Grenze International Journal of Engineering and Technology, Jan Issue

Secured Information System for Healthcare in Cloud with Dual Access Control using Blockchain

Vidhya R[1], Pathi T[2], Prabhanand S[3] and Ramakrishnan M[4]
[1-4]Sri Krishna College of Technology
E-Mail: vidhya.rathinasamy4@gmail.com, pathyraj179@gmail.com, 19tucs146@skct.edu.in, marankrishna1964@gmail.com

***Abstract*— It is crucial to implement security measures and to make sure that vulnerabilities are solved to completely safeguard the health services. To protect the exchange of EMRs between various organizations participating the adaptive healthcare system this research will explore such difficulties in more detail and place a greater emphasis on security issues. Four different types of smart contracts to overcome the security issues: Verifying the identity of the user, authorizing access, detecting misconduct, and revoking access. There are challenges regarding data sharing and access control brought up by the existing Electronic Medical Record (EMR) management system utilized by healthcare organizations. Dual Access Control Framework, a security and privacy management system for blockchain-based EMR, to allay these worries.**

***Index Terms*— EMR, electronic medical records, centralized blockchains, EHR Electronic health record self-Executing contracts, computerized transaction protocols, Elliptic curve cryptography.**

I. INTRODUCTION

By comparing a user's generated content to the data authorization server or in a database of legitimate user, authentication technology limits access to systems. Authentication by itself is insufficient to protect data. A further layer known as authorization is required, to consider if an individual should really be offered access to the info or perform the transaction they're attempting. Most security experts are aware of how important access control is to their company. On how access control should be used, nevertheless, many perspectives exist. In an environment that is fluid and devoid of defined limits, access control demands the establishment of enduring regulations.

Large databases that store data on servers made of cutting-edge hardware are used to do this. These servers can frequently be established by utilizing many computers, supplying the processing power and storage space required to enable more users to look at the database at one time. A spreadsheet or database may be available to anyone, but they are usually owned by a company and managed by a single person who has total control over their functionality and the data they contain.

Crowley contends that authentication by itself is woefully inadequate to safeguard data. Adding yet another layer known as authorization is required to determine whether A visitor should really be capable of accessing the information or execute the operation they are trying to carry out.

II. RELATED WORKS

Researchers suggested numerous strategies to increase the data's scalability and security in the cloud environment. According to J. Sun et al have proposed the system "The Electronic Health Record (EHR)". It frequently engages in cross-organizational or cross-domain collaboration for essential and excellent patient care [3]. Since cross-

Grenze ID: 01.GIJET.10.1.816

domain cooperation invariably entails the exchange and sharing of related sensitive and very confidential patient data, rigorousentrusting process design is required as a advises that new (N. Fatema et al.,2014). The delegation mechanism allows for and limits a bandingpartner's access rights. Patients won't use the EHR system unless they are assured that their health information will be used and disclosed properly (E. B. D. Hussein et al.,2017); this cannot be done without good access control and pass authentication (J. Sun et al.,2009). The delegated powers during the collaboration should be revocable at any point. When working together, sensitive patient data must be shared securely to ensure patient privacy. An electronic clinical recordthat would be encrypted is suggested in this work (L. J. Kish et al,2015).In addition to fundamental authenticated key agreement provided by the use of outsourcing methodology and the fundamental repudiation mechanism, our electronic clinical record system includes advanced techniques for fine-grained access restriction and termination on demand (R. S. Sandhu et al.,1994). There seem to be two kinds of entry monitoring systems that have beenemployed: attribute-based and needed access control (V. C. Hu et al.,2015).

