Research Article

Volume-1 | Issue-1| Jan-Jun-2024|

JOURNAL OF
Information Technology and Cryptography
Double Blind Peer Reviewed Journal
DOI: https://doi.org/10.48001/JoITC

E-Health Privacy and Security through ECC, SHA-256, and Multi-Authority Approaches

Ensteih Silvia[1*], Mohd Tajuddin[1]

[1]Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

[*]Corresponding Author's Email: ensteihs@gmail.com

ARTICLE HISTORY:

Received: 14th Jan, 2024
Revised: 1st Feb, 2024
Accepted: 12th Feb, 2024
Published: 21st Feb, 2024

KEYWORDS:

Ciphertext policy attribute-based encryption, Cloud computing, E-Health, ECC (Elliptic Curve Cryptography), Multi-authority, SHA-256

ABSTRACT: The rapid digitization of healthcare services has led to the proliferation of electronic health (E-Health) systems, providing convenience and improved patient care. However, the increasing use of E-Health platforms also raises concerns about the privacy and security of sensitive medical information. This review paper explores the challenges surrounding E-Health privacy and security and presents a comprehensive approach to addressing these concerns through the implementation of Elliptic Curve Cryptography (ECC), Secure Hash Algorithm 256 (SHA-256), and multi-authority schemes. The synergistic application of these cryptographic techniques not only fortifies the protection of patient data but also establishes a robust framework for secure data sharing and management in E-Health systems.

1. INTRODUCTION

The integration of technology in healthcare, known as E-Health, has revolutionized the medical landscape. However, with increased data digitization and sharing, concerns about privacy breaches and data security have arisen. This paper delves into the critical issues associated with E-Health privacy and security and proposes a comprehensive solution by leveraging ECC, SHA-256, and multi-authority techniques. Due to the interconnection of everything in today's society, IoT is being widely adopted in the field of e-health, creating new healthcare facilities and services. But there are still significant challenges in strengthening security and protecting patient privacy. Although several models and methods for preserving security and privacy have been put forth, they are frequently vulnerable to adversarial attacks. Our goal is to increase their security while making the final system lightweight and able to run on low-power, memory-constrained devices. Healthcare providers are utilizing this trend to offer electronic health records (E-Health Records) that allows the data from the patients to be managed in a robust and scalable manner as cloud computing environments grow more adaptable and accessible. Despite these advantages, E-Health Records include extremely sensitive data, raising serious concerns about security and privacy. To solve this problem, they have created and implemented a secure, granular access control system with access policy updates for outsourced E-Health Records. Ciphertext policy attribute-based encryption (CP-ABE) is the basis of the plan we have suggested.

E-Health Privacy and Security Challenges: This section identifies key challenges such as unauthorized access, data

breaches, patient confidentiality breaches, and system vulnerabilities. The need for advanced security measures to protect sensitive health data is emphasized.

Cryptographic Fundamentals: An overview of Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm 256 (SHA-256) is provided. ECC's efficiency in ensuring data confidentiality and integrity and SHA-256's robust hashing capabilities are highlighted.

ECC and SHA-256 Implementation in E-Health: Detailing the integration of ECC and SHA-256 in E-Health systems, this section explains how ECC's asymmetric encryption can safeguard patient data during transmission, while SHA-256's hashing ensures the integrity of stored information. The efficiency gains achieved by utilizing these cryptographic tools are discussed.

Multi-Authority Access Control: Introducing the concept of multi-authority schemes, this section discusses how multiple entities collaboratively manage access control, enhancing security in data sharing. By combining ECC, SHA-256, and multi-authority models, fine-grained access policies can be enforced, allowing controlled sharing of patient data among authorized parties

Implementation Challenges and Mitigations: Potential implementation challenges, including computational overhead and interoperability, are discussed. Mitigation strategies such as hardware acceleration, optimization techniques, and standardized protocols are proposed.

