Grenze International Journal of Engineering and Technology, June Issue

Cyber-Secure Framework for the Insecure Designs in Healthcare Industry

Nijatulllah Mansoor[1] and Sandeep J[2]
[1]Research Scholar, Department of computer science, CHRIST (Deemed to be University), Bangalore, India
Email: Nijatullah.nijatullah@res.christuniversity.in
[2]Assistant Professor, Department of computer science, CHRIST (Deemed to be University), Bangalore, India
Email: Sandeep.j@christuniversity.in

***Abstract*— Sensitive data protection has been a top priority in the healthcare industry. This has led to the investigation of safe data storage and transaction. Despite various attempts to address this issue, data breaches continue to plague the healthcare industry. This study aims to investigate prevalent storage practices and security methodologies in the healthcare, recognizing the need for a robust framework. The work further extends with design of new security framework for healthcare industry. This framework identifies critical data and implement measures to prevent unauthorized access and data tempering. The industrial hype towards the implementation of adaptive machine learning craves the need for hybrid machine learning approaches to be adapted in the cyber secure framework. In order to improve security and confidentiality in the healthcare sector. Blockchain is used in the proposed cyber secure framework promising integrity of data with the features of immutability. This proposal aims to provide a comprehensive solution to the ongoing problem of protecting medical data.**

***Index Terms*— Cyber Security, insecure design, cleartext storage, sensitive data, blockchain and machine learning.**

I. INTRODUCTION

In today's interconnected digital landscape, the importance of cybersecurity cannot be overstated. As our reliance on technology deepens, the potential threats to our data, privacy, and critical infrastructure grow exponentially. Cybersecurity measures are essential to safeguard sensitive information, prevent unauthorized access, and ensure the continuity of operations for individuals, businesses, and governments alike. The ever-evolving landscape of web threats and vulnerabilities poses significant challenges to digital security. Recent statistics reveal an alarming increase in data breaches, ransomware attacks, and identity theft incidents. As technology advances, so do the techniques employed by cybercriminals, with the potential for more sophisticated and targeted attacks in the future. Cybersecurity ventures predicts that the expenses associated with global cybercrime will experience a 15% annual increase for the upcoming three years. Figure 1 shows the trajectory which is projected to result in a global cost of \$8.7 trillion USD for the current year (2023) and a yearly total of \$10.5 trillion USD by 2025. This growth contrasts with the \$3 trillion USD figure recorded in 2015. Given the critical nature and heightened vulnerability of healthcare data to cyber-attacks, Cybersecurity Ventures anticipates a robust 15% annual growth in the global healthcare cybersecurity market, projecting its value to reach \$125 billion USD by 2025. Furthermore, IBM's data underscores this concern, revealing a notable escalation in the average cost of healthcare data breaches to \$10.10

Grenze ID: 01.GIJET.10.2.166

million USD in 2022. Notably classified as crucial infrastructure by the U.S. government, the healthcare sector has experienced a worrisome doubling of ransomware attacks within the past five years, disproportionately affecting health clinics, as highlighted in a study by JAMA Health Forum [1].
Similarly, the latest report of the second quarter of 2023(by IT governance), shows that 31% of the breach has taken place in the healthcare sector. This report has helped in identification of the sensitive data for the research. In turn, in this research the objective will be to work on improving the security framework in such an application environment [2].

