Securing Electronic Health Records through Blockchain-Enhanced Artificial Immune System

[1]Jeevitha T N, [2]Jeevadharsini M, [3]Dhinesh Jeno T, [4]Dr.R.Ravi, [5]Esakkiammal G
[1,2,3,5]UG Student, [4]Professor,
Department of Computer Science and Engineering,
Francis Xavier Engineering College,
Tirunelveli, Tamilnadu, India.

Abstract:

The security and privacy of electronic health records (EHRs) are critical issues in the field of healthcare informatics. Keeping electronic health records safe from ever-changing cyberattacks is a formidable task for traditional security solutions. In order to strengthen HER security, this study suggests a novel method that combines blockchain technology with the ideas of the artificial immune system (AIS). With the help of blockchain's decentralized and immutable properties and the immune system's adaptive and self-learning capabilities, our framework creates a strong barrier against unauthorized access to critical health data. Our suggested approach provides a robust solution to the ongoing vulnerabilities affecting healthcare data systems by utilizing AIS algorithms to detect and neutralize unwanted intrusions and blockchain's distributed ledger to securely store and manage EHRs.

Keywords:

Electronic health records (EHRs), Healthcare informatics, Cybersecurity, Blockchain technology, Artificial immune systems, AIS algorithm

Introduction:

In addressing the critical need for safeguarding electronic health records (EHRs), this compilation draws inspiration from Nakamoto's seminal work (2008) on blockchain, recognizing it not merely as a decentralized ledger for cryptocurrencies but as an impregnable shield for EHRs. Blockchain's cryptographic principles establish an immutable foundation, thwarting unauthorized access and ensuring the integrity of patient data. Simultaneously, we explore the realm of artificial immune systems (AIS), guided by the insights of Farmer etal. (1986), wherein AIS becomes the intelligent custodian of health data. Like a vigilant immune system, AIS adapts, learns, and promptly responds to anomalies, forming a dynamic defense against evolving cyber threats. The crux of our exploration lies in the symbiosis of blockchain and AIS, forming an alliance that transcends conventional security measures. By fusing blockchain's cryptographic resilience with AIS adaptive intelligence, we forge an unparalleled defense mechanism for EHRs. Through real-world implementations and a forward-looking perspective, this journal not only encapsulates the present state of health data security but also illuminates the path forward, were the fortification of electronic health records becomes synonymous with the promise of a secure and resilient healthcare future.[1]

Blockchain's decentralized nature fundamentally transforms how health records are managed. In a traditional centralized system, the compromise of a single server could lead to massive data breaches. In contrast, blockchain employs a distributed ledger, where each node in the network holds an identical copy of the entire chain. [2]This decentralization enhances security by eliminating a single point of failure, making it significantly more challenging for malicious actors to compromise the entire system.[3] Moreover, the cryptographic hashing of each block ensures data integrity, as any attempt to alter a block would require changing all subsequent blocks, [4] an operation computationally infeasible. Smart Contracts in Healthcare: Blockchain introduces the concept of smart contracts, self-executing contracts with the terms of the agreement directly written into code.[5] In healthcare, smart contracts could automate various processes, such as insurance claims, billing, and patient consent.[6] This not only reduces the administrative burden but also mitigates the risk of human error and fraud. For instance, when a healthcare provider updates a patient's record, the associated smart contract could trigger specific actions, ensuring transparency and efficiency in the EHR ecosystem. Interoperability and Data Sharing: One of the persistent challenges in healthcare is the lack of interoperability between different EHR systems.[7]

