin, Qun/0(	2020-2021	2020-2021	The work w		13	0	0	0	3	SPRINGER	CHAM	GEWERBE	0302-9743	1611-3349	978-
B	Wisdom, DI		Imoize, AL		Wisdom, Da			Mitigating (	ARTIFICIA	IET Health		English	Article; Boo							XAI	As we mov	[Wisdom, D	University c	Wisdom, D		Igulu, King	Igulu, King					44	0	0	2	2	INST ENGI	STEVENA(	MICHAEL I			978-
J	Omar, IAA;				Omar, Ilha			Blockchain	COMPUTEI			English	Article						Ethereum;	OPERATIC	The COVID	[Omar, Ilha	Khalifa Uni	Jayaraman	raja.jayarar	Jayaraman	Omar, Ilha	Khalifa Uni	Khalifa Uni	Acknowled		31	85	88	32	191	PERGAMC	OXFORD	THE BOUL	0360-8352	1879-0550	
J	Pilares, ICA				Pilares, Iris			Addressing	SENSORS			English	Article						blockchain	EHR; IMPL	Electronic I	[Pilares, Iris	Charles Da	Azam, S (c	iris.abacan	Azam, San	AKBULUT,					102	17	20	3	29	MDPI	BASEL	ST ALBAN		1424-8220	
J	Almasoud,				Almasoud,			Deep Lean	CMC-COMI			English	Article						Cyber Phys	CYBER-PH	Cyber-Phys	[Almasoud	Prince Sult	Hamza, MA	ma.hamza(	Almasoud,	Motwakel,	Prince Sult	Prince Sult	The author		20	1	1	2	12	TECH SCIE	HENDERS	871 CORO	1546-2218	1546-2226	
B	Adeniyi, AE		Imoize, AL		Adeniyi, Ab			Examining	ARTIFICIA	IET Health		English	Article; Boo							ARTIFICIA	There has	[Adeniyi, A	University c	Adeniyi, AE		Imoize, Ag						73	0	0	3	3	INST ENGI	STEVENA(	MICHAEL I			978-
J	Salim, MM;				Salim, Mika			Federated	HUMAN-CE			English	Article						DDoS; Fed		Distributed	[Salim, Mik	Seoul Natio	Park, JH (c	jhpark1@s	Salim, Mika		National Re	National Re	This resea		36	1	1	1	4	Korea Com	Seoul	C29, 7F, 1		2192-1962	
B	Shafik, W		Imoize, AL		Shafik, Wa			Artificial int	ARTIFICIA	IET Health		English	Article; Boo							INFORMAT		[Shafik, Wa	University E	Shafik, W (		Shafik, Wa						106	0	0	0	0	INST ENGI	STEVENA(	MICHAEL I			978-
J	Oliveira, M;				Oliveira, Mi			Blockchain	SENSORS			English	Article						blockchain;		Industry 5.	[Oliveira, M	Universida	Oliveira, M	miguel@ua	Pereira, Fil	Pereira, Fil					45	12	12	0	13	MDPI	BASEL	ST ALBAN		1424-8220	
J	Selvarajan,				Selvarajan,			A quantum	SCIENTIFIC			English	Correction									[Selvarajan	University c	Selvarajan	shitharths@	S, Shithart	selvarajan,					1	0	0	1	5	NATURE P	BERLIN	HEIDELBE	2045-2322		
J	Semantha,				Semantha,			PbDinEHR	JOURNAL (			English	Article						privacy by (	ISO/IEC 27	Privacy in E	[Semantha	Charles Da	Azam, S (c	sami.azam	Azam, San	Semantha,					110	7	7	0	9	MDPI	BASEL	ST ALBAN		2224-2708	
J	Chuma, KG				Chuma, Ka			'The Way t	INTERNATI			English	Article						Cybersecu	HEALTH-C	Data secur	[Chuma, K	University c	Ngoepe, M	ngoepms@	Ngoepe, M	Chuma, Ka					77	0	0	1	1	IGI GLOBA	HERSHEY	701 E CHC	1930-1650	1930-1669	
