International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Brief Review and Visualization of Hashing Identity Based on the Data Encryption Using Fog-Chain Technology

Swati Sanap[1], Vijay Shelake[2]

[1]Swati Sanap, Department of Computer Engineering, ARMIET, Maharashtra, India
[2]Vijay Shelake, Department of Computer Engineering, University of Mumbai, Maharashtra, India

Abstract:
In this research article the electronics health records are a patient in the form of a cybernetic version which is combination of lots of personal records that are nothing but the personal contact information, patients' medical history, past diagnosis records, prescription medication, medical test result and at the end overall treatment records. The medical health records should be well protected and highly sensitivity for commercial benefits may cloud servers leak patients' privacy. There are major repercussions when patients' private information is compromised. Transparency, verifiable traceability, immutability, auditability, privacy, and security while handling electronic health information are all lacking in the present healthcare system. The internet of health things (IoHT) is used to capture and collect patients' records and store the information on the cloud by using the fog computing. In this review system where we taken around 50 research articles from the different database and also taken 380 datasets form the PubMed database from 1991 to 2024 (02 June 2024). In addition, depending on the different requirement which is partially processed the information. Then the gathered data is stored at the ledger unit through the blockchain network. The hashing identity-based data encryption is a public key encryption which uses a digital signature to encrypt the data to prevent the information from the third party.

Keywords: Data Encryption, Fog Chain technology, Internet of Health Things.

I. INTRODUCTION:

The days of maintaining paper records and relying mostly on fax machines for communication have long since passed in the healthcare sector. These days, patients may access electronic versions of their paper charts, known as Electronic Health Records (EHRs) [26,28, 29]. The user could assume—to the dismay of the third party—that the original EHRs kept in the cloud have been altered when a medical disagreement arises. Furthermore, data stored in the cloud is hard to transfer across many platforms with varied access control policies [27, 30]. The Internet of Things (IoT) is becoming a more significant factor in the possible revolution of the healthcare industry, offering enormous advantages to the field in areas such as medication development, illness prediction analysis, early warning epidemics, preventive healthcare, and patient health monitoring [9,31]. Medical reports and Patient Health Data (PHD) must be continuously evaluated for certain time-sensitive healthcare applications, such ECG and EEG monitoring [2,32, 33]. In order to further our understanding of DM and to explore for a possible treatment, physicians and re-

searchers also require data. It is vital to research novel approaches to automate data collection on a broad scale since these medical data are typically hard to gather for a variety of reasons (e.g., lack of access to valuable data, current restrictions, lack of user trust) [13,34].

The Fog Computing paradigm has been shown to have several significant properties, including low latency, scalability, support for mobility, real-time interaction, and large geographical dispersion [21, 38–42]. Healthcare systems that use fog computing must have security measures in place to protect patient data from attacks, such as access control and key management protocol [22, 43–45]. Such a large volume of created data is also unsuitable for traditional data storage and security methods. Therefore, a blockchain-based security mechanism offers an immutable security solution for such data at the fog layer in order to address these difficulties (latency, security, centralization, and scalability) [7].