2. RELATED WORK

The study employed a systematic approach encompassing four distinct research strategies (Fernandez et al., 2013). To begin, the initial strategy involved the utilization of relevant keywords pertaining to healthcare systems, such as ("electronic health records" or "healthcare system"), coupled with information security keywords encompassing authentication, authorization, and access control. This initial approach yielded a considerable dataset of 1756 articles. In the second research strategy, a pruning process was enacted to refine the dataset further. By meticulously examining abstracts and titles, the results were whittled down, resulting in a more focused subset. This phase yielded a total of 226 research papers that formed the basis for deeper investigation. Subsequently, the third strategy involved a comprehensive analysis of the identified 226 research papers. This in-depth examination aimed to ascertain the originality and pertinence of each paper. By delving into the entire content of these papers, the researchers were able to distill their research even further, resulting in a subset of 126 research papers. These refined research papers, stemming from diverse years of publication, were then utilized to construct a robust foundation for the study's exploration of various healthcare systems and their corresponding application studies. Moreover, to ensure that the research remained up-to-date, the researchers established automated alerts within search engines. This proactive measure enabled ongoing communication and the prompt identification of newly published research, ensuring that the study's insights remained current and relevant.

A novel approach known as E-SAP (Efficient-Strong Authentication Protocol) is introduced (Kumar et al., 2012). This protocol addresses the critical need for robust user authentication within healthcare applications that employ wireless medical sensor networks (WMSNs). By incorporating a two-factor security mechanism, E-SAP establishes a resilient user authentication process while ensuring confidentiality and facilitating the establishment of secure session keys for healthcare applications that rely on WMSNs. An important highlight is that E-SAP significantly enhances the provision of security services, optimizing computation and communication costs in comparison to existing protocols in the same domain. Through a rigorous analysis, which includes the application of the BAN logic authentication model, the researchers demonstrate that E-SAP effectively attains its stated security objectives. Notably, E-SAP successfully defends against a variety of commonly encountered attack vectors, further attesting to its robust security architecture. This protocol proves to be particularly well-suited for diverse healthcare settings such as hospitals, homecare environments, and clinics that harness wireless medical sensors. The distinct advantage of E-SAP lies in its ability to offer a multifaceted security approach that addresses the specific demands of healthcare applications utilizing WMSNs. By securing user authentication, confidentiality, and session key establishment, E-SAP contributes to enhancing the overall security landscape in these critical healthcare contexts.

The authors present a fresh approach to lightweight authentication tailored for E-health applications (Almulhim & Zaman, 2013). The scheme introduced offers a streamlined yet robust method to authenticate both the Base Station (BS) sensors and the Base Station itself, thereby ensuring the secure collection of health-related data. Central to their approach is the utilization of Keyed-Hash Message Authentication (HMAC) and nonces, strategically employed to guarantee the integrity of authentication exchanges. This innovative scheme not only emphasizes security but also addresses energy efficiency concerns. By employing authentication methods that are mindful of energy consumption, the proposed scheme aligns with the demands of resource-constrained environments. Moreover, the scheme culminates in the establishment of a session key between the BS sensors and the Base Station, adding an additional layer of security to the communication process. The authors underscore the reliability of their approach through a comprehensive security analysis and performance evaluation. The results gleaned from their assessment validate the scheme's

DOI: https://doi.org/10.48001/JoITC.2023.119-13

efficacy in conserving energy resources. Additionally, the scheme exhibits a commendable resistance against a spectrum of potential attack vectors.

The ESEMR framework encompasses several integral components, including an ECC integration unit, a smart card, a terminal device, and a cloud database (Tsai et al., 2016). Within this architecture, the cloud database serves as a repository for public keys, initial parameters such as Gs for hospital staff, and Electronic Medical Records (EMRs) for patients. In parallel, the smart card retains an encryption/decryption key designed exclusively for authorized hospital personnel. For individuals with authorization, the process commences as they insert their smart card into the ECC integration unit, which can be connected to a portable device or personal computer. After inputting their unique key, the ECC integration unit grants access. Subsequently, users can proceed to retrieve or upload data from or to the cloud database. Encryption/ decryption circuits integrated within the ECC integration unit facilitate these actions. Concurrently, a terminal device, which may be a personal computer or portable device, aids in the input and display of patients' medical data. The ESEMR system introduces a strategic solution to ensure the secure and expedited transmission of health information over wireless networks. This approach harnesses the inherent security benefits of the ECC security scheme to effectively encrypt Electronic Medical Records (EMRs). Core elements of the ESEMR system encompass an ECC encryption/decryption chip, a Zigbee wireless network, a smart card reader, and a USB controller. Collectively, these components empower users to access cloud-stored data via smart cards and the ECC integration unit. Central to the appeal of the proposed system is its adaptability across diverse platforms. The robust security features facilitated by ECC are harmoniously balanced with efficient utilization of hardware resources. Consequently, this framework not only ensures data security but also extends the convenience of cloud-based EMR exchange. Distinct from many contemporary EMR exchange systems, the focus here transcends mere EMR access and extends to encompass the secure exchange of medical information.