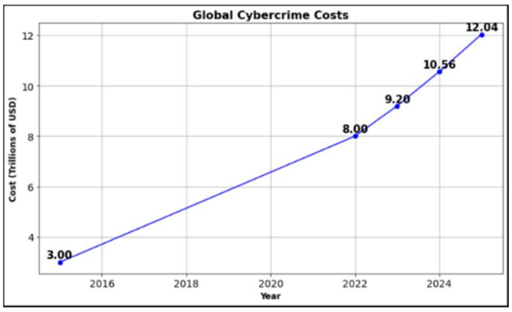

Figure 1. Projected global cybercrime costs: A 15% annual growth trend

Fig. 1 also presents how the global cybercrime damage cost has increased in the last 10 years. It can be observed that the trend has taken a steep hype in the year 2022. This shows that the research scope in this domain is very high. Convinces the author to extend the research to study different security frameworks and build an efficient framework for insecure designs.
The Open Web Application Security Project (OWASP) and the Common Weakness Enumeration (CWE) are pivotal in identifying and categorizing web vulnerabilities. A notable entry in the OWASP Top Ten, Insecure Design, emphasizes the critical role that secure design practices play in preventing attacks. One vulnerability that falls under this category is Cleartext Storage of Sensitive Information. This vulnerability highlights the risk associated with storing sensitive data without proper encryption [3]. Amidst the changing landscape, the shift towards remote work has introduced new challenges to cybersecurity. With an increasing number of individuals working from home, the attack surface has expanded, making organizations more susceptible to phishing attacks, insecure Wi-Fi connections, and the potential compromise of personal devices. As cyber threats continue to evolve, staying vigilant and proactive in implementing comprehensive cybersecurity measures is essential to safeguarding our digital world.

II. Healthcare Industry and Data Sensitivity

Healthcare data is critical for informing medical decisions, improving patient outcomes, and advancing medical research. It includes patient records, treatment histories, and medical imaging. Access to accurate and secure healthcare data is essential for healthcare providers, researchers, and policymakers to enhance the quality of care, streamline processes, and develop effective healthcare strategies. Additionally, healthcare data involves elements vital for authorization, ensuring that only authorized personnel have access to specific patient information. Integrity of healthcare data is essential, influencing the reputation of hospitals, medical professionals, and even public figures or celebrities. Maintaining the confidentiality, authorization, and integrity of healthcare data is paramount for ensuring trust in healthcare systems and protecting individuals' privacy and reputations. The research work presented by S. Mukherjee et al., incorporates security of sensitive data in the system by ensuring the access differences between users and authorities [33].
Blockchain technology can address these challenges by providing integrity, security, and accessibility to medical data [4-5]. It ensures data authenticity and transaction security through its consensus mechanism [6]. Machine learning can be used to extract relevant data from the vast amount of healthcare data, improving data management [7]. Blockchain also enables the integration of various healthcare aspects like medicine, appointments, and medical procedures through smart contracts [8]. Blockchain with machine learning, artificial intelligence, big data, and IoT, the healthcare system can be strengthened. Blockchain technology offers a decentralized and tamper-proof way to store and share healthcare data, addressing the need for transparency, traceability, and security.

III. Healthcare Cybersecurity Framework

A healthcare cybersecurity framework is a set of requirements and guidelines designed specifically for the healthcare industry to address the unique cyber challenges it faces. It aims to protect patients' data and health environments in the rapidly digitized healthcare systems. HIMSS (Healthcare Information and Management Systems Society) conducted a comprehensive Cybersecurity survey [9], illuminating the prevailing frameworks widely embraced in the healthcare industry. In our forthcoming discussion, we will explore prominent frameworks extensively utilized in the healthcare industry to bolster data security.

A. NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF)

The NIST CSF is a set of best practices, standards, and recommendations that organizations can use to improve their cybersecurity measures. It focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organizations' cybersecurity risk management. The framework provides a common organizing structure for multiple cybersecurity approaches and includes the framework core, framework implementation tiers, and a framework profile. NIST's five functions of cybersecurity are Identify, Protect, Detect, Respond, and Recover. The NIST CSF can be adapted and used to assess and improve the security of healthcare organizations, as well as other critical sectors. It is one of the most widely used in the healthcare sector. It can be complemented with the HITRUST Model, which provides information security control measures specifically for the medical field [10-12].

B. HITRUST (Health Information Trust Alliance)

The HITRUST (Health Information Trust Alliance) [13] framework is a comprehensive cybersecurity framework tailored for the healthcare industry. It offers a set of controls and best practices, aligning with regulations such as HIPAA (Health Insurance Portability and Accountability Act), to ensure the protection of sensitive health information. With a focus on risk management and scalability, HITRUST provides organizations in healthcare a standardized approach to assess, manage, and certify their cybersecurity practices. The framework's certification program, known as HITRUST CSF Assurance, allows organizations to demonstrate their commitment to robust cybersecurity measures. HITRUST framework ranks second: 26.4% of healthcare frameworks users claim to follow the guidelines created by the Health Information Trust Alliance.