J	Mani, V; Ma				Mani, Vino			Hyperledge	ELECTRONI			English	Article						IPFS; heal	BLOCKCH/	Blockchain	[Mani, Vinc	SRM Institu	Mani, V (cc	vm6461@	Alotaibi, Yc	M, Prakash	Taif Univer	Taif Univer	This resea		29	72	73	0	39	MDPI	BASEL	MDPI AG, (	2079-9292		
C	Samonte, I			ASSOC CC	Samonte, I			Exploring I	PROCEEDI			English	Proceeding	12th Intern	JUL 19-21,	JAPAN			cyberattacl		Integrating	[Samonte,	Mapua Uni	Samonte, I	mjcsamont							18	0	0	0	0	ASSOC CC	NEW YORI	1601 Broa			979-
J	Rivera, AO				Gomez Riv			Resilient s	CLUSTER (			English	Article						Cyber-phys	THINGS	Industrial C	[Gomez Riv	University c	Tosh, DK (	aogomezri	Ghosh, Utt	Ghosh, Utt					45	9	9	0	9	SPRINGER	NEW YORI	ONE NEW	1386-7857	1573-7543	
J	Martínez, A				Lopez Mar			A Compreh	ACM COMI			English	Review						Healthcare	IMPLANTA	Currently, h	[Lopez Ma	University c	Martínez, /	antonio.lop	Perez, Gre	LOPEZ MA	European	European	This work h		162	31	32	0	25	ASSOC CC	NEW YORI	1601 Broa	0360-0300	1557-7341	
J	Tarish, HA;				Tarish, Hib			Network se	JOURNAL (			English	Article						Internet of	BLOCKCH/	Limited de	[Tarish, Hit	Universiti K	Tarish, HA	P119044@	Jaber, Mus		Centre for	Centre for	The author		71	5	5	5	7	DE GRUYT	WARSAW	BOGUMIL/	0334-1860	2191-026X	
J	Mahadik, S				Mahadik, S			Digital Priv	IEEE ACCE			English	Article						Privacy; Me	CONTROL	The article	[Mahadik, S		Pawar, PM	pranav@dt	MUTHALA(	Mahadik, D					78	2	2	7	11	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Chengoder				Chengoder			Metaverse	IEEE ACCE			English	Article						Medical se	BIG DATA	The rapid p	[Chengode	Vellore Ins	Gadekallu,	alazab.m@	yenduri, gc	Gadekallu,					226	143	144	46	139	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Hameed, K				Hameed, K			Digital tran	DISCOVER			English	Review						Good healt	COMMUNI	Ensuring g	[Hameed, I	University c	Hameed, K	hameed.kh	Naha, Ran	Naha, Ran					159	4	4	8	12	SPRINGER	LONDON	CAMPUS, 4		2662-9984	
J	Alzahrani, I				Alzahrani, I			Towards D	APPLIED S			English	Article						medical de	BLOCKCH/	The majorit	[Alzahrani,	Umm Al Qu	Ansari, MT	tjtjansari@	Ansari, Tar	Ansari, Md	National Sc	National Sc	The work is		46	19	19	0	15	MDPI	BASEL	MDPI AG, (		2076-3417	
J	Hathaliya, .				Hathaliya, .			A systemat	SECURITY			English	Article						blockchain	TRACEABI	Several de	[Hathaliya,	Nirma Univ	Tanwar, S	sudeep.tar	Tanwar, Su	Tanwar, Su					86	1	1	4	11	WILEY	HOBOKEN	111 RIVER	2475-6725		
