Blockchain Technology In Healthcare Services

Adesh Mukati

***Abstract:** The recent ransomware attack on AIIMS (All India Institute of Medical Sciences) has highlighted internal system weaknesses in the healthcare sector, and blockchain technology has emerged as a potential solution to improve security and reduce the risk of future attacks. The decentralized blockchain technology makes it much more difficult for ransomware attackers to focus on a single point of failure. Additionally, blockchain technology provides recipients and data providers with the reassurance that their data has not been changed, enabling enterprises to have confidence and assurance in the integrity of their sensitive data. The sharing of data also restores control of data to its owners. The information is dispersed so that no one company can control it, yet it is still organized around the owner. Thamrin and Xu's research paper proposes a framework for healthcare data storage that includes hospital, city, and state blockchain networks. The proposed system uses a private cloud, but the researchers recommend a hybrid cloud for improved efficiency and adaptability. This innovative approach has the potential to enhance healthcare systems' data security, privacy, and accountability. However, a comprehensive analysis of the problem and an assessment of the potential effectiveness of blockchain technology is necessary before implementing any solutions.*

***Keywords:** Blockchain technology, Healthcare, EHR (Electronic Health Records), Ransomware attack, Distributed ledger technology.*

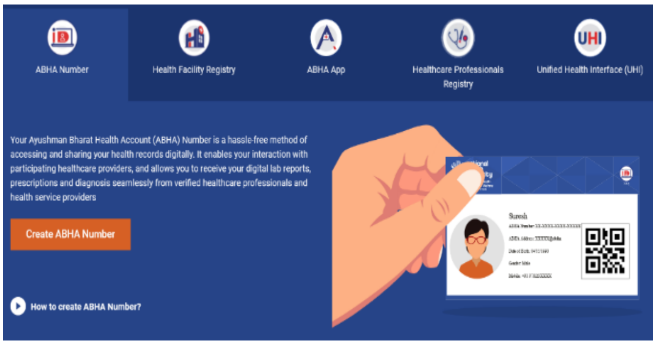
I. INTRODUCTION

The need for better healthcare stems from the reality that it is one of the most pressing issues facing modern civilization. There are seven different parts to the Indian healthcare industry, which uses a lot of data. [1] The ability for these numerous components to interact and exchange data in real time has been enabled by technological advancements. Due to the simplicity of communication and data sharing, the whole healthcare industry is making the shift from a paper-based strategy to digitalization. With the use of EHRs (Electronic Health Records), a step in this direction has been made. But, after the Indian government announced the "Ayushman Bharat Digital Mission" on September 27, 2021, security worries have increased. [2]

Manuscript received on 24 March 2023 | Revised Manuscript received on 05 April 2023 | Manuscript Accepted on 15 May 2023 | Manuscript published on 30 May 2023.

***Correspondence Author(s)**

Adesh Mukati*, 1st Year Student, Master of Cyber Law and Information Security, National Law Institute University, Bhopal (M.P), India. E-mail: adeshmukati.mclis@nliu.ac.in, ORCID ID: https://orcid.org/0000-0001-6449-2508

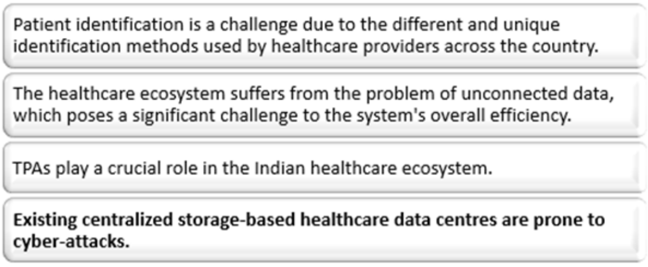

ABHA Number
Health Facility Registry
ABHA App
Healthcare Professionals Registry
Unified Health Interface (UHI)
Create ABHA Number
How to create ABHA Number?
Suresh

Your Ayushman Bharat Health Account (ABHA) Number is a hassle-free method of accessing and sharing your health records digitally. It enables your interaction with participating healthcare providers, and allows you to receive your digital lab reports, prescriptions and diagnosis seamlessly from verified healthcare professionals and health service providers

Figure 1. Health identification explained by the National Health Authority [2]

The recent cyberattack on AIIMS [3][19] has served as a wake-up call during India's efforts to digitize health records. After the AIIMS (All India Institute of Medical Sciences) hack, two additional Indian hospitals disclosed breaches in less than a week. [2][8][20] A hack in November 2021 at Delhi's Safdarjung Hospital prevented several staff members from logging into their computers. The HSE (Health Service Executive), Ireland's health department, experienced a severe ransomware hit earlier in May 2021, which forced the state-wide shutdown of its computer systems. [9] According to a BioMed Central article, the healthcare sector has been identified as being particularly susceptible to cyberattacks because of inherent flaws in its security posture. [2]

Although common, centralized data exchange solutions provide a serious single point of failure issue. We are susceptible to threats and manipulations because the majority of our information is kept on centralized servers (our vital information can end up in the wrong hands). Large centralized systems are frequently attacked by hackers, and there are numerous breaches each year. [10]


Patient identification is a challenge due to the different and unique identification methods used by healthcare providers across the country.