C. CIS (Critical Security Controls)

The CIS [14] Controls, developed by the Center for Internet Security (CIS), constitute a set of 20 best practices organized into three categories: Basic Controls (1-6), Foundational Controls (7-16), and Organizational Controls (17-20). These controls provide a prioritized and practical approach to cybersecurity, addressing fundamental cyber hygiene, building a robust security foundation, and implementing strategic security measures. By adhering to these controls, organizations can enhance their cybersecurity defenses, mitigate common threats, and improve overall resilience against cyberattacks. In healthcare, the CIS Critical Security Controls are instrumental for fortifying cybersecurity defenses, ensuring the protection of patient data, and bolstering the resilience of healthcare systems against evolving cyber threats.

D. ISO 27000

The ISO 27000 series is a set of international standards focusing on information security management systems (ISMS) [15]. ISO/IEC 27001 is the core standard, providing requirements for establishing, implementing, maintaining, and continually improving an ISMS. The series includes additional standards like ISO/IEC 27002, offering guidelines and best practices for information security controls. Organizations adhering to the ISO 27000 series demonstrate a commitment to systematically managing information security risks and maintaining the confidentiality, integrity, and availability of information assets. In healthcare, adherence to the ISO 27000 series, particularly ISO/IEC 27001 and 27002, ensures the implementation of robust information security management systems, safeguarding patient data and maintaining the integrity and confidentiality of health information [16].

D. COBIT

COBIT, which stands for Control Objectives for Information and Related Technologies, is a comprehensive framework developed by ISACA for IT governance and management. COBIT 2019, the latest version, emphasizes aligning IT goals with business objectives, ensuring effective risk management, and optimizing resource utilization. The COBIT Core Framework (CFS) provides a foundational set of principles, enabling organizations to govern and manage enterprise IT in a structured and holistic manner. By utilizing COBIT, organizations can enhance the value derived from IT investments, manage risks effectively, and establish a robust governance structure for information and technology. The application of COBIT in different contexts has been studied in several papers. Talab and Flayyih found that the application of ITG under the COBIT framework had a positive impact on financial performance in the banking sector in Iraq [17]. Alramahi, Barakat, and Haddad emphasized the importance of effective controls and risk management in the IT environment, highlighting the role of COBIT in achieving efficient and secure information technology services [18]. Results from the 2018 HIMSS Cybersecurity Survey [19] stem from input provided by 239 qualified information security professionals across diverse healthcare organizations. They participated in a web survey commissioned by HIMSS and responded to inquiries regarding the security frameworks utilized by their organizations. When asked to select applicable security frameworks, the majority of respondents (57.9%) reported using NIST, followed by HITRUST (26.4%), Critical Security Controls (24.7%), and ISO (18.5%). Respondents could choose multiple frameworks. Additionally, 16.9 percent noted that their organizations had not implemented any security framework.

IV. Literature Review on Framework for Secure Storage of Sensitive Information

In recent times the demand of highly secure storage has bought the interest of researchers to work on different challenges related to storage. As the environment has expanded from the premises of the organization to external cloud service providers. It has increased the scope for research on secure storage in a wide range. Much research work can be evident of the solution being built to secure the storage. Some of the recent contributions have been discussed further to present the base of the proposal. In a study led by Wei Liu a et. al., a novel federated learning scheme was introduced for smart healthcare systems. This approach, utilizing dynamic secret sharing, substantially reduces time overhead and boosts efficiency in federated learning. Employing reusable subkeys and dynamic secret sharing, the system ensures secure user-server communication through elliptic curve cryptography. Notably, the scheme allows dynamic user management, making it adaptable to diverse real-world scenarios. Rigorous security analysis confirmed its resilience against various adversaries, and simulations demonstrated its practicality and effectiveness [20]. Similarly in another study led by Qiang Chen et al., a pioneering multi- modal network security framework for healthcare was introduced, enhancing flow classification efficiency and ensuring superior accuracy. The framework, based on deep learning and pretraining techniques, outperformed existing methods, particularly on the ISCXVPN2016 dataset. This advancement holds significant practical implications for human health systems, suggesting future explorations into innovative techniques like capsule networks and encrypted flow data analysis [21].