J	Messinis, S				Messinis, S			Enhancing	COMPUTEI			English	Review						Internet of	HEALTH-C	Over the p	[Messinis, !	National Te	Messinis, S	smessinis@	Protonotar	Rallis, Ioan	European	European	This paper		212	11	11	20	47	PERGAMC	OXFORD	THE BOUL	0010-4825	1879-0534	
J	AboulEla, S				AboulEla, S			Navigating	AI			English	Review						cybersecur	HEALTH-C	The Intern	[AboulEla,	Toronto M	Kashef, R	samar.g.ab		Ibrahim, Nc	Toronto Me	Toronto Me	This resea		62	3	3	4	8	MDPI	BASEL	ST ALBAN		2673-2688	
C	Rahman, S		Jin, H; Liu,		Rahman, S			An Investig	COGNITIVI	Lecture No		English	Proceeding	14th Europ	NOV09, 20	ELECTR N	European /		IoHT; Heal	MEDICAL I	Medical de	[Rahman, S	Edith Cowa	Rahman, S	saifurb@ou	Kayes, A./I						31	0	0	0	2	SPRINGER	CHAM	GEWERBE	1867-8211	1867-822X	978-
B	Choudhary		Mastorakis		Choudhary			Artificial int	INTELLIGE	IET Teleco		English	Article; Boo							KEY AGRE	Advent of (	[Choudhar	Lovely Pro	Choudhary		Kansal, La	Kansal, La					64	5	5	0	4	INST ENGI	STEVENA(	MICHAEL I			978-
J	Almutairi, N				Almutairi, N			IoT-Cloud I	ELECTRONI			English	Review						IoT and clc	INTERNET	The conflu	[Almutairi, I	University c	Almutairi, N	almu9701@		Sheldon, F					91	0	0	0	0	MDPI	BASEL	MDPI AG, (	2079-9292		
C	Chatterjee,			ACM	Chatterjee,			An Approa	PROCEEDI			English	Proceeding	Internation	OCT 23-26	Washingto	Assoc Com		Internet of		The Intern	[Chatterjee	Howard Un	Chatterjee,	pushpita.c(	Banerjee, S	Ghosh, Utt	National Sc	National Sc	This work w		25	3	4	1	3	ASSOC CC	NEW YORI	1601 Broa			978-
J	Ghadi, YY;				Ghadi, Yaz			Security ris	PEERJ CO			English	Article						Smart grid;	CYBER-AT	The need f	[Ghadi, Ya	Virtual Univ	Mazhar, T	tehseenma	Shahzad,	laghari, asi					112	9	9	15	23	PEERJ INC	LONDON	341-345 O		2376-5992	
J	Kumar, M; !				Kumar, Ma			Hybrid dee	FUTURE G			English	Article						Convolutio	MEDICAL T	The Intern	[Kumar, Ma	Seoul Nati	Kumar, M;	manish.gu	Kumar, Ma		Institute of	Institute of	This work w		39	1	1	3	3	ELSEVIER	AMSTERD	RADARWE	0167-739X	1872-7115	
C	Afolabi, AS			IEEE	Afolabi, Ak			Vulnerable	2024 IEEE	IEEE Intern		English	Proceeding	IEEE Intern	SEP 18-20	Puebla, ME	IEEE		adversarial	ADVERSA	Nowadays,	[Afolabi, Al	University c	Afolabi, AS	afolabiseg	Akinola, Ol						30	0	0	0	0	IEEE	NEW YORI	345 E 47T	2158-3404		979-
J	Nalin, M; Ba				Nalin, Marc			The Europ	JOURNAL (			English	Article						Cross-bord	OPENNCP	Health data	[Nalin, Mar	Imperial Cc	Faiella, G (	giuliana.fai	clemente, f	Tzovaras, I	European	European	The resear		19	27	27	3	41	ACADEMIC	SAN DIEG	525 B ST,	1532-0464	1532-0480	