The healthcare ecosystem suffers from the problem of unconnected data, which poses a significant challenge to the system's overall efficiency.

TPAs play a crucial role in the Indian healthcare ecosystem.

Existing centralized storage-based healthcare data centres are prone to cyber-attacks.

Figure 2. Challenges[11]

The motivation behind this research project arises as the existing centralized storage-based healthcare data centers are prone to cyber-attacks (recent attack on AIIMS Delhi), and the Indian government has launched the "Ayushman Bharat Digital Mission", which increases the chances of the AarogyaChain (a blockchain-based health policy implementation) providing a solution to ransomware attacks.

II. REVIEW OF LITERATURE

- Alvin Thamrin, and Haiping Xu, ‘Hierarchical Cloud-Based Consortium Blockchains for Healthcare Data Storage’ [4]

The researcher suggests a cloud-based hierarchical consortium blockchain infrastructure to store and share EHRs, including multimedia files, securely. Local hospital blockchain networks can store huge data with the framework and share it with hospitals outside the network via higher-level blockchain networks.

- Francesco Sanmarchi and others, ‘Distributed Solutions for a Reliable Data-Driven Transformation of Healthcare Management and Research’[12]

This paper highlights the potential of DLT (Distributed Ledger Technology) based solutions to transform healthcare management and research, with practical examples for patients, healthcare management, and research activities. Data and digital technology are essential for efficient healthcare delivery in clinical practice and healthcare management.

- Noor Thamer and Raaid Alubady, ‘A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research’ [11]

The researcher looked at healthcare services' susceptibility to cyberattacks, particularly Ransomware. Researchers are looking into technologies like Blockchain, Software-Defined Networking, and Machine Learning to stop ransomware assaults.

- Brodersen, and others, ‘Blockchain: Securing a New Health Interoperability Experience’ [5]

This research explored how current investments in health IT might be paired with a permissioned blockchain DLT ecosystem to enhance patient outcomes and comply with the ONC's reform plan.

- Yan Zhuang and others, ‘Generalizable Layered Blockchain Architecture for Health Care Applications: Development, Case Studies, and Evaluation’[6]

The research aims to understand emerging healthcare applications, data coordination across multiple facilities is crucial, but distrust is a challenge. By exploiting its qualities, blockchain technology can promote trust, but for actual implementation and performance testing, a standard model is required.

III. STATEMENT OF PROBLEM

A centralized database server in healthcare services is vulnerable to ransomware attacks.

IV. HYPOTHESIS

Using blockchain technology in healthcare services mitigates the risk of ransomware attacks.

V. RESEARCH QUESTIONS

1. Does the implementation of blockchain in healthcare services mitigate the possibility of a ransomware attack?
2. How to implement blockchain in healthcare services?

VI. RESEARCH OBJECTIVES

1. To study and understand the basics of blockchain technology.
2. To determine the potential of blockchain as a security in healthcare.
3. To research the reason behind AIIMS India and HSE Ireland ransomware attacks.
4. To determine the applicability of Indian EHR standards to the proposed structure.
5. To study and analyze the different ways to implement blockchain in healthcare.
6. To investigate the scalability of blockchain technology for large-scale healthcare systems and its potential impact on system performance.

VII. RESEARCH METHODOLOGY

The research methodology used in this research is doctrinal, as the facts are collected from various secondary sources. The research method employed is exploratory since the researcher determines the reason behind the AIIMS India and HSE Ireland ransomware attacks and a potential solution to stop these attacks and assure recovery.

VIII. BLOCKCHAIN AND RANSOMWARE ATTACK

The healthcare sector is undergoing significant changes worldwide, and the recent ransomware attack on AIIMS has highlighted that the primary cause of database vulnerability is internal system weaknesses rather than external factors. To increase security and lower the likelihood of future assaults, blockchain technology has emerged as a possible alternative. However, it is crucial to conduct a comprehensive analysis of the problem and assess the potential effectiveness of blockchain technology before implementing any solutions. [3]

IX. VULNERABILITIES OF CENTRALIZED DATABASES

Security, ethics, and confidentiality are seriously threatened by the use of centralized platforms for data sharing. These topologies make it difficult to share data among many systems, which could result in monopolies. A centralized data system is more vulnerable to dangers since the management of its operation is concentrated in the hands of a single individual, group, or business. Furthermore, centralized data systems frequently violate user privacy by disclosing their information to third parties. Centralized data systems are also valuable targets for hackers, giving them the means to launch assaults and leaving them open to security breaches and data theft. [13]

X. SECURITY VIA BLOCKCHAIN TECHNOLOGY

The immutable record of transactions created by blockchain technology, which cannot be deleted, changed, or destroyed, makes it a highly secure system. [7] It is impervious to manipulation because of its decentralized implementation and special data structure. It is challenging to change the contents of the blockchain unless a majority of the network has come to a consensus to do so because every new block added to the blockchain updates every system on the network.