Malik Mustafa et al., investigated perceived security risks and moderating factors related to applying blockchain technology in cloud storage for a secure healthcare system. Their study, centered on the Middle East, delved into the factors influencing customer interest in adopting blockchain for healthcare, encompassing anticipation, effort expectancy, social influence, facilitating conditions, personal innovativeness, and perceived security risk. The research emphasizes the pivotal role of blockchain technology in fortifying healthcare data in the cloud and its transformative potential for healthcare information exchange [22]. Similarly, Jing Liu et al., conducted research on safeguarding sensitive data in the industrial internet, employing a three-layer approach of local, fog, and cloud storage. For real time sensitive data, they utilized the improved M-RAPPOR local differential privacy algorithm, followed by Reed- Solomon (RS) encoding and storage on local devices. Non-real-time sensitive data adopted a cloud-fog collaborative storage scheme with AES-RS encoding, distributing data between fog and cloud nodes for heightened protection. This scheme offers superior data safeguarding compared to conventional methods, maintaining real-time data sharing continuity [23]. Li Lin et al., developed a Lightweight Dynamic Audit approach for safeguarding sensitive data within cloud storage (Ldasip). Addressing the challenge of auditing data integrity in the cloud with incomplete trust, the study introduces Ldasip, which incorporates identity-based data integrity audit and data masking technology. Ldasip supports dynamic audit and sensitive information protection, offering lightweight challenge response and integrity verification compared to conventional schemes. The method aims to assure private key correctness, TPA audit authorization, sensitive data protection, and storage integrity. It provides valid audit proof under the condition of trusted TPA, CSP, and accurately stored data files [24]. Jing Liu et al., conducted research on safeguarding sensitive data in the industrial internet, employing a three-layer approach of local, fog, and cloud storage. For real-time sensitive data, they utilized the improved M-RAPPOR local differential privacy algorithm, followed by Reed-Solomon (RS) encoding and storage on local devices. Non-real-time sensitive data adopted a cloud-fog collaborative storage scheme with AES-RS encoding, distributing data between fog and cloud nodes for heightened protection. This scheme offers superior data safeguarding compared to conventional methods, maintaining real-time data sharing continuity [25]. Shengjing Sun et al., in research have proposed concept on healthcare operators 4.0 and implemented the practical application of the proposed concept. The work incorporates the systemic view of the Industrial IoT and technologies with wearable devices. The work brings new advantages to the application with the technology's features. These features expose new vulnerability in terms of security in the system [32].

Sheng Luo et al., introduced a user-sensitive information protection schema via blockchain technology. Their scheme involves a distributed k-anonymous location privacy protection mechanism to address challenges in ensuring honest cooperation and user privacy in location-based ser- vices. This approach effectively safeguards user location privacy, encourages broader user participation in anonymous zone construction, and advances the creation of anonymous areas without revealing cooperative users' actual locations. The paper additionally proposes a blockchain accounting rights competition mechanism to motivate user engagement in maintaining the blockchain [26]. Ying Liu et al., developed a novel self-attention-based detection algorithm employing a graph convolutional network (GCN) for sensitive information identification in natural language processing (NLP). Their approach employs a weighted GCN to encode word pairs from documents and corpus, integrating an attention mechanism for candidate word-corpus interactions. This algorithm showcases promising detection performance when compared to existing methods, highlighting its positive outcomes [27]. Abdullah Al Omar et al., introduced a blockchain-based privacy-preserving platform for healthcare data. Their study presents a patient-centric healthcare data management system that employs blockchain technology to ensure patient data privacy and pseudonymity. The system capitalizes on blockchain's decentralized and distributed nature to establish accountability and data integrity. Through cryptographic functions, patient data is protected and privacy maintained. The paper underscores the significance of controllability, traceability, and scalability in preserving privacy, addressing anonymity concerns effectively [28].