The role of wearable and portable systems emerges as pivotal in facilitating the transition toward proactive and economically viable healthcare solutions (Lee et al., 2014). This work introduces a secure key management scheme, rooted in elliptic curve cryptography (ECC), tailored for integration into healthcare systems. The scheme is thoughtfully structured across three distinct phases: setup, registration, and verification, culminating in the critical exchange of cryptographic keys. While acknowledging the significance of this contribution, certain aspects require further development to enhance the feasibility of continuous monitoring systems. This entails augmenting the existing scheme with additional security mechanisms. To fortify the overall system's authentication, for instance, one could consider integrating symmetric algorithms such as DES or AES. These algorithms, characterized by their simplicity and computational efficiency, could provide a more robust layer of security. It is important to note that while symmetric cryptography is advantageous in terms of simplicity and computational efficiency, it does bring about challenges in terms of effective key management. Moreover, a key consideration lies in the computational capabilities of sensor devices within the healthcare system. These devices must possess the requisite computational power to effectively execute data encryption procedures for safeguarding patient information. As part of this process, the encrypted data is transformed into ciphertext, which is subsequently securely stored within designated data repositories, ensuring the confidentiality and integrity of sensitive patient data.

The paper introduces VAHAK, an innovative secure blockchain-based delivery scheme designed for outdoor healthcare supplies facilitated by Unmanned Aerial Vehicles (UAVs) (Gupta et al., 2020). This solution addresses the challenges inherent in conventional UAV systems operating on blockchain technology. By harnessing the potential of External Secure Channels (ESC), InterPlanetary File System (IPFS), and 5G-Trust Infrastructure (5G-TI), the authors intricately tackle issues such as latency, network bandwidth constraints, and storage expenses. A pivotal facet of this work lies in the fusion of these technologies to achieve a synergetic effect. Through the amalgamation of ESC, IPFS, and 5G-TI, the scheme ensures paramount attributes, including heightened security, privacy preservation, minimal latency, exceptional reliability, and cost-effective data storage. An intriguing aspect is the deployment of Smart Contracts (SCs) through the Remix Integrated Development Environment (IDE) to offer transparency and insight into the block information. The paper culminates in a comparative analysis, wherein VAHAK's performance is evaluated against traditional blockchain-based systems within the context of an LTE-Advanced communication network. Metrics such as latency, scalability, and network bandwidth are assessed to showcase the advantages of VAHAK's approach. As the authors steer toward future endeavours, a central focus revolves around augmenting the performance of the priority queue. This involves the integration of Artificial Intelligence (AI) techniques to mitigate challenges like the partial convoy effect. This forward-looking perspective underscores the commitment to continuous improvement and innovation within the realm of blockchain-enabled healthcare supply delivery systems.

The paper delves into the realm of transaction and Access Management through Blockchain in healthcare systems (Chakraborty et al., 2019). In the context of the burgeoning volume of patient-generated data, the demand for secure