The network hashes communications into a hash-based proof-of-work timestamps are created continuously, because of which a document cannot be altered without repeating the conclusive evidence. The largest line demonstrates this, it was the first to emerge from the largest CPU power pool and that the events happened in the order theywere observed (M. A. Khan et al,2018). Mankind's primary concern has always been health protection. Despiteplaying a crucial social function, present healthcare data management systems are cumbersome, inefficient, occasionally expensive, and prone to misunderstandings and human mistake (J. Priisalu et al,2017).By using blockchain technology as a platform, the medical chainproject appears to have the ability to set a new standard for monitoring health records in the healthcare industry (Rallies et al.,2017). According to Rallies et al, “For maintaining and storing registered patients' electronic health records (EHR), a novel approach based on a permissioned blockchain is suggested.”. This approach guarantees efficiency for both doctors and patients and, ideally, preserves faith in the public health system. It does so by ensuring openness and, more importantly, fixity, which are vital for secure administration and preservation (J. Priisalu et al.,2017).To implement widespread and reliable control of accession to Interconnected devices (S. Ravidas et al.,2019), For each subject-object pair, each ACC offers a single access control mechanism that carries out both confirmation of inactive access rights based on predeterminedpolicies and Validation of changing access through employing dynamic analysis (A. Ouaddah et al., 2017).

A. Difficulty Faced By Users

- Centralized data security
- Time constraint, Event driven approach.
- High cost, Privacy breaches.
- Existing system follows a centralized data storage of E-healthrecords, which makes it less scalable and difficult to maintain.
- Additionally, they are centralized and liable to a single spot ofcollapse.

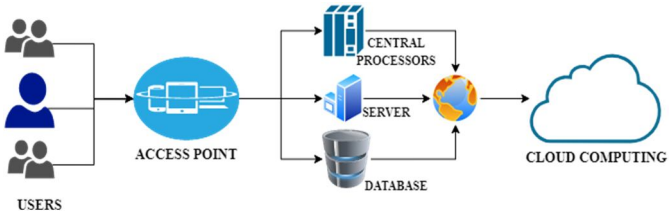

Figure 1 cloud computing architecture

III. System Model

To ensure the safe sharing of electronic clinical record between different stakeholders in the automated healthcare sector, the current approach intends to create a smart contracts-based user access framework, which are established over through the shared databases. To achieve this, we encourage the use of four distinct kinds of smart contracts: account identification, approval for entry, spotting of misconduct, and Denial of access. In this framework, the electronic clinical records are saved using cryptographic techniques in the cloud using Elliptic Curve Cryptography (ECC). Their congruent hashes aresimultaneously stored in blockchain. Using a private performanceevaluation.

Contrarily, the approach we propose considers the scenario of complete medical tracks, which primarily involves three distinct kinds of entries:Patients, hospitals, and smart medical technology with computational supervision made possible by the Internet of Things. We have begun utilizing cloud storage to prevent crowding and lower overhead on theblockchain network. In other words, the blockchain stores the relevantindex number and hash when an EMR is created, and it is encrypted and maintained in the cloud. The following benefit of the proposed system, because actions can be predefined, this autonomous behaviors grow thanks to smart contracts based on the blockchain. Such ideasare simple to combine, which has numerous advantages.

- Since its inception a decade ago, big data analytics has analyzed enormous amounts of data to give users a wealth of business insight.
- Comparative analysis of the data collected and kept in the cloud can give the user insightful information that can lead to improvedproductivity and financial success.
- The usage of the cloud minimizes latency, which can be important in specific use cases.
- The majority of these can aid in improving user and device data processing as well as service quality.

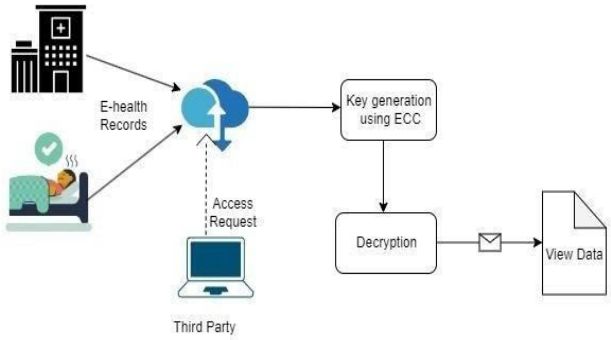

Figure 2 system architecture

A. E-Health Records

The next advancement in health care services that would improve patient- physician interactions is the adoption of electronic clinical records. Themetadata's accessibility and immediate nature will help doctors make more accurate diagnoses and treatments.