J	Raval, KJ; .				Raval, Khu			A survey o	INTERNATI			English	Article						Critical infra	HEALTH-C	Technolog	[Raval, Khu	Nirma Univ	Tanwar, S	20bce244(	Eng, Comp	Tanwar, Su					91	5	6	14	21	ELSEVIER	AMSTERD	RADARWE	1874-5482	2212-2087	
J	Palmer, GA				Palmer, Gil			The Intern	REPRODU			English	Review						Automatior	ARTIFICIA	The Intern	[Palmer, G	Universidac	Cohen, J (	jc@embryo		Martin Alca					122	2	2	2	4	ELSEVIER	London	125 Londo	1472-6483	1472-6491	
J	Svandova,				Svandova,			Internet of	JOURNAL (			English	Review						cybersecur	HEALTH; E	Backgroun	[Svandova		Smutny, Z	zdenek.sm	; Smutny, Z	Svandova,	Prague Un	Prague Un	The work w		80	1	1	8	15	DOVE MED	ALBANY	PO BOX 3	1178-2390		
J	Campbell, I				Campbell, I			Transitionir	JOURNAL (			English	Article						Hyperledge		Hyperledge	[Campbell,	Capitol Tec	Campbell,	rc@medcyt							11	2	2	2	11	BRITISH B	LONDON	KEMP HOU		2516-3957	
C	Vayadande			IEEE COM	Vayadande			A Compreh	2024 SECC			English	Proceeding	2nd Interna	JUN 11-12,	S E A Coll		S E A Coll	Web securi		Web 3.0 re	[Vayadand		Vayadande	kuldeep.va	Vayadande	VAYADAN					33	0	0	1	1	IEEE COM	LOS ALAM	10662 LOS			979-
C	Bangui, H;		Bastieri, D;		Bangui, Hir			Shifting tov	PROCEEDI			English	Proceeding	7th Interna	APR 22-24	ELECTR N	INSTICC		Critical Infra	BLOCKCH/	Antifragility	[Bangui, H	Masaryk Ui	Bangui, H		Bangui, Hir		ERDF/ESF	ERDF/ESF	The work w		73	0	0	0	13	SCITEPRE	SETUBAL	AV D MAN			978-
J	Alassafi, M				Alassafi, M			Optimized I	SIGNAL IM			English	Article						Industrial ir		The Indust	[Alassafi, N	King Abdu	Hasan, SH	shhasan@	Hasan, Sy	Hasan, Sy					33	1	1	6	9	SPRINGER	LONDON	236 GRAY	1863-1703	1863-1711	
J	Nankya, M;				Nankya, Ma			Security ar	IEEE ACCE			English	Article						Medical se	CARE	The adopti	[Nankya, N	Massachus	Nankya, M	mnankya@	Chataut, R	Chataut, R					84	1	1	12	12	IEEE-INST	PISCATAV	445 HOES	2169-3536		
C	Chukkapall			ACM	Chukkapall			Ontology d	SAT-CPS'2			English	Proceeding	Secure and	APR 28, 2(	ELECTR N	ACM SIGS		Smart Fish	ARTIFICIA	Increasing	[Chukkapa	University S	Chukkapal	saisreel@u	Gupta, Ma	Gupta, Ma					49	13	14	3	25	ASSOC CC	NEW YORI	1601 Broa			978-
J	Chiaradonr				Chiaradonr			Framework	APPLIED S			English	Article						applied prc	DEPENDE	Cyber risk I	[Chiaradon	Arizona Sta	Jevtic, P (c	pjevtic@as			National Sc	National Sc	The author		94	0	0	3	3	WILEY	HOBOKEN	111 RIVER	1524-1904	1526-4025	