Controlling 51% or more of the blockchain copies would be necessary for this, which would necessitate a costly and resource-intensive attack. As a result, a high level of security and transparency is associated with blockchain technology. [14]

XI. LESSON LEARN FROM HSE ATTACK

The HSE attack, which occurred in May 2021, was a massive ransomware attack that had a tremendous effect on the Irish healthcare sector. The HSE attack made it clear how important it is to put strong cybersecurity safeguards in place, to regularly back up important data, and to have an effective incident response strategy in place. To guarantee that all stakeholders are informed promptly and openly, it is also crucial to have a communication plan in place. To ensure that staff employees are knowledgeable about the risks of cyberattacks and can recognize and report potential security issues, firms should also invest in employee training. Finally, the HSE attack emphasizes the necessity of coordination and teamwork between businesses and government entities to combat cybersecurity threats and guarantee the security and resilience of vital infrastructure. [9]

XII. RANSOMWARE PREVENTION THROUGH BLOCKCHAIN TECHNOLOGY

Blockchain technology adoption involves more than just deciding where to store data, it also involves separating applications from data. Beyond security aspects, blockchain technology offers other benefits. The ability to conduct secure, decentralized, and encrypted peer-to-peer transactions is altering the way we use the software. Due to decentralization, there isn't a single copy of the data that may be taken, hostage. Instead, a few authorized individuals can securely access the data. Another advantage of blockchain is its immutability, which prevents anyone, including system administrators, from changing data once it has been written to a blockchain. It is nearly impossible to alter data on the ledger without being promptly discovered because of the sequential hashing method used in blockchain technology, which creates a distinctive fingerprint of the data content. Including dependable sources of input, such as smart devices, biometrics, or location awareness, which seals data within the blockchain transaction fabric, can also increase security. These precautions produce a more reliable and secure system that is more difficult to attack.

XIII. LEGAL ISSUES WITH BLOCKCHAIN AND EHR (ELECTRONIC HEALTH RECORD)

1. Data privacy and security: The DPDP (Digital Personal Data Protection Bill) Law, which has not yet been passed in India, raises questions about how personal data is handled and safeguarded. Any application of blockchain technology must adhere to the strict requirements imposed by HIPAA (Health Insurance Portability and Accountability Act) rules in the US for safeguarding patient privacy and security.

2. Legal Validity: As a relatively new technology, blockchain has not yet achieved full legal legitimacy in India. Blockchain transactions and contracts require legal recognition as well as regulatory clarity.

3. Interoperability and Standardization: Standardization of protocols and interoperability across different blockchain networks are essential for blockchain to be successful in the healthcare industry. Collaboration between regulatory agencies and stakeholders is necessary for this.

4. Governance: To ensure transparency, accountability, and regulatory compliance, blockchain networks must be properly governed and overseen.

XIV. EHR STANDARDS (INDIA)

India's EHR standards play a critical role in ensuring that EHRs are designed and implemented in a way that supports data privacy, interoperability, and patient-centered care. The development and adoption of blockchain-based EHRs in India are supported by these standards, which are compliant with international best practices. Healthcare organizations in India may make sure that patient health information is secure by following these standards and that their EHR systems are compatible with other healthcare systems by making sure that they can communicate with them. [21]

XV. SUGGESTED BLOCKCHAIN-BASED MODEL FOR HEALTHCARE SERVICES

Beyond its roots in cryptocurrencies, blockchain technology has a wide range of applications, including the storage and management of medical data. Such data can be difficult to store and convey, but blockchain offers a solution. In their study titled "Hierarchical Cloud-Based Consortium Blockchains" for Healthcare Data Storage, Thamrin and Xu propose a cloud-based hierarchical consortium blockchain framework with blockchain networks for hospitals, cities, and states. Although the proposed system uses a private cloud, the researchers recommend a hybrid cloud for improved efficiency and adaptability. This innovative approach has the potential to enhance healthcare systems' data security, privacy, and accountability. [15]

XVI. HIERARCHICAL HYBRID CLOUD-BASED CONSORTIUM BLOCKCHAIN FRAMEWORK

The proposed system consists of three layers (hospital, city, and state) of blockchain networks. The hospital layer comprises multiple HBNs (Hospital Blockchain Networks), with each HBN including several hospitals within a city and their end-users (doctors, nurses, and patients). To handle the issue of scalability, the HBN utilizes a cloud-based and lite block scheme for storing large amounts of data. Each hospital is represented by a βHOS (Hospital Super Peer Agent), which manages its hybrid cloud. A group of βHOSs representing different hospitals within a city is responsible for approving or rejecting requests from end-users [Regular Peer Agents, βREPs (Regular Peer Agents)]. The city layer consists of several CBNs (City Blockchain Networks), each involving several βCITs (City Super Peer Agents) from the same state. A CBN is connected directly to a βSTA (State Super Peer Agent), which functions as a network regulator and representative of the state.