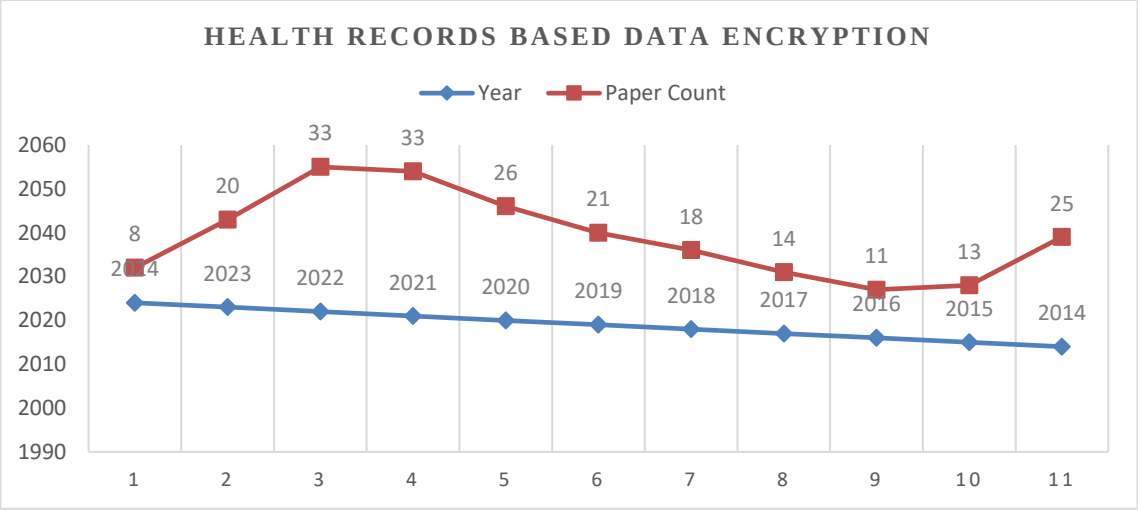

Fig 1: Survey based on Health records-based data encryption keywords.

Because of its decentralized structure and cryptographic features, blockchain technology has shown to be a successful remedy for fog computing and Internet of Things issues in recent years [17,46–52]. Blockchain is an immutable decentralized platform for data management. Because of their structural similarities, it can therefore properly support file tracing metadata on a distributed file system such as IPFS [23]. A fine-grained access control method for Internet of Things devices can be provided by integrating access controls using blockchain [17].

II. LITERATURE REVIEW:

Dammak Bouthaina et al. [23] In this study, we presented LoRaChainCare, an Internet of Things architecture built on Blockchain technology that uses qualitative technologies to enable the safe and authorised exchange of health data, such as patient vital signs and medical reports. To address the QoS needs of HCS, which are mainly low cost, security, scalability, and dependable performance, blockchain, Edge/Fog computing, and LoRaWAN were used. By enabling health professionals to keep an eye on their patients, our suggested approach guarantees patient safety and protection of health. The use of a decentralized file sharing system based on IPFS for private-permissioned blockchain storage maintains security while resolving issues with blockchain scalability and cost while sharing and storing massive amounts of data. Additionally, our suggested HCS combines the Edge and Fog levels with the Cloud and IoT layers. In order to maintain dependable performance, an Arduino Uno board serves as an edge de-

vice and talks with the Fog device via the LoRa communication protocol. We put in place a complete LoRaChainCare prototype as a proof of concept. The system in place incorporates health and environmental sensors that are linked to an Arduino Uno board that has an integrated ATmega328P microprocessor with a LoRa shield. Additionally, a web application is being built so that medical personnel may post reports with large storage capacity into IPFS or investigate Blockchain services.

Al Omar Abdullah et al. [2019] Cybercriminals have always been drawn to data stored in cloud environments. These days, their new area of focus is cloud-based healthcare data. Attacks on these medical records might have disastrous effects on the healthcare companies. Attacks can be lessened by decentralizing this cloud data. Peer-to-peer (P2P) networks provide decentralization, which makes it feasible to store and process sensitive private healthcare data in the cloud. Through the utilization of decentralized or distributed properties, blockchain technology guarantees integrity and accountability. A variety of decentralized attack control strategies have been put forth, but they haven't been able to guarantee the overall privacy of patient-centric systems. In this research, we describe a blockchain-based patient-centric healthcare data management system that enhances privacy through data storage. To guarantee pseudonymity and encrypt patient data, cryptographic functions are employed. We examine the methods utilized for data processing as well as the smart contracts' financial viability in our system [24].

In 2020, Bhaskara S. Egala We have explained a revolutionary solution in this article for decentralized IoMT-based smart healthcare systems that addresses issues with traceability, privacy, anonymity, data security, and latency. Additionally, it demonstrates how to use hybrid computing, DDSS, and blockchain to provide architecture-level answers to the problems raised. Blockchain-based tamper-proof public ledgers provide system level traceability. The security and privacy of medical data are guaranteed by the SRAC and other suggested cryptographic approaches. Conversely, core medical services and medical emergency alerting are automated via smart contracts. In addition, the suggested architecture offers a digital agreement-making platform for various healthcare business players. Our solution demonstrated anticipated features in the logical analysis, such as minimal latency while exchanging data in urgent circumstances [25].