Sihua Wu et al., introduced a secure and efficient electronic medical record sharing model based on blockchain technology. Their approach combines data masking and the Inter Planetary File System (IPFS) to ensure medical data security while conserving blockchain resources. This model tackles the challenge of sharing medical information across institutions. The incorporation of data masking techniques, including generalization, occlusion, and replacement, safeguards patient privacy information effectively [29]. Yamei Zhan et al., designed Medical Record Encryption Storage Systems based on the Internet of Things (IoT) to tackle healthcare data storage and management challenges. Their approach introduces IoT technology, facilitating intelligent data processing and secure information services. They further pro- posed a medical record encryption management system, enhancing cost-effectiveness, convenience, and security of storage. Simulation experiments confirm paper cost reduction, standardized record forms, and controlled access to medical data [30]. Joseph Habiyaremye et al., developed a predictive machine learning model for storing temperature- sensitive medical products, like vaccines, in Rwandan pharmacies. The model employs multiple linear regression to anticipate when the inner fridge temperature will breach the allowed range. If the time is limited, the system advises against opening that chamber, suggesting an alternative with sufficient time slots to reach the upper limit. Evaluation yielded an R^2 coefficient of determination of 77%, underscoring its promise for creating an efficient multiple-room smart fridge for highly sensitive medical products [31]. In conclusion, the mounting demand for secure storage has driven extensive research into the challenges posed by evolving storage environments, extending from organizational premises to external cloud service providers. This dynamic landscape has led to investigations that encompass various dimensions of secure storage.

V. Research Scope on Cybersecurity Framework for Healthcare

Based on the discussion in the previous sections, it can be learned that different approaches have been designed for securing the data storage. Also, it is at high demand to build a framework which can ensure the security of data storage for healthcare. This brings into a problem where there is a need for study to be conducted on different storage practices and securing approaches in the healthcare industry. Even though the solution has been proposed by different authors still the data breach has increased in the healthcare sector. This research proposal is to build a secure framework for the storage of sensitive information in the healthcare industry. The design will make use of machine learning and private blockchain concepts to ensure the security of data. The objective of the research will be to identify critical data and secure it against leakage and tampering of data.

VI. Proposed Framework for Healthcare Security Management

Based on the study conducted in the literature review section and the insights from scope on cyber security. It is witnessed that the current security system is very specific. Such systems work along with other security systems to provide wider security to the overall system. Research conducted by different authors are either specific to the security architecture built for organizations or building a secure framework for implementing security to systems. In this research an architecture has been designed for the healthcare industry. The architecture considers the complete work process followed in different hospitals as standards. Thereby the architecture matches with the current healthcare systems.

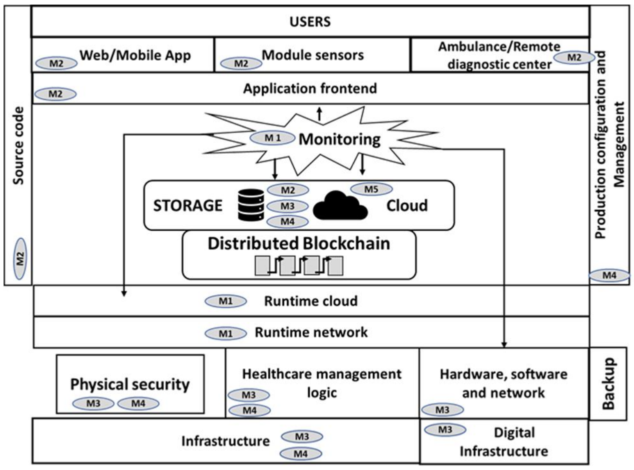

Figure 2. Security management architecture in healthcare.

Different information systems have been identified in the healthcare domain and been categorized based on data criticality. Information flow has been used to identify different relations in the system. Finally, a system architecture for healthcare was developed based on the relationship between different functional modules of any healthcare system, as shown in fig. 2. Table 1 shows, the application of framework modules over the Healthcare system architecture. The use of blockchain and cloud for storage in the design is to emphasize on the modern technology usage in the contribution. The benefits of modern technology in the healthcare adds on to provide features for easy and secure access with more effective and efficient usage.

TABLE I. THE MODULES OF HEALTHCARE INFORMATION SYSTEM ARCHITECTURE.