As an illustration, the EHR can improve patient care by

1. Increasing the fact of being accurate and readability of clinicalrecords to reduce the possibility of surgical mistakes.
2. Making the knowledge on health more broadly accessible, obviatingthe need for pointless testing, accelerating the pace of diagnosis, and enabling people to make conscious decisions.
3. Reducing clinical errors by making clinical records more precise andfurthermore understandable.

B. Access Control

A security method is known as approval for entry limits the access to resources in the environment of computation. It is a vital protection measure. that lessens risk to the organization or group. Logical and physical regulation on entering is both available. The ability to view information, system files, and computer networks is restricted using conceptual security controls. Organizations use the system of electronic entry management to monitor staff access to protected areas such as data centers and other restricted corporate areas. These systems use user credentials, access card readers, auditing, and reports. Some of the technologies used to restrict access to buildings and rooms include alarms and access control panels.

IV. Result Analysis

A secured information system for health care using a dual access control framework by blockchain can provide robust security by allowing access to sensitive patient data only to authorized personnel. The use of blockchain technology can ensure that the system's data is tamper-proof and secure, and the dual access control framework can add an additional layer of security by requiring two-factor authentication.

The analysis of such a system would typically involve assessing itseffectiveness in preventing unauthorized access, detecting, and responding to security breaches, and mitigating potential vulnerabilities. Some key metrics that could beused to evaluate the system's performance include:

Blockchain security: Blockchain technology uses cryptographic algorithms to secure data and prevent tampering. An effective blockchain-based system for health care should demonstrate a high level of security against data breaches, hacking attempts, and other security threats.

- *Authentication success rate*: This metric measures the percentage ofsuccessful logins by authorized personnel using the two-factor authentication system. A high authentication success rate indicates that the systemis functioning effectively, and legitimate users are being granted access to the system.
- *Unauthorized access attempts*: This metric measures the number of unsuccessful login attempts made by unauthorized personnel. A high number of unauthorized access attempts could indicate that the system is being targeted by malicious actors or that the user credentials are being compromised.
- *Breach detection and response time*: This metric measures the timeit takes for the system to detect a security breach and initiate a response. A fast response time is critical in preventing further data loss or damage.
- *Vulnerability assessment*: This involves regularly evaluating thesystem's security posture to identify potential vulnerabilities andprioritize remediation efforts.

Overall, an effective secured information system for health careusing a dual access control framework by blockchain should demonstrate a high level of security.

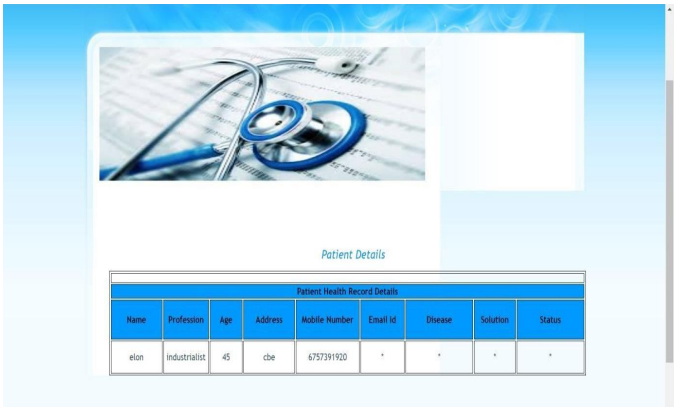

Figure 3 result page

V. STATISTICAL DATA

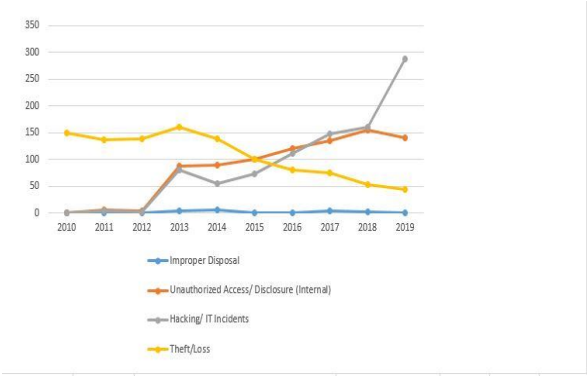

Figure 4 Graphical Presentation of Different Data Disclosure Types

According to the graph above, illegal access occurrences and hacking/IT incidents have increased in frequency while theft/loss and inappropriate disposal incidents have reduced. Notably, during the past few years, there has been a sharp rise in IT and hacking instances. The locations of information breaches and the sources from which sensitive health information has been exposed are covered in the sections that come next.