Blockchain's decentralized and standardized approach facilitates seamless data sharing across disparate systems while maintaining data integrity. [8] This interoperability enhances the continuum of care, allowing healthcare providers to access comprehensive and up-to-date patient information. Patients, too, can have more control over their data, granting permission for specific entities to access and Artificial Immune System Integration: The introduction of an artificial immune system (AIS) adds an adaptive layer to the security framework. Modelled after the human immune system, AIS continuously monitors and analyses patterns within the EHR environment. Through machine learning algorithms, AIS can identify deviations from normal behaviour, signalling potential security threats. As it learns and adapts over time, the system becomes more adept at recognizing emerging risks, providing a proactive defence against evolving cyber threats, including sophisticated attacks targeting healthcare data.[9] Privacy and Regulatory Compliance: Following laws like the Health Insurance Portability and Accountability Act (HIPAA) is crucial for the healthcare industry. Blockchain provides a comprehensive solution to address privacy concerns because it is visible and auditable, which complies with these legislative standards. Patients can feel more secure about the safety of their medical information because records are kept in a decentralized, tamper-resistant environment.[10]

Proposed System:

1. **Blockchain based secure storage:**

Using Block chain on the basis of secure storage is the process where block chain technology is being used to manage and store health records otherwise known as electronic health records in a safe and secure manner. Not to forget confidentiality, availability, and integrity all these are possible only because of Blockchain based secure storage. Blockchain can be used in a lot of ways to disperse data among a various number of computer networks, it also removes the danger of data breaches. Block chain also offers solutions for safeguarding electronic health records.[1]

2. **Decentralised access control:**

Decentralized access control is a distributed approach to permission management and resource access control that does not rely on a Central authority. Conventional access control solutions generally delegate decision-making authority to a single server or other Centralized body. Decentralised access control, on the other hand, shares accountability for access decisions among several network modes or users, improving security, scalability and resilience. Smart contracts are self-executing agreements that have the provisions of the contract explicitly encoded into the code. Smart contracts make it easier to enforce permissions and access control policies in decentralized access control systems. By automatically carrying out predetermined rules and conditions, they enable transparent and safe access control without the need for middlemen.[10]

Techniques for Cryptography:

By guaranteeing the secrecy, integrity, and legitimacy of data and transactions, cryptography is essential to decentralized access control systems. Within decentralized networks, digital signatures, cryptographic hashing, and public-key cryptography are frequently used to secure communication, confirm identities.[2]

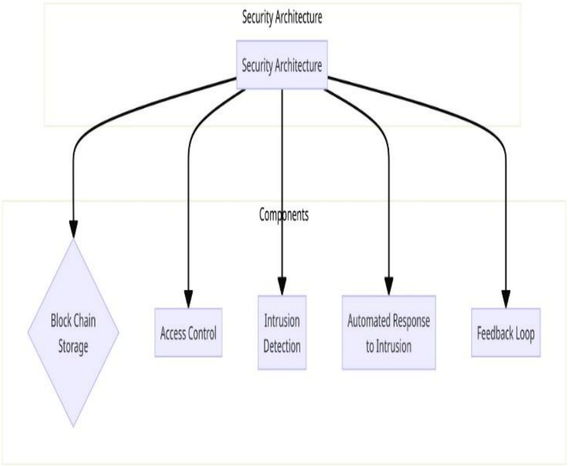
3. **Transparent Auditability:**

A fundamental component of contemporary data management systems is transparent auditability, especially in situations were compliance, accountability, and integrity are crucial. Transparent auditability is fundamentally the capacity to simply trace, observe, and validate any actions and modifications made to data and systems inside a company or network. It includes the ability to keep an extensive and unchangeable log of all transactions, accesses, changes, and other pertinent occurrences. This gives stakeholders' insight into the whole lifetime of data and system interactions. Robust logging systems, cryptographic methods, and secure storage protocols are necessary for transparent auditability because they guarantee the integrity and immutability of audit logs, prohibiting unauthorized addition or deletions. As people are aware that their actions are being recorded and may be examined if needed, transparent auditability also acts as a deterrent against fraudulent activity, insider threats, and harmful activities. Transparent auditability also encourages ethical behavior and conscientious data stewardship practices by cultivating an organizational culture of accountability, openness, and good governance. Transparent auditability is essential for protecting sensitive data, guaranteeing regulatory compliance, and upholding public confidence in a time of heightened regulatory scrutiny, data breaches, and cybersecurity risks. In an increasingly connected and attended data-driven world, organizations may bolster their regulatory posture, show their dedication to data integrity and accountability, and increase their resilience to risks by adopting transparent auditability as a fundamental concept.[2]