The state layer comprises a single SBN (State Blockchain Network), which involves all βSTAs (State Super Peer Agents) in the country. This hierarchical design enables users to search and retrieve EHRs from various hospitals across cities and states via βCITs and βSTAs. [4]

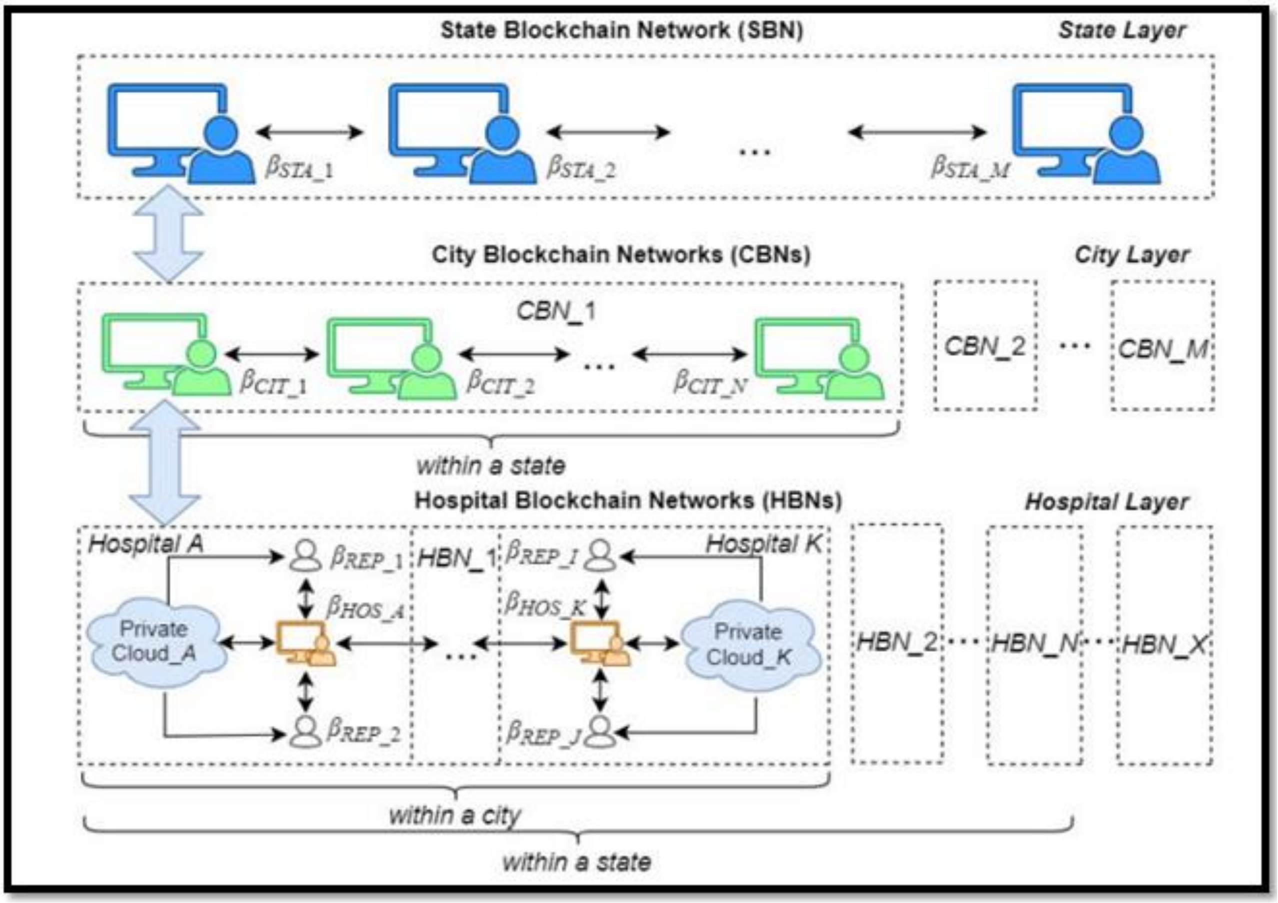


Figure 3. Hierarchical cloud-based consortium blockchain architecture[4]