J	Hijji, M; Alai				Hijji, Mohar			A Multivoca	IEEE ACCE			English	Review						COVID-19;		The novel	[Hijji, Moha	University c	Hijji, M (cor	m.hijji@ut.e	Hijji, Mohar	Alam, Gulz	Industrial Ir	Industrial Ir	This work w		107	42	48	3	81	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Demertzi, V				Demertzi, V			An Overvie	APPLIED S			English	Review						smart city; (	CONSORT	A smart cit	[Demertzi, '	Internation	Demertzis,	kdemertz@	Demertzis,						151	23	25	8	47	MDPI	BASEL	ST ALBAN		2076-3417	
J	Azad, MA;				Azad, Muh			Verify and	INTERNET			English	Article						Blockchain	INTRUSIOI	The zero-tr	[Azad, Muh	Birminghar	Azad, MA (	muhamma(	Azad, Raja	Ajmal Azac					167	3	3	9	20	ELSEVIER	AMSTERD	RADARWE	2543-1536	2542-6605	
J	Nowrozy, R				Nowrozy, R			Privacy Pre	ACM COMI			English	Article						Block chair	CARE; BL(	Building a	[Nowrozy, I	Victoria Un	Nowrozy, F	raza.nowro	McIntosh, '	McIntosh, '					155	17	17	20	32	ASSOC CC	NEW YORI	1601 Broa	0360-0300	1557-7341	
J	Raman, R;				Raman, Ra			Unveiling tl	JOURNAL (			English	Review						Thematic a	ARTIFICIA	In a world t	[Raman, R	Amrita Vish	Raman, R	raghu@am	Raman, Ra	Hughes, La					79	10	10	122	168	ELSEVIER	MADRID	CALLE DE	2530-7614	2444-569X	
J	Makris, I; K				Makris, Ioa			A compreh	COMPUTEI			English	Review						Cybersecu	DEEP LEA	Cyberattac	[Makris, Ioa	University c	Radoglou-I	makris@me	Iturbe, Eid	Lalos, Aris	European	European	This projec		321	0	0	21	21	ELSEVIER	AMSTERD	RADARWE	1574-0137	1876-7745	
J	Ahanger, T				Ahanger, T			Machine le	COMPUTEI			English	Article						Internet of	OF-THE-AI	The Intern	[Ahanger,	Prince Satt	Ahanger, T	t.ahanger@	Algamdi, S		Prince Satt	Prince Satt	The author		374	0	0	1	1	PERGAMC	OXFORD	THE BOUL	0045-7906	1879-0755	
J	Urrea, C; K				Urrea, Clau			Recent Adv	PROCESSI			English	Review						industrial rc	BLOCKCH/	Industrial r	[Urrea, Cla	Universida	Urrea, C (c	claudio.urr	Claudio, Ul		Faculty of I	Faculty of I	This work h		124	1	1	4	4	MDPI	BASEL	MDPI AG, (		2227-9717	
J	Gupta, M; /				Gupta, Ma			Security ar	IEEE ACCE			English	Article						Security; pi	ACCESS-C	Internet of	[Gupta, Ma	Tennessee	Gupta, M (	mgupta@tr	Abdelsalar	Gupta, Ma					134	243	257	37	250	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Golda, A; M				Golda, Abe			Privacy and	IEEE ACCE			English	Article						Generative	ARTIFICIA	Generative	[Golda, Ab	Kalinga Ins	Chamola, V	vinay.cham	Hassija, Vil	, Kidus/000					128	23	23	87	143	IEEE-INST	PISCATAV	445 HOES	2169-3536		
J	Pérez, MQ;				Quiles Pere			Breaching	JOURNAL (			English	Article							ODDBALL	Brain-comp	[Quiles Per	University c	Bernal, SL	slopez@ur	Martínez B	Huertas Ce	Bit & Brain	Bit & Brain	This work h		49	7	7	1	9	HINDAWI L	LONDON	ADAM HOU	2040-2295	2040-2309	