Modules	Functions	Security Frame
Users	Healthcare professionals, patients, researchers, and insurance companies	M1
Web/Mobile APP	Access and manage healthcare data, schedule appointments, communicate with professionals, access educational resources.	M2
Sensor Module	Collect data about patient health (wearables, implants, home monitoring).	M2
Ambulance / Remote Diagnostic Centre	Access patient data in real-time for faster, more effective care.	M2
Application Frontend	User interface for interacting with the system.	M2
Source Code	Detects and alerts for security threats and performance issues.	M1
Monitoring	Underlying code written in Python, Java, etc.	M2
Storage	Securely stores encrypted healthcare data.	M2, M3, M4 & M5
Blockchain	The blockchain is a distributed ledger technology that can be used to store and share healthcare data in a secure and tamper-proof manner.	M2
Runtime Cloud	The runtime cloud provides a scalable and reliable platform for running the system's applications.	M1
Runtime Network	Securely connects system components.	M1
Physical Security	Protects hardware from unauthorized access.	M3, M4
Infrastructure	The infrastructure layer provides the basic resources that the system needs to operate, such as computing, storage, and networking.	M3, M4
Digital Infrastructure	Provides software and services like databases and server.	M3

VII. FRAMEWORK DESIGNED AND ENROLLED FOR HEALTHCARE SYSTEM ARCHITECTURE

Security assessment has been designed to cover the overall security of the proposed healthcare system architecture.

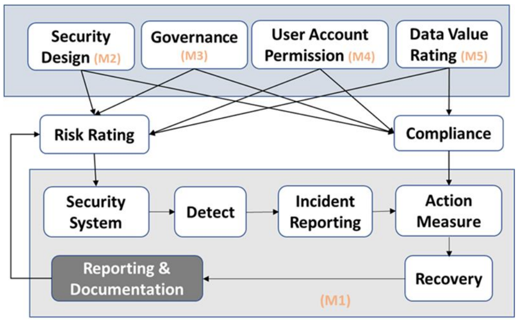

Figure 3. Security framework for the healthcare system architecture.

The layered framework as shown in fig. 3 categorizes each layer based on functionality. The proposed framework is developed after a detailed study of different frameworks being used in literature. The secure design module is to monitor security requirements from the start of the system design process and incorporating rules such as using the latest privileged tools, methods, encryption, and secure coding practices. Address the vulnerabilities in hardware, software, and networks. Data rating classifies data based on its sensitivity and values, from low to high (public, Business use, confidential, restricted, and highly restricted). Prioritizes protection of the most critical data and specifies appropriate security controls based on data classification. The module can be implemented with a machine learning approach to classify into critical and non-critical data based on data sensitivity. User account permission grants users access to only the information and systems they need to perform their jobs. Forces the user to use robust authentication methods like passwords, multi-factor authentication biometrics, etc. The governance establishes policies, procedures, and oversight for security management. Defines roles and responsibilities for security tasks. In the compliance module, healthcare system complies with relevant regulatory requirements and standards are ensured. It demonstrates responsible handling of sensitive information. The risk rating module deals with the conducts risk assessments to identify potential threats and vulnerabilities. Prioritizes resources for security measures based on the risk levels. The risk rating can be categorized further into design-based risk and behavioral risk. Any flaw in the implemented source code could lead to risk in the system. Behavioral risk includes the log data collection and identification of risk based on data history. The module can be built with an efficient machine learning model. Security system implements technical controls to protect the system, for example, firewalls, intrusion detection, anti-virus, malware software, and data encryption. Updates and patches security systems frequently to handle new threats. The detect modules monitors the system for security events and potential breaches. Uses the latest tools and techniques to identify suspicious activity. Incident reporting, establishes a process for reporting security incidents to ensure timely response and investigation. Action measures are defined and implements actions to be taken in response to security incidents. In the recovery, the recovery plans to restore normal operations after a security incident are recommended in priority. Report and documentation create detailed records of security incidents that happened, and actions that have been taken in response to those events. Generates regular reports to stakeholders on the state of security, compliance, and any notable event. Utilizes this information for analysis, improvement, and regulatory compliance.

VIII. Significance and Contribution

The proposed research work has significance and importance in the field of securing critical healthcare data from unauthorized access and data tampering. According to the survey conducted by OWASP, healthcare is one of the most targeted vulnerable industries. This research proposal aims to provide the following:

A. Enhancing Data Security

Addressing persistent challenges in healthcare data security, the research pioneers a Hybrid Machine Learning Based Cyber Secure Framework, leveraging adaptive machine learning and blockchain technologies.

B. Mitigating Data Breaches

By investigating prevalent storage practices and implementing robust measures, the study aims to curb data breaches, offering a timely solution to the rising threat in the healthcare sector.