XVII. INTEGRATE HYBRID CLOUD WITH HIERARCHICAL CLOUD-BASED CONSORTIUM BLOCKCHAIN

To integrate the hybrid cloud with blockchain-based healthcare services, the following steps can be taken:

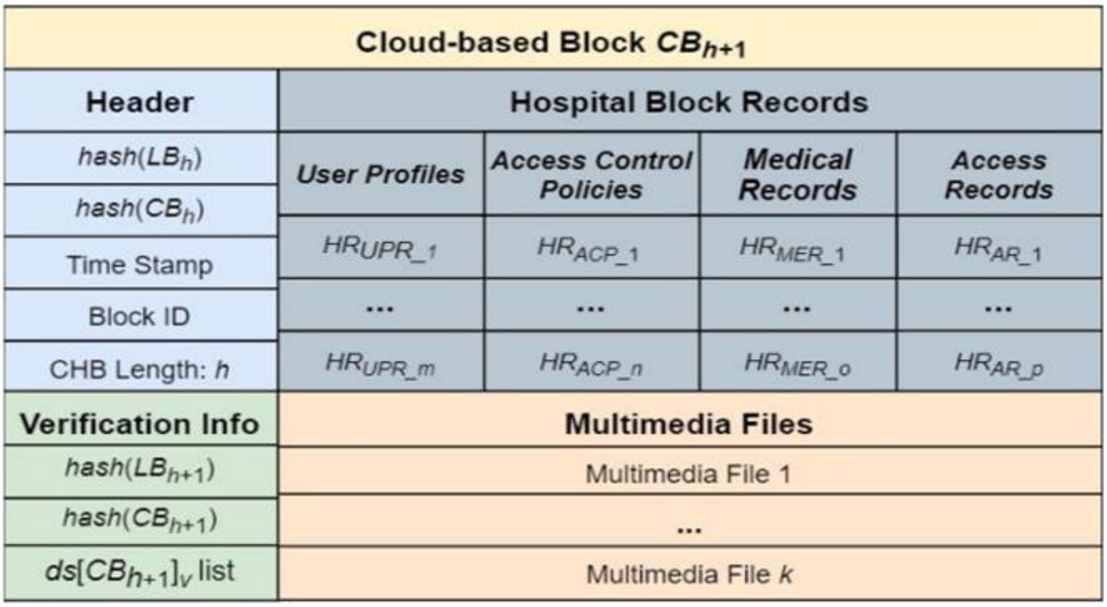
1. Identify the healthcare data that needs to be stored and secured on the private cloud and public cloud.
2. Choose hierarchical cloud-based consortium blockchain network architecture.
3. Implement the necessary access control mechanisms, such as smart contracts and public-key cryptography, to ensure that only authorized users have access to healthcare data.
4. Deploy the private cloud for storing sensitive data and the public cloud for storing non-sensitive data.
5. Use data encryption methods to protect the data, such as symmetric encryption, asymmetric encryption, and hashing.
6. Implement data replication strategies for disaster recovery, such as geographically distributed data centers.
7. Continuously monitor the hybrid cloud infrastructure and blockchain network for potential security threats and vulnerabilities. [4]

XVIII. HOSPITAL BLOCKS AND BLOCK RECORD TYPES

The HBN (Hospital Blockchain Network) can have two variants: a hybrid cloud-based CHB (Cloud-Based Hospital Blockchain) and a simplified version called an LHB (Lite Hospital Blockchain). There are four types of block records (HRUPR, HRACP, HRMER, and HRAR) that can be stored in both CHB and LHB.

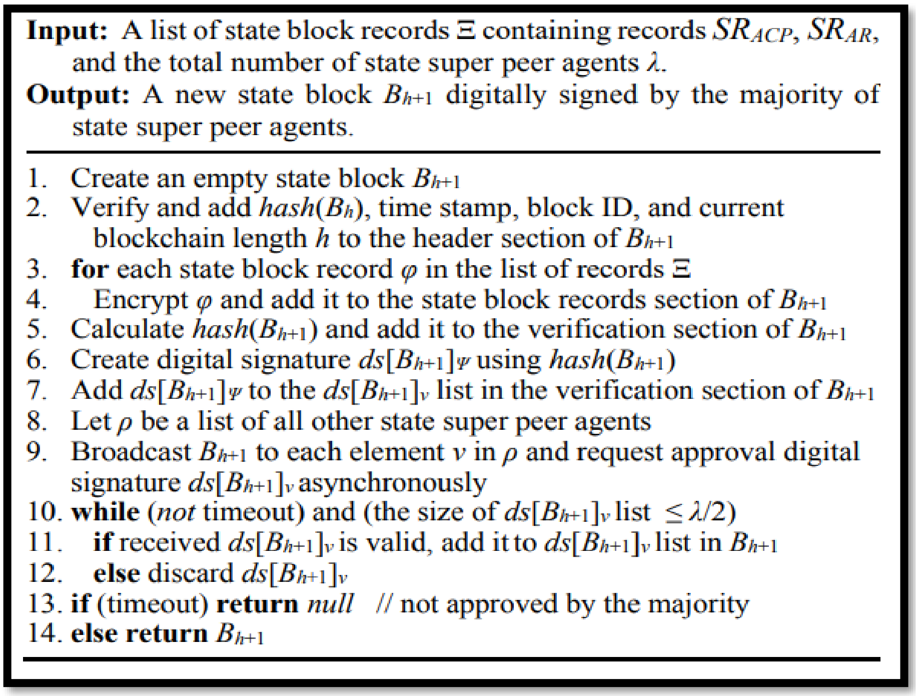
1. HRUPR (Hospital Record User Profile Record) contains user profiles and account information of regular peers
2. HRACP (Hospital Record Access Control Policies) stores access control policies enforced by the hospital super peer agent βHOS (Hospital Super Peer Agent).
3. HRMER (Hospital Record Medical Reports) stores medical reports of patients and metadata of associated multimedia files.
4. HRAR (Hospital Record Access Record) records store access requests or search information of a patient's EHRs in hospitals within the same city.