ABSTRACT

Since the start of Blockchain in Satoshi Nakamoto's 2008 paper, it has become a significant technology for protecting information storage and transfers in a trustless environment. This thesis presents a literature review of decentralized technology and peer-to-peer networks, offering a scientific study of the most often employed blockchain security applications in cybersecurity operations. The results indicate that the Internet of Things (IoT), machine visualization, and public-key cryptography facilitate blockchain applications, especially in the secure storage of Personally Identifiable Information and online applications and certification schemes. This is a pertinent study based on systematic research from several scientific journals. It will serve as an additional assessment of prospective avenues in Blockchain and cybersecurity research, with particular emphasis on blockchain security for AI data, the safety of Blockchain in IoT, and sidechain security.

Blockchain technology has recently attracted considerable attention due to its exceptional tamper-resistant characteristics and strong security. The sector is anticipated to attain 1.2 billion US dollars by 2030, growing at an annual pace of 82.8 percent.

Recent research has shown numerous vulnerabilities and breaches related to blockchain technology, which highlights the critical necessity for strong blockchain security and effective management to ensure safety and optimal performance.

SUMMARY / ZUSAMMENFASSUNG

Based on the literature review, the study of Blockchain Security in combination with the hospital system requires further research, as the total number of studies that draw valid conclusions, which we considered at the beginning of this paper, is only 144.

The low research numbers make this field, which is still very young, one of the most rapidly developing and valuable fields for the market and society.

It is also necessary to continue studying the incorporation of AI into health, not only in itself but also in all its subfields, such as pharmacy and studies on various diseases. At the global level, many countries still lack studies in this field. However, we would like to

highlight the United States and certain Eastern countries, which have the most significant number of researchers and universities with teams dedicated to studying blockchain in the field of medicine.

From an economic perspective, there is a way in which we can benefit endlessly, not only the hospital but also more broadly. If hospitals create their farms for the creation of blockchain and the benefit of rewards or coins, in this case, then the hospitals themselves can become self-financing. In this case, the benefit would be much higher, but the hospital would need an IT team for the part of the farm if it were allowed to build it in the respective country.

This PhD thesis policy is to improve security in blockchain technology through a hospital case study necessitates a sophisticated methodology that harmonizes technological integrity, regulatory adherence, and practical execution. We present a proposed policy framework that may be considered the "optimal". This policy aims to address security, privacy, interoperability, and scalability while adhering to healthcare standards, including HIPAA and GDPR. We will elucidate the appropriateness of this policy and its adaptability to a healthcare case study.

Proposed Policy: Decentralized Trust Framework Incorporating Layered Security and Privacy-Enhancing Mechanisms.

In the context of data management, decentralization refers to the practice of ensuring that there is no single point of failure while yet maintaining data integrity and accessibility.

Implementing techniques such as pseudonymization, encryption, zero-knowledge proofs, and differential privacy in order to protect patient information is an example of a privacy-preserving technique.

Automating access control, permission management, and audit trails in order to assure compliance and transparency is what we mean when we talk about smart contract governance.

HL7 FHIR, which stands for Fast Healthcare Interoperability Resources, is one example of an interoperability standard that can be implemented in conjunction with blockchain technology to ensure the secure flow of data across different healthcare systems.

Scalability options include the utilization of off-chain storage and layer-2 solutions (such sidechains or state channels) in order to alleviate the challenges posed by performance limits.

Integrating HIPAA and GDPR standards into the blockchain architecture, which includes patient consent and data minimization principles, is an example of regulatory compliance.

Essential Elements of the Policy Hybrid Blockchain Framework:

Integrating public blockchain components will increase transparency in non-sensitive data, such as audit logs or the origin of pharmaceutical supply chain products, which will ultimately lead to an increase in customers' confidence.The rationale is that permissioned blockchains provide a balance of protection and control, which is essential for sensitive healthcare data, while incorporating public parts to guarantee verifiable transparency when necessary.

Mechanisms for Preserving Privacy:

The process of substituting pseudonyms for PII (personally identifiable data) in order to prevent re-identification is known as pseudonymization.

ECC (Elliptic Curve Cryptography) and the AES (Advanced Encryption Standard) are two ways that can be utilized to encrypt data while it is both at rest and as it is transferred. Zero-Knowledge Proofs, also known as ZKPs, are a method that allows for confirmation of information (such as patient eligibility) without divulging the intricacies that lie under the surface.

Introduce noise into aggregated data in order to protect individual records while they are being analyzed. This is known as differential privacy.

The justification for these approaches is that they reduce the risk of privacy breaches, guarantee compliance with regulations such as HIPAA and GDPR, and maintain the usefulness of data collection for research purposes and more.

Governance Based on Smart Contracts:

Implement smart contracts to regulate patient permission, specifying who may access which data and under what circumstances.

Utilize smart contracts for automated auditing, recording every data access or modification attempt in an immutable manner.