DOI: https://doi.org/10.48001/JoITC.2023.119-13

protocols to manage and process this data emerges as a necessity. Particularly, in scenarios where multiple stakeholders are involved in the data lifecycle, a crucial component—access management—needs implementation, a role well-suited for the capabilities of the Blockchain Network. The architectural blueprint laid out in this study introduces the integration of two pivotal blockchain networks: the Personal Health Care (PHC) Blockchain and the External Record Management (ERM) Blockchain. The PHC Blockchain is primarily governed by the patient, serving as the repository for data harnessed from personal wearable devices. This data is further granted access to healthcare professionals, enabling informed medical decisions and tailored treatments. The flow of data from wearable devices to an external cloud database is closely monitored by the blockchain network, enhancing security and accountability. Parallelly, the ERM Blockchain takes on the responsibility of managing data generated during patient visits to healthcare providers. This encompassing ledger encompasses diverse information, encompassing healthcare center records, pharmacy bills, medical test reports, prescriptions, and even image data. To maintain the integrity of this information, data is meticulously appended to the blockchain through a "Proof of Stake" algorithm, with consensus among all stakeholders within the network.

This paper undertakes a comprehensive exploration of the current state of blockchain implementation and integration within the healthcare sector (Bodeis et al., 2021). Collecting a total of seven papers from the ACM Digital Library, the authors undertake a meticulous categorization of these works, segregating them into three distinct groups: adoption, implementation, and integration. The review illuminates that the landscape of blockchain adoption within healthcare has been extensively scrutinized. Notably, the authors highlight their significant contribution in offering an updated and organized classification of existing research within this dynamic domain. However, their overarching observation underscores the potential for more extensive investigation into the domains of implementing and integrating blockchain into healthcare systems. From their vantage point, the authors underscore the necessity for continued research efforts in the realm of blockchain technology. They advocate for the cultivation of deeper insights before the healthcare industry can seamlessly embrace advanced levels of acceptance, implementation, and integration. This perspective serves as an impetus for further scholarly endeavours, catalysing the momentum required to elevate the application of blockchain technology within the healthcare sector.

The authors introduce a groundbreaking distributed storage model that significantly streamlines the blockchain network (Kumar et al., 2020). In this innovative paradigm, medical records are not stored directly in the blockchain; instead, they adopt an approach where only the content-addressed hash of these records is stored. This strategic maneuver effectively curtails the network's size. The pivotal role of the IPFS distributed file storage system comes into play here, serving as the repository for these medical records' content. In line with this methodology, a proof-of-work consensus mechanism is employed for the validation of transactions and the creation of blocks within the blockchain network. What sets this approach apart is the localized mining procedure, which bolsters scalability. This mining procedure plays an instrumental role in ensuring the network's expansion remains manageable. The core of this framework revolves around a blockchain-based distributed off-chain storage model, earmarked for patient diagnostic reports. These reports are seamlessly accommodated within the IPFS distributed file storage system. This storage model, underscored by immutability and content-addressability, aligns harmoniously with the overarching goal of patient report privacy. The authors break down their framework into three distinct modules, each with a dedicated purpose. The data upload module empowers healthcare providers to input patient details via a user-friendly Web User Interface (Web-UI). Following this step, the mining process is executed to validate transactions and maintain network coherence. Ultimately, to ensure the utmost privacy for patient diagnostic reports, a hash-based data storage mechanism is harnessed.

The authors present an innovative framework that integrates blockchain into Personalized Healthcare Systems (PHS) through the application of the Artificial Clinical Practice (ACP) approach (Wang et al., 2018). This approach demonstrates a novel amalgamation of artificial system modeling, computational experimentation, and parallel execution with actual healthcare scenarios. At its core, PHS employs artificial system modeling to emulate real-world healthcare dynamics. This modeling enables the simulation and representation of diverse healthcare scenarios. Subsequently, the framework engages in computational experiments to train and evaluate different disease diagnosis and treatment strategies. By establishing a parallel execution between actual healthcare scenarios and simulated ACP-based systems, the framework achieves a remarkable capability—accurate prediction and guidance for disease diagnoses and treatments. Furthermore, the authors delve into the exploration of integrating emerging blockchain technology into the healthcare sector. The study showcases the initial prototype system named PGDTS, which embodies the proposed parallel healthcare framework. This prototype has been successfully implemented in China, signifying the feasibility of the approach. Anticipating the need for enhanced integrity, scalability, and security, the authors advocate for the establishment of a consortium blockchain. This blockchain would encompass various stakeholders such as patients, hospitals, and health bureaus.