The cloud-based block CBh+1 (h is the length of the current blockchain) with four types of hospital block records has a structure shown in Figure 4.



Cloud-based Block CB_{h+1}				
Header	**Hospital Block Records**			
$hash(LB_h)$ $hash(CB_h)$	*User Profiles*	*Access Control Policies*	*Medical Records*	*Access Records*
Time Stamp	HR_{UPR_1}	HR_{ACP_1}	HR_{MER_1}	HR_{AR_1}
Block ID	...	...	...	...
CHB Length: h	HR_{UPR_m}	HR_{ACP_n}	HR_{MER_o}	HR_{AR_p}
Verification Info	**Multimedia Files**			
$hash(LB_{h+1})$	Multimedia File 1			
$hash(CB_{h+1})$	...			
$ds[CB_{h+1}]_v$ list	Multimedia File k			

Figure 4. Cloud-based block (CBh+1) in a hospital blockchain [4]



```
Input: A list of state block records $\Xi$ containing records $SR_{ACP}$, $SR_{AR}$,
    and the total number of state super peer agents $\lambda$.
Output: A new state block $B_{h+1}$ digitally signed by the majority of
    state super peer agents.

Create an empty state block $B_{h+1}$
Verify and add $hash(B_h)$, time stamp, block ID, and current
    blockchain length $h$ to the header section of $B_{h+1}$
for each state block record $\varphi$ in the list of records $\Xi$
    Encrypt $\varphi$ and add it to the state block records section of $B_{h+1}$
Calculate $hash(B_{h+1})$ and add it to the verification section of $B_{h+1}$
Create digital signature $ds[B_{h+1}]_\Psi$ using $hash(B_{h+1})$
Add $ds[B_{h+1}]_\Psi$ to the $ds[B_{h+1}]_v$ list in the verification section of $B_{h+1}$
Let $\rho$ be a list of all other state super peer agents
Broadcast $B_{h+1}$ to each element $v$ in $\rho$ and request approval digital
signature $ds[B_{h+1}]_v$ asynchronously
while (not timeout) and (the size of $ds[B_{h+1}]_v$ list $\leq \lambda/2$)
    if received $ds[B_{h+1}]_v$ is valid, add it to $ds[B_{h+1}]_v$ list in $B_{h+1}$
    else discard $ds[B_{h+1}]_v$
if (timeout) return null   // not approved by the majority
else return $B_{h+1}$
```

Figure 5. Generation and approval algorithm of a new block [4]

XIX. SEARCHING AND RETRIEVING EHRS

The system obtains patient permission and creates access control policies to retrieve their EHRs. The search process involves SPAs (Super Peer Agents) in the hierarchical blockchain network structure and is broken down into three tasks. Access control policies are stored in blockchains in HBN, CBN, or SBN as HRACP, CRACP (City-Wide Records for Access Control Policies), or SRACP (State-wide Records for Access Control Policies), which specify which data can be accessed by participants based on their credentials. A standard peer can make access requests for patient EHRs, and super-peer agents authenticate those requests. If the request is approved based on the policy records, the hospital super peer agent retrieves the requested EHRs from its CHB and sends the original requester the access link. [4]

XX. BENEFITS OF USING HYBRID CLOUD INSTEAD OF PRIVATE CLOUD

Using a hybrid cloud for blockchain technology can offer several benefits over a private cloud. Firstly, a hybrid cloud allows for greater scalability by enabling organizations to allocate resources between public and private clouds as required. This flexibility helps to optimize resource utilization and reduce infrastructure costs. Secondly, a hybrid cloud provides higher levels of security and privacy by allowing sensitive data to be stored on private clouds while enabling non-sensitive data to be stored on public clouds. This approach ensures better data integrity and availability, Thereby increasing trust and reducing the risk of cyber-attacks. Additionally, a hybrid cloud ensures better disaster recovery by allowing for quick data replication and recovery in case of a disaster. Overall, a hybrid cloud is a more efficient and cost-effective option for a blockchain-based model (suggested above) that requires the security of a private cloud and the flexibility of a public cloud. [16][17][18]