C. Fostering Confidentiality

The proposed framework not only fortifies data integrity but also ensures confidentiality, contributing significantly to patient privacy and trust within healthcare systems.

D. Industry Advancement

Providing a comprehensive approach, the research accelerates industry standards, paving the way for enhanced security protocols and setting a benchmark for secure data storage practices in healthcare.

IX. CONCLUSIONS

In conclusion, the increasing number of cybersecurity threats to the healthcare industry data demand a proactive response. The proposed hybrid machine learning, blockchain based cyber-secure framework, integrating adaptive ML and private blockchain technologies, seeks to strengthen data security, prevent unauthorized access, data breaches and ensure confidentiality. This research makes a substantial contribution to the advancement of safe data storage techniques in the healthcare industry by addressing the existing weaknesses and establish industry standards. In the future, the framework could be useful for decentralized applications and more widespread industry applications, emphasizing the ongoing need for innovation in safeguarding healthcare data.

REFERENCES

[1] Freeze, D. (2023) 2023 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics, Cybercrime Magazine \url{https://cybersecurityventures.com}. Last accessed 22 Dec 2023.

[2] Irwin, L. (2023, July 11). Data Breaches and Cyber Attacks Quarterly Review: Q2 2023 - IT Governance UK. IT Governance UK Blog. \url{https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-quarterly-review-q2-2023}. last accessed 22 Dec 2023.

[3] OWASP Top Ten | OWASP Foundation. (n.d.). OWASP Top Ten | OWASP Foundation. \url{https://owasp.org/www-project-top-ten/}. last accessed 22 Dec 2023.

[4] Aniket, Rajani., Aashutosh, Singh., Abhishek, Kumar., Chirayu, Bandekar., Prof., S., M., Patil. (2023). Healthcare Management System using Blockchain with ML Integration. International Journal of Advanced Research in Science, Communication and Technology, doi: 10.48175/ijarsct-8565.

[5] Govardhan, R., Jagadeesh, V, Ranagatti., Lakshminath, S, M., Linganand, Sangamad., Dr., Nagaraja, J. (2023). A Literature Review of Blockchain Applications in Healthcare. International Journal For Science Technology And Engineering, doi: 10.22214/ijraset.2023.48808.

[6] Shilpa, Srivastava., Millie, Pant., Sunil, Kumar, Jauhar., Atulya, K., Nagar. (2022). Analyzing the Prospects of Blockchain in Healthcare Industry. Computational and Mathematical Methods in Medicine, doi: 10.1155/2022/3727389.

[7] Shilpa, Srivastava., Millie, Pant., Sunil, Kumar, Jauhar., Atulya, K., Nagar. (2022). Analyzing the Prospects of Blockchain in Healthcare Industry. Computational and Mathematical Methods in Medicine, doi: 10.1155/2022/3727389.

[8] (2023). Healthcare Data Management System Using Blockchain. International journal of scientific research in computer science, engineering and information technology, 382-387. doi: 10.32628/cseit2390250.

[9] (2023). Healthcare Data Management System Using Blockchain. International journal of scientific research in computer science, engineering and information technology, 382-387. doi: 10.32628/cseit2390250.

[10] Moller, D.P.F.: NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In Guide to Cybersecurity in Digital Transformation. Advances in Information Security, Springer, Cham {103}, 231--271 (2023).

[11] Hanisch, RJ; Kaiser, DL; Yuan, A; Medina-Smith, A. Carroll, BC Campo, EM.: NIST Research Data Framework (RDaF) Version 1.5. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) US, Department of Commerce (2023).

[12] Adriana-Meda, Udroiu., Mihail, Dumitrache., Ionuț, Sandu: Improving the cybersecurity of medical systems by applying the NIST framework. In: 14th International Conference on Electronics, Computers and Artificial Intelligence. IEEE, Ploiesti, Romania , (2022). \doi: 10.1109/ecai54874.2022.9847498.

[13] HITRUST - Accorian. Accorian, \url{https://accorian.com/hitrust/}. Last accessed 8 December 2023.

[14] CIS (Center for internet security), \url{https://www.cisecurity.org/}. Last accessed 23 December 2023.