The rationale is that smart contracts diminish dependence on intermediaries, bolster confidence, and guarantee adherence to patient consent stipulations.

Interoperability and Adherence to Standards:

By integrating blockchain technology with HL7 FHIR, you can make it easier for different healthcare systems to share data in a consistent manner.

Using programmable policies contained within smart contracts, ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) (data minimization, right to erasure).

The reasoning behind this is that interoperability is a big difficulty in the healthcare industry, and blockchain technology has the potential to provide secure, standardized data transfer while complying to regulatory norms.

Enhancement of Performance and Capacity for Scalability:

Off-chain storage, such as IPFS or cloud solutions, should be utilized for the storage of large medical data, such as image files, while the on-chain storage of metadata or hashes are maintained.

Reducing transaction latency and expenses can be accomplished through the utilization of layer-2 technologies such as state channels or sidechains.

It is difficult to implement blockchain technology in the healthcare industry because of its scalability issues, which are highlighted by Bitcoin's restriction of seven transactions per second. This is because immediate access is vital in this field. In order to ease these constraints, off-chain and layer-2 methods are utilized.

Defending Oneself Against the Attack:

By utilizing permissioned networks that contain dependable nodes, you can reduce the risk of 51% attacks.

In order to protect against ransomware and insider assaults, it is necessary to set up intrusion detection systems that are resilient and irregularity detection procedures.

When conducting vital transactions, it is important to use multi-signature wallets to prevent illegal access.

It is justified that It is important to note that healthcare systems are prominent targets for cyberattacks; these measures strengthen resistance to such attacks.

Putting the Case Study into Practice: Safe and Secure Administration of Electronic Health Records (EHR)

Consider how this policy can be applied to electronic health record management in order to provide evidence for it using a healthcare case study:

In addition to providing people with the ability to take control of their own data, a network of hospitals, clinics, and pharmacies is working to ensure the safe exchange of electronic health records. Utilizing hospitals and clinics as nodes, the execution will involve the implementation of a blockchain that is built on Hyperledger Fabric for the purpose of maintaining electronic health records.

The implementation of patient consent can be accomplished through the utilization of smart contracts, which will allow patients to provide or withdraw access through a mobile application.

The electronic health records should be stored off-chain (for example, on IPFS), while the hashes should be maintained on-chain for the purpose of integrity verification.

In order to enhance interoperability and ensure that providers are able to exchange data fluidly with one another, integrate with HL7 FHIR.

Make use of Zero-Knowledge Proofs in order to verify the eligibility of patients for insurance claims while also protecting sensitive information during the process. Patients are able to maintain control over their data, healthcare providers are able to access authenticated records in a secure manner, and regulators are able to conduct compliance audits by utilizing logs that cannot be altered. Logs that cannot be altered are a solution to the problems of fragmentation, privacy, and interoperability that have been addressed in the research literature.

Recommendations for Patient Record Management

The option that is recommended is Filecoin (via Web3.Storage) because of the way it strikes a balance between cost, robustness, and compatibility with IPFS. Through incentive storage contracts, it guarantees that the resource will be available continuously.

An alternative choice would be to use IPFS in conjunction with a pinning service, such as Pinata, in order to achieve cost-effective solutions, particularly during the development phase.

Archweave is a niche application that is used for vital, immutable information that need to be permanently accessible. Examples of such records include birth certificates and surgical histories.

With its elevated performance specifications, Storj is ideal for systems that require rapid access, such as those that retrieve clinical data in real time.

In conclusion, blockchain displays superiority in security, privacy, interoperability, and trust, which makes it very ideal for the delicate and collaborative parts of healthcare, despite the fact that it is not just expensive but also complex.

With regard to the first study question, it can be stated that blockchain technology offers a solid basis for improving cybersecurity across a wide range of domains due to the fact that it is decentralized and secure. Blockchain technology is quickly becoming a powerful tool for safeguarding devices and networks, particularly in light of concerns around data integrity, unauthorized access, and various forms of fraud. In comparison, as was said previously in this thesis, traditional networks are unable to match with the potential that blockchain technology possesses.