III. RESEARCH GAP AND CHALLENGES:

After Literature review of research article and find the research gap and challenges:

- The quantity and quality of data flow has increased due to the proliferation of IoT devices and their growing usage. Managing massive IoT data flow has emerged as a key concern [2].
- The traditional data storage and security methods are therefore unsuitable for handling the enormous volume of created data in fog computing. As a result, problems with latency, security, centralization, and scalability arose [7].
- The overall healthcare sector is still plagued by worries about data protection in the cloud. As a result, controlling safe IoT data aggregation and granular access to the contracted EMR data is difficult [12].
- In this era of huge data, communication costs are always rising. Fog computing will experience a bottleneck when certain privacy protection mechanisms are implemented because additional communication resources will be used [19].
- The quantity of data that wearable IoT devices in predictive healthcare require to function well is still a problem. Because of the nature of the data utilized for analysis, a lot of personal data is gathered, raising security and privacy issues [18].

IV RESULT AND DISCUSSION

In this research article here, we are going to analyze two different type of analysis that are nothing but network analysis and Statistical analysis with the help of VOS viewer Software tools on the PubMed database.

a. Co-authorship Analysis:

Co-authorship and Authors: An Analysis

Out of the 1164 writers, 3 fulfil the minimum number of documents required for an author. The co-authorship linkages between each of the three writers will be assessed, and the authors with the strongest overall link strength will be chosen. Three authors will be chosen out of the total.

Id	Author	Documents	Total link strength
1	albahri, a s	5	10
2	zaidan, a a	5	10
3	zaidan, b b	5	10

Analysis between Co-authorship and Organization:

We used the complete counting approach for this investigation, where a maximum of 25 organizations are allowed per document. Following this, 8 organizations fulfil the threshold value, with the minimal count of papers from 2 out of the 716 organizations having been picked. The overall final strength of the co-authorship relationships with other organizations will then be computed for each of the eight organizations. This is the point at which the organisation with the strongest overall relationship will be chosen. where eight organizations are to be chosen.

There are just a handful of the eight things in the network that are not connected to one another; the three items that make up the greatest collection of connected objects are those that will be chosen for the network analysis.

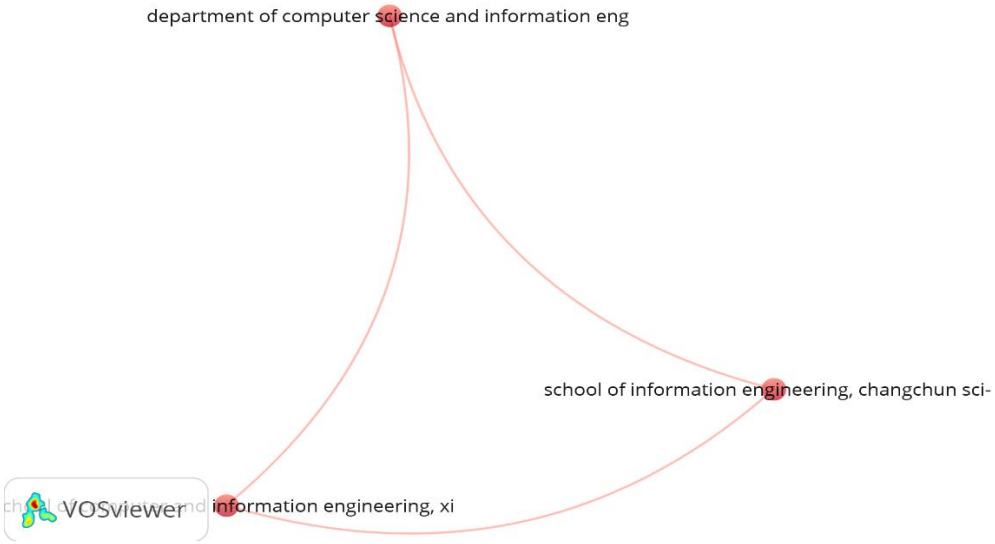

Fig 2: Analysis between Co-authorship and organization.