On the other hand, improper disposal and theft/loss have clearly decreased over the past four years. Only 257 theft/loss instances out of 1077 total incidents, or 23.86% of the total, were recorded in the last four years. Additionally, only 34 instances of waste that were inappropriate out of a total of 90 cases—or 37.77% of the total—were recorded in the previous four years. These findings demonstrate that the healthcare sector is far less negatively impacted by theft/loss and inappropriate disposal.

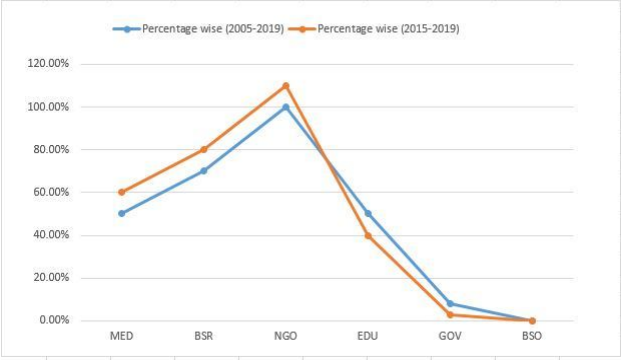

FIGURE 5 Representation of Data Breach Incidents.

The graph's slope in each sector has decreased in the second scenario (2015-2019), except for the MED sector, which was followed by the BSF sector, according to the figure. The graph shows that due to the important commercial value of electronic health records (E the healthcare sector is the main target of attackers.

VI. Future Scope

Future work proposes to combine the AES encryption mechanism withan innovative encryption methodology to address these problems. In this work, the owner of the data and PHR manager can securely swap their public keys and generate the secret by employing an ECC-DH keyexchange method. The following are this paper's main contributions.

Improve access permission by granting access to a variety of people sothat they can view various categories of files based on their PHR responsibilities.

VII. Discussion

The implementation of a secured information system for healthcare in the cloud with dual access control using blockchain technology represents a significant advancement in healthcare data management and security. In this section, we will discuss the key findings and implications of this system.

1. *Enhanced Security*: Blockchain technology provides an immutable and decentralized ledger for storing healthcare data, which significantly enhances security. With dual access control, only authorized personnel can access sensitive patient information, reducing the risk of data breaches.
2. *Data Integrity*: Blockchain ensures the integrity of healthcare data. Any changes made to the data are recorded in a transparent and tamper-proof manner, making it easy to track and verify the authenticity of records.
3. *Patient Privacy*: Dual access control ensures that both healthcare providers and patients have control over who can access their data. This empowers patients to maintain their privacy and control over their medical records.
4. *Interoperability:* The use of blockchain can improve interoperability among different healthcare systems.
5. *Reduced Costs*: Storing healthcare data in the cloud can reduce infrastructure costs for healthcare organizations.

VIII. Conclusion

In conclusion, the implementation of a secured information system for healthcare in the cloud with dual access control using blockchain technology offers a robust solution to the pressing challenges of data security and privacy in the healthcare industry. By leveraging blockchain's immutability and decentralization, along with dual access control mechanisms, this system not only ensures the confidentiality and integrity of patient data but also empowers patients to have greater control over their own health information.

Furthermore, the system aligns with regulatory requirements and provides a foundation for improved interoperability and data sharing among healthcare providers. While it represents a significant step forward, it's essential to consider the practical implementation challenges, such as the need for robust identity management and the integration of legacy systems.

In the future, as blockchain technology continues to evolve, it is likely that such systems will become even more sophisticated, offering healthcare organizations even greater security and efficiency in managing patient data.

Overall, this system holds great promise in revolutionizing healthcare data management in a secure, efficient, and patient-centric manner.

REFERENCES

[1] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," Computer Networks, vol. 112,

[2] N. Fatema and R. Brad, "Security requirements, counterattacks and projects in healthcare applications using wsns-a review," arXiv preprint arXiv:1406.1795, 2014.

[3] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, 2009.