DOI: https://doi.org/10.48001/JoITC.2023.119-13

This collective effort holds the potential to amplify the reliability and security of the PHS.

The literature survey highlights the importance of robust encryption in securing E-Health Records. The integration of Elliptic Curve Cryptography and SHA-256 in EHR systems has exhibited encouraging outcomes in providing secure data transmission, storage, and integrity verification. The utilization of ECC's small key size and SHA-256's resistance to collisions make them well-suited for safeguarding sensitive medical information in EHR systems. However, further research and real-world implementation studies are necessary to validate and optimize the efficiency and scalability of this cryptographic approach in E-Health Record systems.

3. CONCLUSION

Throughout the research, there is a strong emphasis on user privacy and data security. The ECC and SHA-256 encryption algorithms, combined with the tamper-proof nature of Blockchain, have safeguarded sensitive patient medical information from unauthorized access and malicious attacks by combining the power of ECC, SHA-256, and multi-authority mechanisms, E-Health systems can establish a formidable defence against privacy breaches and unauthorized access. This review paper emphasizes the importance of safeguarding patient data and provides a comprehensive roadmap for implementing a secure and privacy-preserving E-Health ecosystem. To sum up, the research is based on novel integration of ECC, SHA-256, and user-defined Blockchain technology has resulted in an advanced, secure, and privacy-centric E-Health Record system that harbours substantial promise for revolutionizing the healthcare industry. By safeguarding patient data, enabling efficient access, and ensuring tamper-proof data storage, the EHR system stands as a reliable and invaluable asset in modern healthcare practice.

As future work, the project aims to explore scalability and interoperability aspects to accommodate a growing number of users and guarantee smooth incorporation into current healthcare infrastructures. A result represents the ultimate outcome of actions or events, expressed either qualitatively or quantitatively. Multi authority access has been effectively delivered for maintaining confidentiality of the patient files. Performance analysis involves operational examination, focusing on establishing fundamental quantitative relationships between various performance metrics.

REFERENCES

Almulhim, M., & Zaman, N. (2018, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In *2018 20th International Conference on Advanced Communication Technology (ICACT)* (pp. 481-487). IEEE. https://doi.org/10.23919/ICACT.2018.8323802.

Bodeis, W., & Corser, G. P. (2021, March). Blockchain adoption, implementation and integration in healthcare application systems. In *SoutheastCon 2021* (pp. 1-3). IEEE. https://doi.org/10.1109/SoutheastCon45413.2021.9401885.

Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 260-264). IEEE. https://doi.org/10.23919/ICACT.2019.8701983.

Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. A. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541-562. https://doi.org/10.1016/j.jbi.2012.12.003.

Gupta, R., Shukla, A., Mehta, P., Bhattacharya, P., Tanwar, S., Tyagi, S., & Kumar, N. (2020, July). VAHAK: A blockchain-based outdoor delivery scheme using UAV for healthcare 4.0 services. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 255-260). IEEE. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162738.

Kumar, P., Lee, S. G., & Lee, H. J. (2012). E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors*, *12*(2), 1625-1647. https://doi.org/10.3390/s120201625.

Kumar, R., Marchang, N., & Tripathi, R. (2020, January). Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In *2020 International Conference on Communication Systems & Networks (COMSNETS)* (pp. 1-5). IEEE. https://doi.org/10.1109/COMSNETS48256.2020.9027313.

Lee, Y. S., Alasaarela, E., & Lee, H. (2014, February). Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system. In *The International Conference on Information Networking 2014 (ICOIN2014)* (pp. 453-457). IEEE. https://doi.org/10.1109/ICOIN.2014.6799723.

Tsai, K. L., Leu, F. Y., & Tan, J. S. (2016). An ECC-based secure EMR transmission system with data leakage prevention scheme. *International Journal of Computer Mathematics*, *93*(2), 367-383. https://doi.org/10.1080/00207160.2014.955482.

Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., ... & Wang, F. Y. (2018). Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Transactions on Computational Social Systems*, *5*(4), 942-950. https://doi.org/10.1109/TCSS.2018.2865526.

DOI: https://doi.org/10.48001/JoITC.2023.119-13