Co-occurrence and all keywords are analyzed as follows:

This is the full counting approach, where 74 out of the 1080 keywords fulfil the criterion, with a minimum of 5 occurrences of a term. The overall strength of the cooccurrence linkages with other keywords will be computed for each of the 74 keywords. The highest combined link strength keywords will be chosen. There are 74 total keywords that need to be chosen.

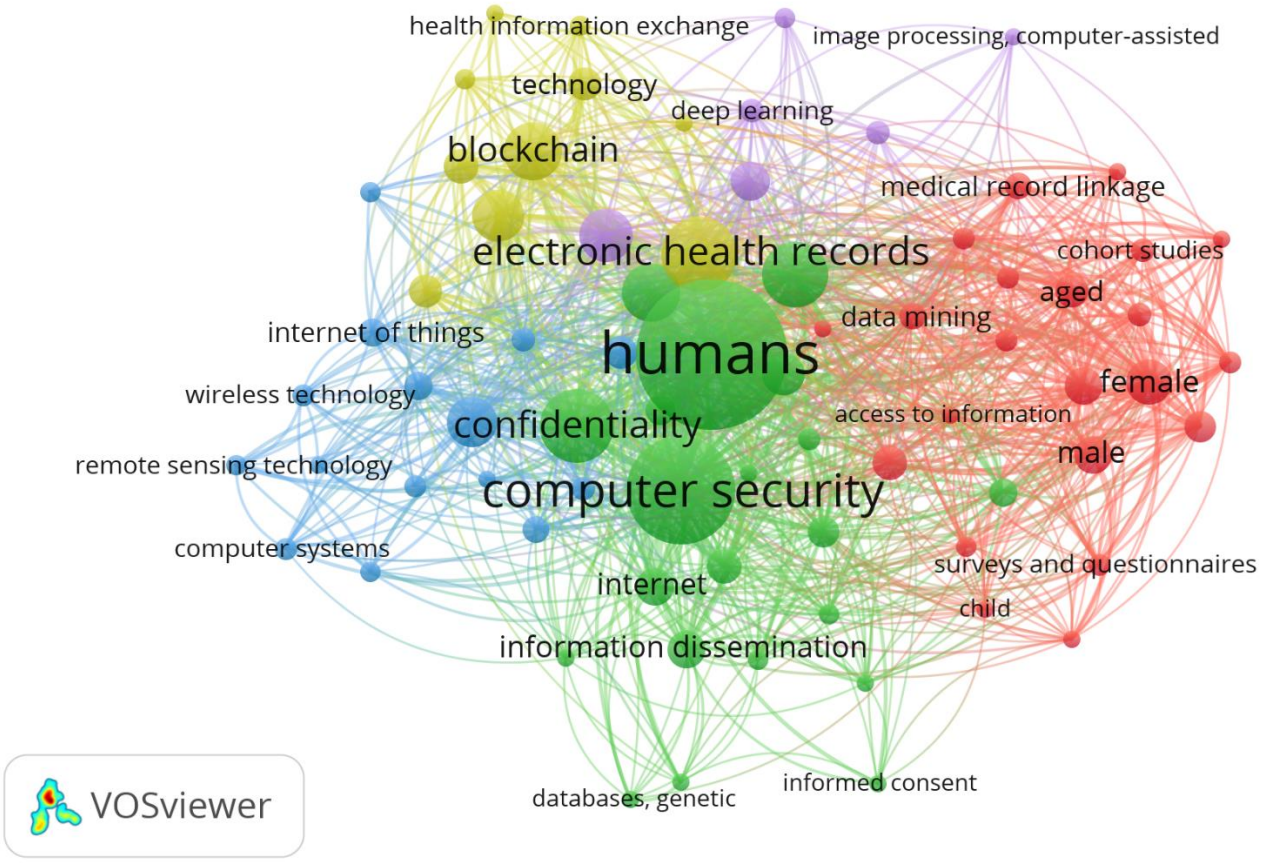

Fig 3: Network analysis between Co-occurrences and All keywords

Keywords for the Network Analysis between Co-occurrence and Authors:

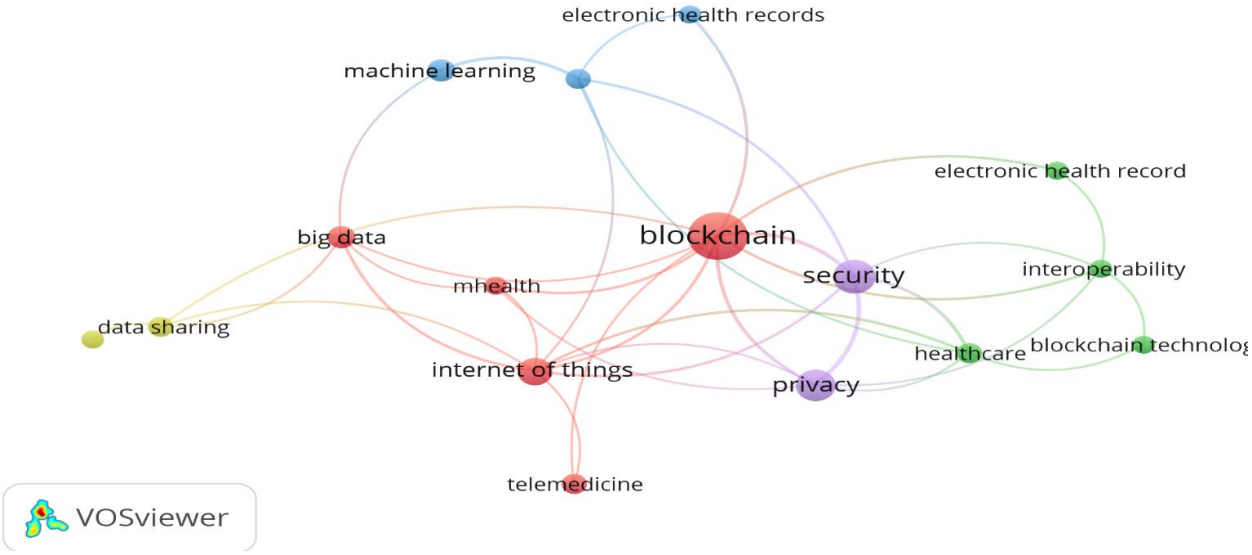

fig 4: Network Analysis of Co-occurrence and Authors Keywords

This is the full counting approach, where 16 out of the 687 keywords fulfil the criterion, with a minimum of 5 occurrences of a term. The overall strength of the co-occurrences linkages with other keywords will be computed for each of the 16 keywords. The terms with the strongest overall link profile will be chosen, with a maximum of 16 counts.

Co-occurrence and MeSH Keyword Network Analysis:

This is the full counting approach, where 63 out of the 459 keywords fulfil the criterion, with a minimum of 5 occurrences of a term. The overall strength of the cooccurrence linkages with other keywords will be computed for each of the 63 keywords. The highest combined link strength keywords will be chosen. There are 63 total keywords that need to be chosen.