[4] L. J. Kish and E. J. Topol, "Unpatients-why patients should own their medical data," Nature biotechnology, vol. 33, no. 9, p. 921, 2015.

[5] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in internet-of-things: A survey," Journal of Network and Computer Applications, vol. 144, pp. 79–101, 2019.

[6] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," ACM Transactions on Information and System Security (TISSEC), vol. 3, no. 2, pp. 85–106, 2000.

[7] R. S. Sandhu, "Role-based access control," in Advances in computers. Elsevier, 1998, vol. 46, pp. 237–286.

[8] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," Computer, vol. 48, no. 2, pp. 85–88, 2015.

[9] R. S. Sandhu and P. Samarati, "Access control: principle and practice," IEEE communications magazine, vol. 32, no. 9, pp. 40–48, 1994.

[10] E. B. D. Hussein and V. Frey, "A community-driven access control approach in distributed Iot environments," IEEE Communications Magazine, vol. 55, no. 3, pp. 146–153, 2017.

[11] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[12] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[13] "Blockchain momentum rallies healthcare," http://www.ibm.com/blogs/ blockchain/2017/01/blockchain- momentum-rallies-healthcare/, [Online; accessed 06-January-2017].

[14] J. Priisalu and R. Ottis, "Personal control of privacy and data: Estonian experience," Health and technology, vol. 7, no. 4, pp. 441– 451, 2017.

[15] A. Gumaei, M. M. Hassan, S. Huda, M. R. Hassan, D. Camacho, "Introduction to ethereum,"http://ethdocs.org/en/latest/introduction/ index.html, [Online].

[16] J. D. Ser, and G. Fortino, ''A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids,'' Appl. Soft Computer., vol. 96, Nov. 2020, Art. no. 106658, doi: 10.1016/j.asoc. 2020.106658

[17] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren, ''Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model,'' IEEE Trans. Ind. Inform at., vol. 16, no. 9, pp. 6154–6162, Sep. 2020, doi: 10.1109/TII.2020.2970074.

[18] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, ''Identifying cyber threats to mobile-IoT applications in edge computing paradigm,'' Elsevier Sci. Direct Future Gener. Comput. Syst., vol. 89, pp. 525–538,Dec.2018,doi:10.1016/j.future.2018.06.053.

[19] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, ''Cyberattacks detection in IoT-based smart city applications using machine learning techniques,'' Int. J. Environ. Res. Public Health, vol. 17, no. 24, p. 9347, Dec. 2020, doi: 10.3390/ijerph17249347.

[20] M. M. Hassan, S. Huda, S. Sharmeen, J. Abawajy, and G. Fortino, ''An adaptive trust boundary protection for IIoT networks using deep- learning feature-extraction based semi supervised model,'' IEEE Trans.Ind. in format., vol. 17, no. 4, pp. 2860– 2870, Apr. 2021, doi: 10.1109/TII.2020.3015026.

[21] M. M. Hassan, M. R. Hassan, S. Huda, and V. H. C. de Albuquerque, ''A robust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment,'' IEEE Internet Things J., vol. 8, no. 12, pp. 9611–9621, Jun. 2021, doi: 10.1109/JIOT.2020.3019225.

[22] A. Mohasseb, B. Aziz, J. Jung, and J. Lee, ''Predicting cybersecurity incidents using machine learning algorithms: A case study of Korean SMEs,'' in Proc. INSTICC, 2019, pp. 230–237, doi: 10.5220/ 0007309302300237. 71.

[23] Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, and M. Liu, ''Cloud with a chance of breach: Forecasting cyber security incidents,'' in Proc. 24th USENIX Secur. Symp., Washington, DC, USA, 2015, pp. 1009–1024.

[24] Guide to Cyber Threat Information Sharing, document NIST 800- 150, 2018, doi: 10.6028/NIST.SP.800-150.

[25] A. Yeboah-Ofori, S. Islam, and E. Yeboah-Boateng, ''Cyber threat intelligence for improving cyber supply chain security,'' in Proc. Int. Conf. Cyber Security. Internet Things (ICSIoT), May 2019, pp. 28–33, doi: 10.1109/ICSIoT47925.2019.00012.SS.S