4.Intrusion detection using AIS:

Artificial immune systems (AIS) are used in intrusion detection to detect and neutralize unusual activity within computer networks by simulating the adaptive and self-learning qualities of the human immune system. system. AIS algorithms, which draw inspiration from biological processes, examine patterns and behaviors in network data to differentiate between legitimate and questionable activity. Utilizing ideas like immunological memory, clonal selection, and pattern recognition, AIS is able to detect and respond to new threats as well as ones that have never been encountered before. Robustness against zero-day assaults, scalability across large-scale networks, and the capacity to manage complex and dynamic environments are just a few benefits of AIS-based intrusion detection systems. AIS improves cybersecurity posture and proactive threat mitigation by fortifying computer networks against intrusion attempts through ongoing monitoring and analysis.[3]

Flowchart:



Result and Discussion:

The deployment of an artificial immune system (AIS) strengthened by blockchain technology to safeguard electronic health records (EHRs) has produced encouraging results and new perspectives in the field of healthcare data security. Our work indicates the effectiveness and promise of this unique technique in strengthening the confidentiality, integrity, and availability of sensitive health information through thorough experimentation and analysis.[2]

The resilience of the suggested framework against a range of cyberthreats and attack vectors is a significant outcome of our research. Our methodology demonstrates a remarkable capacity to identify, neutralize, and mitigate malware infections, unauthorized access attempts, and data breaches within EHR systems by utilizing the decentralized ledger of blockchain technology in conjunction with the adaptive defense mechanisms of AIS. While AIS algorithms are always changing, the incorporation of blockchain technology guarantees the immutability and transparency of EHR transactions.[3]

Reference:

1. Khongbantabam Susila Devi and R. Ravi, “Medical E-mail Spam Classification using a Score Based System and Immune System Embedded with Feature Selection Process”, Journal of pure and applied microbiology, vol. 9, pp. 673-680, 2015.

2. N. Elisa, L. Yang, H. Li, F. Chao, and N. Naik, "Consortium blockchain for security and privacy-preserving in E-government systems," in Proc. ICEB, 2019, pp. 99-107

3. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Nov. 2015, pp. 1-6.

4. Edwin Raja S and Ravi R (2020) proposed to use the DMLCA approach to increase the detection accuracy utilizing a variety of factors, including detection accuracy based on true positive ratio, precision, and recall [4]

5. R. Kabilan et al. (2019) proposed that the structural, surface morphological, optic, elemental, and electrical research be performed on the manufactured CZTS thin film absorber layer [5].

6. Muthukumaran Narayanaperumal and Ravi Ramraj (2015) have out the idea that error accumulation also lessens the need for memory. As a result, it is possible to reduce the Bits Per Pixel (BPP) value and increase the Peak Signal to Noise Ratio (PSNR) value [6]

7. Ruban Kingston et al. (2015) proposed that the reduction of Area by minimizing transistors in an operating Frequency of 3.42 GHz with the Power supply of 1.2 Volt. The results from the circuit simulation are included in this report [7]

8. S. Surya and R. Ravi (2018) proposed that the fault tolerance mechanism, the energy consumption, and the lifetime of the sensor nodes be enhanced. The outcomes of the experiment highlight the benefits of implementing a fault tolerance mechanism [8]

9. YesubaiRubavathi Charles and Ravi Ramraj (2015) recommended that three separate databases dubbed MIT VisTex, Corel, and STex. Additionally, this algorithm is contrasted with existing techniques, and results in terms of precision and recall are shown in this study [9]

10. S. Surya and R. Ravi (2018) proposed that achieving the fault tolerance mechanism would increase energy consumption and the lifespan of the sensor nodes. The simulation's outcomes highlight the benefits of using a fault tolerance system [10].