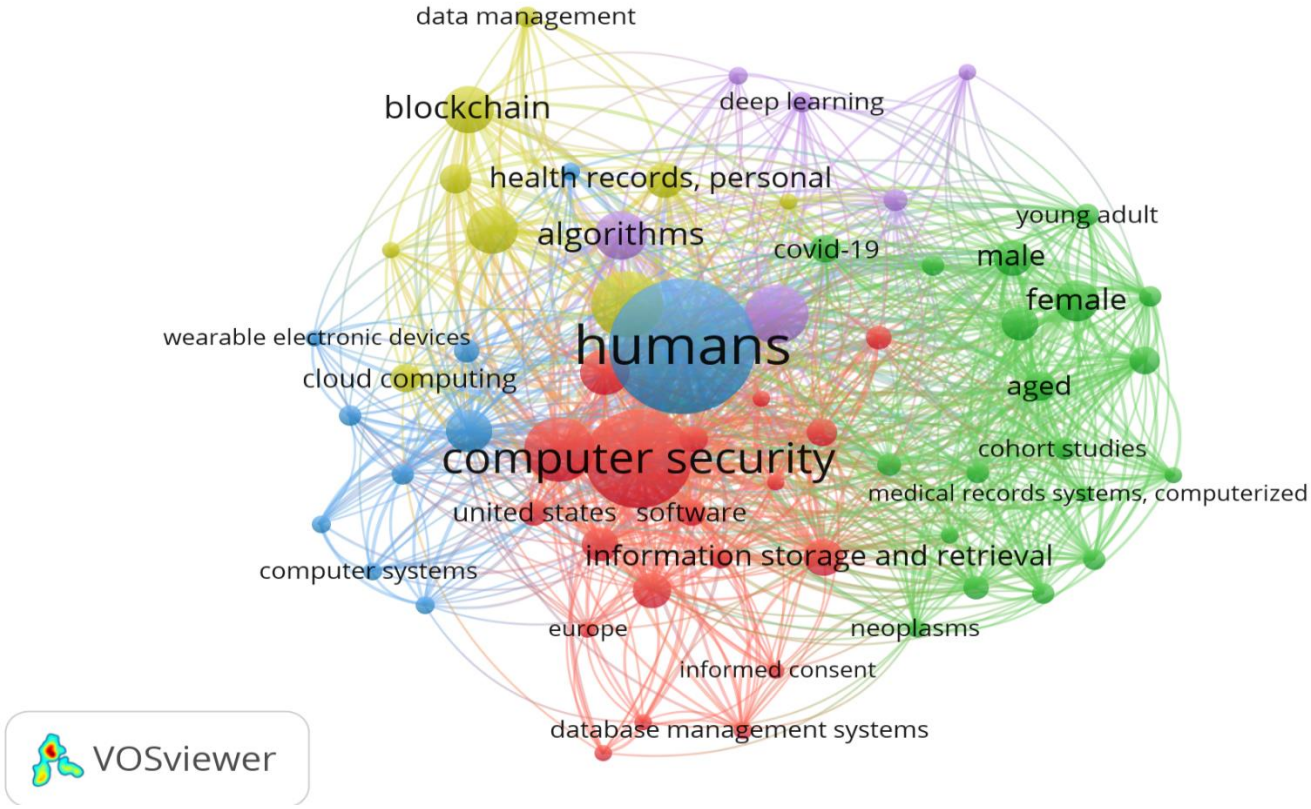

Fig 5: Co-occurrence and MeSH Keyword Network Analysis

Statistical Analysis between Co-occurrences with All Keywords:

Id	Keyword	Occurrences	Total Link strength
1	Adult	16	52
2	Algorithms	29	83
3	Biomedical research	12	38
4	Blockchain	34	104
5	Computer security	94	292
6	Confidentiality	49	178
7	Databases, factual	41	131
8	Delivery of health care	28	75

9	Electronic health records	51	183
10	Female	23	70
11	Health records, personal	18	69
12	Humans	161	409
13	Medical informatics	14	55
14	Privacy	33	121
15	Telemedicine	26	72

Statistical Analysis between Co-occurrence and Authors Keywords:

Id	Keyword	Occurrences	Total Link Strength
1	Artificial intelligence	6	8
2	Big Data	7	6
3	Blockchain	25	20
4	Data protection	5	1
5	Data sharing	6	4
6	Electronic health record	5	3
7	Electronic health records	5	3
8	Healthcare	6	8
9	Internet of things	10	13
10	Interoperability	5	6
11	Machine Learning	7	4
12	Mhealth	5	5
13	Privacy	13	12
14	Security	14	17
15	Telemedicine	6	2

Statistical Analysis between Co-occurrences and MeSH Keywords:

Id	Keyword	Occurrences	Total link strength
1	Artificial intelligence	9	20
2	Biomedical research	12	28
3	Blockchain	28	77
4	Cloud computing	12	39
5	Computer security	94	254
6	Confidentiality	47	160
7	Covid-19	12	31
8	Electronic health records	49	156
9	Female	23	67
10	Health records, personal	18	60
11	Humans	161	336
12	Male	17	52
13	Privacy	27	81
14	Risk factors	7	21

15	Telemedicine	24	64

CONCLUSION

The Scopus, PubMed, IEEE, WoS and Elsevier these are the one of the largest databases in the technological Research word, are used for the literature review, network and statistical analysis and bibliometrics analysis of work done so far in the field of Data Encryption and healthcare using fog-Chain and IoHT technology. Here, we have considered all scientific articles published between June 02, 2024, and 1991. The database was searched using various keywords. A total of 380 documents from the fields of data encryption and healthcare were included in this bibliometrics visualization analysis. This database's evaluation takes into account a few appropriate parameters. It's important to note that practically all of the articles are published in English. The keyword "Blockchain & fog computing" occurs in the most articles, according to the keyword search results, followed by "Data encryption." Network analysis is also supported by VOS viewer software. The same database is used for several study types, including co-authorship and co-occurrences analyses. Numerous network investigations and statistical analyses reveal a great deal about the discrepancies that were previously highlighted.