XXI. CONCLUSION

Using blockchain technology can be an effective way to prevent ransomware attacks as it provides secure backups, automated prevention measures, access controls, and secure communication channels. Its decentralized design makes it difficult for attackers to target a single point of failure. Additionally, blockchain technology guarantees data integrity and gives data owners control over their data through both distributed and centralized storage. Only authorized individuals can access the data.

Healthcare organizations can gain several advantages by integrating blockchain-based healthcare services with a hybrid cloud. This integration improves security, scalability, and flexibility while lowering costs and boosting the quality of healthcare services. With this approach, all hospitals and peers at the hospital level can collaborate and share data effortlessly and efficiently, irrespective of the blockchain networks they belong to. The resulting comprehensive and integrated healthcare system improves patient care and data management. Validity of Hypothesis: The potential benefits of blockchain technology in preventing ransomware attacks and integrating it with hybrid cloud for healthcare services seem plausible. Nonetheless, the actual implementation and effectiveness of these solutions may vary depending on various factors such as technology infrastructure, regulatory frameworks, and operational practices. Legal issues arise with the deployment of blockchain in healthcare. Assuring patient privacy, interoperability, and patient-centered care by adhering to Indian EHR standards is in line with international best practices for blockchain-based EHR development. By adhering to these guidelines, patient information can be protected and compatibility with other healthcare systems is guaranteed.

SUGGESTIONS

1. Organizations ought to invest in educating and training staff members on ransomware detection and avoidance.
2. To protect sensitive patient data and comply with applicable data protection laws, healthcare organizations should make sure that the necessary security measures are in place.
3. To securely store and manage patient medical records and to improve efficiency and lower costs for healthcare services, healthcare providers can investigate the use of blockchain technology linked with the hybrid cloud.
4. By integrating access restrictions, secure backups, automated preventative measures, and communication channel security, businesses can use blockchain technology to prevent ransomware attacks.
5. Organizations should be proactive in preserving patient data by staying up to date on new technologies, and they should think about using secure storage options.

SCOPE OF FUTURE RESEARCH

1. Due to a lack of resources, and time, the researcher was unable to research the below-mentioned elements, despite their high research potential. However, the reader is encouraged to do so if they so choose.
2. Investigating the use of smart contracts and other blockchain-based automation tools to improve patient outcomes and streamline healthcare procedures.
3. Examining how blockchain technology might help the pharmaceutical industry with supply chain management and drug tracking.

DECLARATION

I, Adesh Mukati, declare that the research paper titled "Blockchain Technology in Healthcare Services" submitted for publication in the *Indian Journal of Cryptography and Network Security (IJCNS)* is my original work.

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	To successfully carry out the research, the researcher gathered information from secondary sources, including books, law review journals, research papers, journal articles, and newspaper articles. The links to various sources are given in the reference section of this research article.
Authors Contributions	I am only the sole author of the article.

REFERENCES

1. Pandey P, and Litoriya R, 'Implementing healthcare services on a large scale: Challenges and remedies based on blockchain technology' (*ScienceDirect*, 15 January 2020) <https://www.sciencedirect.com /science/article/abs/pii/S2211883720300046> accessed 3 January 2023.
2. Barnagarwala T, 'Amid India's mega-push to digitise health records, AIIMS cyberattack comes as a wake-up call' *Scroll* (7 December 2022) <https://scroll.in/article/1039106/amid-indias-mega-push-to-digitise-health-records-aiims-cyberattack-comes-as-a-wake-up-call> accessed 4 January 2023.
3. IANS, 'AIIMS ransomware attack: Key patient data at risk of leak, sale on dark web' *ET Healthworld* (28 November 2022) <https://health.economictimes.indiatimes.com/news /hospitals/aiims-ransomware-attack-key-patient-data-at-risk-of-leak-sale-on-dark-web/95 820909#:~:text=The%20cyber%20attack%20on%20AIIMS,%22prepare%20for%20a%20negotiation%22> accessed 3 January 2023.
4. Thamrin A, and Xu H, 'Hierarchical Cloud-Based Consortium Blockchains for Healthcare Data Storage' (*IEEE*, 1 April 2022)