As part of my response to the second research question, I have discussed all of the recent applications of blockchain technology. For this reason, I will now discuss the projects that are now being carried out in Europe and Albania:

Empower individuals to retain and manage their identity data, facilitate secure sharing when it is necessary, and limit the risk of data breaches through the use of digital signatures, electronic identities, and verifiable credentials. Self-sovereign identity (SSI) and trusted data are also referred to as digital IDs. Utilized in a number of countries that are members of the European Union, including Estonia, Belgium, and Spain. In addition, companies who operate within the identity and data trust sectors include cheqd (UK), which is a company.

Risk management, consumer protection, anti-money laundering, mitigation of hostile operations, operational audits, and adherence to cybersecurity requirements are all made easier by the regulation of cryptocurrency exchanges and platforms. Utilized in a number of EU countries in order to implement license, supervision, and transparency requirements in accordance with recent directives (MiCA, AML/CFT rules, DLT pilot regimes, etc.).

Threat intelligence and cyber security solutions that make use of shared immutable logs guarantee the integrity of data, encourage trust in collaborative intelligence, protect the privacy and anonymity of companies that exchange information, and ensure responsibility. These solutions also ensure that companies must take responsibility for their actions. TRADE, which is an acronym that stands for Trusted Anonymous Data Exchange, is a research initiative that focuses on the ways in which businesses have the capacity to share cyber threat intelligence by utilizing blockchain technology while

conforming to regulatory norms. Having said that, our endeavor is not limited to the country of Albania. Unalterable records, secure logs, enhanced authentication, speedy access, and legal validity are all features that are included in document management and secure records. A number of blockchain companies in Europe, including those in Spain, Ireland, and Switzerland, are working on building solutions for the secure storage of documents, the migration to distributed ledger technology infrastructure, and the notarization of documents. Binarii Labs, for example, offers secure document management from beginning to end as well as migration to distributed ledger technology (DLT).

To answer the third and last research question, there are numerous applications and uses for blockchain technology in the healthcare industry. However, the ones that I have researched and found to be more pertinent at the moment include electronic health record management, clinical trials, supply chain management, claims management, consent management, internet of things, and remote monitoring.

Blockchain technology offers numerous advantages to corporations in the healthcare industry; however, the most significant advantages include the following: secure and interoperable records; integrity, transparency, traceability; anti-fraud; fraud reduction; automation; compliance with the General Data Protection Regulation (GDPR); control; and real-time integrity.

The following are some of the issues that we can identify: privacy, interoperability, regulatory approval, scalability, data linkage, integration with legacy systems, immutability, conflict with privacy regulations, latency, and bandwidth.

In conclusion, we are not reiterating the advantages and disadvantages of blockchain in the area of security in general or in medicine in particular, as we have already listed them in the text. Still, we can say that regardless of the cost, the benefits in the area of security are unimaginable if the system is built correctly. Hospitals, in this case, as well as other fields such as the army or government sites for large tenders, can use this system through contracts, which not only preserves anonymity but will also be much fairer. Based on the system that hospitals decide to implement, there are several ways to configure it. In the

text we have listed some of them and specified how they can be built, as well as which one is the best in this case.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my dear Supervisor, Prof.Dr.Rajnai Zoltan. His generous expertise, support, and guidance made me finish my PhD thesis in time. His inspiration and support helped me a lot in completing this thesis.

I am grateful for all my colleagues I found at Obuda University, especially Dr. Esmeralda Kadena for her support and guidance, and, of course, my international friends, for their support and time.

I gratefully acknowledge the support of the Doctoral School of Security and Sciences, Obuda University, for the time and opportunities provided to all International Students, including myself.

Finally, I want to convey my heartfelt thanks to my family and my husband, Teodor, for their unwavering love and support over the years.

I am grateful for my little boy, Andrea, for simply existing and bringing beauty and grace into my life.

(P.S. Never Lost, Always found)