Additionally, it is evident that much of the work aimed at securing medical records created by health-related IoT devices through the adoption of blockchain and fog computing technologies will be finished between 1991 and 2024. Initially, the link between the most notable texts released is mapped in order to visualize significant contributions to the field. A significant quantity of development in this sector is anticipated in the upcoming year.

ACKNOWLEDGEMENT

We would like to take this opportunity to express our heartfelt gratitude to my supervisor, family, friends, and teachers for their guidance, support, and knowledge in assisting us to complete this research-based project. We would also want to thank the organization's leaders for their continued support and kind help. Lastly, we would like to express our appreciation to everyone who has indirectly contributed to the success of this research endeavor.

References

1. Alsaeed, Norah, Farrukh Nadeem, and Faisal Albalwy. "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing." Future Generation Computer Systems 151 (2024): 162-181.
2. Shukla, Saurabh, Subhasis Thakur, Shahid Hussain, John G. Breslin, and Syed Muslim Jameel. "Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model." Internet of Things 15 (2021): 100422.
3. Mehbodniya, Abolfazl, Rahul Neware, Sonali Vyas, M. Ranjith Kumar, Peter Ngulube, and Samrat Ray. "Blockchain and IPFS integrated framework in bilevel fog-cloud network for security and privacy of IoMT devices." Computational and Mathematical Methods in Medicine 2021 (2021).
4. Islam, Naveed, Yasir Faheem, Ikram Ud Din, Muhammad Talha, Mohsen Guizani, and Mudassir Khalil. "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services." Future Generation Computer Systems 100 (2019): 569-578.
5. Shynu, P. G., Varun G. Menon, R. Lakshmana Kumar, Seifedine Kadry, and Yunyoung Nam. "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog compu-

ting." IEEE Access 9 (2021): 45706-45720.
6. Al Omar, Abdullah, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.
7. Ngabo, Desire, Dong Wang, Celestine Iwendi, Joseph Henry Anajemba, Lukman Adewale Ajao, and Cresantus Biamba. "Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things." Electronics 10, no. 17 (2021): 2110.
8. ElRahman, Sahar A., and Ala Saleh Alluhaidan. "Blockchain technology and IoT-edge framework for sharing healthcare services." Soft Computing 25, no. 21 (2021): 13753-13777.
9. Kumar, Randhir, and Rakesh Tripathi. "Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology." the Journal of Supercomputing (2021): 1-40.
10. Ray, Partha Pratim, Biky Chowhan, Neeraj Kumar, and Ahmad Almogren. "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem." IEEE Internet of Things Journal 8, no. 13 (2021): 10857-10872.
11. Ahmad, Israr, Saima Abdullah, and Adeel Ahmed. "IoT-fog-based healthcare 4.0 system using blockchain technology." The Journal of Supercomputing 79, no. 4 (2023): 3999-4020.
12. Fugkeaw, Somchart, Leon Wirz, and Lyhour Hak. "Secure and Lightweight Blockchain-enabled Access Control for Fog-Assisted IoT Cloud based Electronic Medical Records Sharing." IEEE Access (2023).
13. Fernández-Caramés, Tiago M., Iván Froiz-Míguez, Oscar Blanco-Novoa, and Paula Fraga-Lamas. "Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care." Sensors 19, no. 15 (2019): 3319.
14. Nasir, Muhammad Umar, Safiullah Khan, Shahid Mehmood, Muhammad Adnan Khan, Atta-Ur Rahman, and Seong Oun Hwang. "IoMT-based osteosarcoma cancer detection in histopathology images using transfer learning empowered with blockchain, fog computing, and edge computing." Sensors 22, no. 14 (2022): 5444.
15. Mayer, André Henrique, Vinicius Facco Rodrigues, Cristiano André da Costa, Rodrigo da Rosa Righi, Alex Roehrs, and Rodolfo Stoffel Antunes. "Fogchain: a fog computing architecture integrating blockchain and internet of things for personal health records." IEEE Access 9 (2021): 122723-122737.
16. Alam, Shadab, Mohammed Shuaib, Sadaf Ahmad, Dushantha Nalin K. Jayakody, Ammar Muthanna, Salil Bharany, and Ibrahim A. Elgendy. "Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration." Sustainability 14, no. 22 (2022): 15312.
17. Liu, Yanhui, Jianbiao Zhang, and Jing Zhan. "Privacy protection for fog computing and the internet of things data based on blockchain." Cluster Computing 24 (2021): 1331-1345.
18. Baucas, Marc Jayson, Petros Spachos, and Konstantinos N. Plataniotis. "Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare." IEEE Transactions on Computational Social Systems (2023).