<https://ieeexplore.ieee.org/document/9741958> accessed 7 January 2023

5. Brodersen, and others, 'Blockchain: Securing a New Health Interoperability Experience' (*Semantic Scholar*, August 2016) <https://www.semanticscholar.org/paper/Blockchain%3A-Securing-a-New-Health-Interoperability-Brodersen/8b24dc9cffeca8cc276d3102f8a e17467c7 343b0> accessed 6 January 2023.
6. Zhuang Y and others, 'Generalizable Layered Blockchain Architecture for Health Care Applications: Development, Case Studies, and Evaluation' (*JMIR*, 27 July 2020) <https://www.jmir.org/2020/7/e19029/> accessed 5 January 2023. [CrossRef]
7. Yaga D and others, 'Blockchain Technology Overview' (*NIST*, October 2018) <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> accessed 15 January 2023.
8. Privacy Ninja, 'Hackers Are Actively Exploiting Password-Stealing Flaw in Zimbra' (6 August 2022) <https://www.privacy.com.sg/cybersecurity/hackers-are-actively-exploiting -password-stealing-flaw-in-zimbra/> accessed 5 January 2023.
9. HSE Board, 'Conti cyber-attack on the HSE' (*PWC*, 3 December 2021) <https://www. hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf> accessed 2 January 2023.
10. Ow B, 'Major Centralized Systems are Hacked Multiple Times a Year' (*Medium*, 30 October 2018) <https://medium.com/@AxelUnlimited/major-centralized-systems-are-hacked-multiple-times-a-year-9c2ad612462b> accessed 6 January 2023.
11. Thamer N and Alubady R, 'A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research' (*ResearchGate*, April 2021) <https://www.researchgate.net/publication/353859530_A_Survey_of_Ransomware_Attacks_for_Healthcare_Systems_Risks_Challenges_Solutions_and_Opportunity_of_Researc> accessed 1 January 2023. [CrossRef]
12. Sanmarchi F and others, 'Distributed Solutions for a Reliable Data-Driven Transformation of Healthcare Management and Research' (*Frontiersin*, 7 July 2021) <https://www.frontiersin.org/articles/10.3389/fpubh.2021.710462/full> accessed 5 January 2023. [CrossRef]
13. Weldon D, 'Centralized vs. decentralized data systems —which choice is best?' (*VentureBeat*, 12 September 2022) <https://venturebeat.com/data-infrastructure/centra lized-vs-decentralized-data-systems-which-choice-is-best/> accessed 13 January 2023.
14. Afraz N, 'Is blockchain a friend or foe in ransomware attacks?' (*Siliconrepublic*, 20 July 2021) <https://www.siliconrepublic.com/enterprise/blockchain-cybersecurity-nima-afraz> accessed 14 January 2023.
15. Molteni M, 'Moving Patient Data Is Messy, But Blockchain Is Here to Help' (*Wired*, 1 February 2017) <https://www.wired.com/2017/02/moving-patient-data-messy-blockchain -help/> accessed 29 January 2023.
16. Factioninc, 'Top 10 Advantages of a Hybrid Cloud Solution' (24 January 2022) <https://www.factioninc.com/blog/advantages-of-the-hybrid-cloud/> accessed 28 January 2023.
17. Koegler S, 'Check These Alternatives to Cloud Computing' (*CloudTech Brief*, 6 December 2021) <https://www.cloudtechbrief.com/index.php/cloudservices/item/7254-check-these-alternatives-to-cloud-computing> accessed 27 January 2023.
18. Crust Network, 'Crust Network Brings Decentralized Storage to Blockchains Through Chainlink' (*Medium*, 6 June 2022) <https://medium.com/crustnetwork/crust-network-brings-decentralized-storage-to-blockchains-through-chainlink-aaa15b27e29c> accessed 12 February 2023.
19. Singh V, 'AIIMS cyber-attack | Investigators asking E&Y about its audit of hospital's cyber systems' *TheHindu* (3 December 2022) <https://www.thehindu.com/news/national/aiims-cyber-attack-investigators-asking-ey-about-its-audit-of-hospitals-cyber-systems/article66 218762.ece> accessed 4 January 2023.
20. Paganini P, 'Flaws in Zimbra could allow to takeover webmail server of a targeted organization' *Security Affairs* (27 July 2021) <https://securityaffairs.co/120603/hacking /zimbra-vulnerabilities.html> accessed 5 January 2023.
21. Electronic Health Record (EHR) Standards for India, 2016, Ministry of Health and Family Welfare eHealth Section, Q-11011/3/2015-eGov.

AUTHORS PROFILE

Adesh Mukati is a 1st-year student of Master of Cyber Law and Information Security at NLIU, Bhopal, and completed his undergrad in Biochemistry from Govt. Motilal Vigyan Mahavidyalaya, Bhopal. He is a highly motivated individual who is diligently working towards securing a challenging position in a reputable organization. He aims to expand his learning, knowledge, and skills and further develop his professional capabilities. With a strong work ethic and dedication to his career, he is eager to make a valuable contribution to any organization that he joins.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/ or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.