19. Qu, Youyang, Longxiang Gao, Tom H. Luan, Yong Xiang, Shui Yu, Bai Li, and Gavin Zheng. "Decentralized privacy using blockchain-enabled federated learning in fog computing." IEEE Internet of Things Journal 7, no. 6 (2020): 5171-5183.
20. Mohammed, Mazin Abed, Dheyaa Ahmed Ibrahim, and Karrar Hameed Abdulkareem. "Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment." Journal of King Saud University-Computer and Information Sciences 35, no. 1 (2023): 1-12.
21. Costa, Humberto Jorge De Moura, Cristiano Andre Da Costa, Rodrigo Da Rosa Righi, Rodolfo Stoffel Antunes, Juan Francisco De Paz Santana, and Valderi Reis Quietinho Leithardt. "A fog and blockchain software architecture for a global scale vaccination strategy." IEEE Access 10 (2022): 44290-44304.
22. Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, Joel JPC Rodrigues, and Mohsen Guizani. "AISCM-FH: AI-Enabled Secure Communication Mechanism in Fog Computing-Based Healthcare." IEEE Transactions on Information Forensics and Security 18 (2022): 319-334.
23. Dammak, Bouthaina, Mariem Turki, Saoussen Cheikhrouhou, Mouna Baklouti, Rawya Mars, and Afef Dhahbi. "Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring." Sensors 22, no. 4 (2022): 1497.
24. Al Omar, Abdullah, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.
25. Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." IEEE Internet of Things Journal 8, no. 14 (2021): 11717-11731.
26. Donawa, Alyssa, Inema Orukari, and Corey E. Baker. "Scaling blockchains to support electronic health records for hospital systems." In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0550-0556. IEEE, 2019.
27. Xu, Jie, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, and Nenghai Yu. "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data." IEEE Internet of Things Journal 6, no. 5 (2019): 8770-8781.
28. Haux, Reinhold. "Medical informatics: past, present, future." International journal of medical informatics 79, no. 9 (2010): 599-610.
29. Thakkar, Minal, and Diane C. Davis. "Risks, barriers, and benefits of EHR systems: a comparative study based on size of hospital." Perspectives in Health Information Management/AHIMA, American Health Information Management Association 3 (2006).
30. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).
31. Digiteum, “Internet of medical things and medical software development,” 2020, [Online; accessed 5-June-2020]. https ://www.digit eum.com/inter net-medical-things- medical-software-development.
32. A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," in IEEE Access, vol. 8, pp. 118433-118471, 2020, doi: 10.1109/ACCESS.2020.3004790.
33. Shukla, Saurabh, Mohd Fadzil Hassan, Muhammad Khalid Khan, Low Tang Jung, and Azlan Awang. "An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment." PloS one 14, no. 11 (2019): e0224934.

34. Sen, Kabir C., and Kaushik Ghosh. "Designing Effective Crowdsourcing Systems for the Healthcare Industry." In Crowdsourcing: Concepts, Methodologies, Tools, and Applications, pp. 257-261. IGI Global, 2019.
35. Waqar, Adeela, Asad Raza, Haider Abbas, and Muhammad Khurram Khan. "A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata." Journal of Network and Computer Applications 36, no. 1 (2013): 235-248.