[15] International Organization for Standardization, \url{https://www.iso.org/home.html}. Last accessed 25 November 2023.

[16] Tembisa, Grace, Ngqondi. ,The ISO/IEC 27002 and ISO/IEC 27799 information security management standards : a comparative analysis from a healthcare perspective. South East Academic Libraries System, (2009).

[17] Hassnain, Raghib, Talab., Hakeem, Hammood, Flayyih: An Empirical Study to Measure the Impact of Information Technology Governance Under the Control Objectives for Information and Related Technologies on Financial Performance. International Journal of Professional Business Review {8}(4), 1--19 (2023), doi: 10.26668/businessreview/2023.v8i4.1382.

[18] Nedal, M., Alramahi., Abdallah, I., Barakat., Hossam, Haddad: Information Technology Governance Control Level in Jordanian Banks Using Control Objectives for Information and Related Technology (COBIT 5). European Journal of Business and Management {6}(5) 194--206 (2014)

[19] Healthcare Information and Management Systems Society (HIMSS), \url{https://www.himss.org/}. Last accessed 20 September.

[20] S. El Kafhali, W. Liu, Y. Zhang, G. Han, J. Cao, H. Cui, and D. Zheng: Secure and efficient smart healthcare system based on federated learning In:International Journal of Intelligent Systems, Said El Kafhali vol. 2023, pp. 1--12. Hindawi, (2023). \doi:10.1155/2023/8017489.
[21] F. Ali, Q. Q. Chen, J. P. Li, A. u. Haq, B. L. Y. Agbley, A. Hussain, I. Khan, R. U. Khan, J. Khan, and I. Ali: A multimodal network security framework for healthcare based on deep learning. In: Computational Intelligence and Neuroscience, Farman Ali, Hindawi, \url{https://doi.org/10.1155/2023/9041355} (2023).
[22] O. I. Khalaf, M. Mustafa, M. Alshare, D. Bhargava, R. Neware, B. Singh, and P. Ngulube: Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems, Osamah Ibrahim Khalaf, Computational and Mathematical Methods in Medicine, Hindawi (2022). \doi{10.1155/2022/6112815}.
[23] P. Gope, J. Liu, C. Yuan, Y. Lai, and H. Qin: Protection of sensitive data in industrial internet based on three-layer local/fog/cloud storage, In: Security and Communication Networks, vol. 2020, p. 2017930, Hindawi (2020). \doi{10.1155/2020/2017930}
[24] W. Ding, L. Lin, W. Tan, and Z. Chu: Ldasip: A lightweight dynamic audit approach for sensitive information protection in cloud storage. In: Wenxiu Ding, Security and Communication Networks, Hindawi vol. 2022, Article ID 8508755, (2022), \doi{10.1155/2022/8508755}.
[25] A. Bagwari and S. Luo: User sensitive information protection scheme based on blockchain technology,Mobile Information Systems, vol. 2022, Article ID 2328734, 15 pages, 2022. \url{https://doi.org/10.1155/2022/2328734}.
[26] Ying Liu, Chao-Yu Yang, Jie Yang, M. Irfan Uddin: A Graph Convolutional Network-Based Sensitive Information Detection Algorithm, Complexity, Hindawi, vol. 2021, pages 1-8, (2021), \doi{10.1155/2021/6631768}.
[27] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto: Medibchain: A blockchain based privacy preserving platform for healthcare data, in Security, Privacy, and Anonymity in Computation, Communication, and Storage (G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, eds.), (Cham), pp. 534--543. Springer International Publishing, (2017), \doi{10.1007/978-3-319-72395-2_49}.
[28] Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto: Medibchain: A blockchain based privacy preserving platform for healthcare data, in Security, Privacy, and Anonymity in Computation, Communication, and Storage (G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, eds.), (Cham), pp. 534--543. Springer International Publishing, (2017), \doi{10.1007/978-3-319-72395-2_49}.
[29] S. Wu and J. Du: Electronic medical record security sharing model based on blockchain,In: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, ICCSP '19, (New York, NY, USA), pp. 13–-17, Association for Computing Machinery, (2019), \doi{10.1145/3309074.3309079.
[30] C.-L. Chen, Y. Zhan, and Z. Xuan: Medical record encryption storage system based on internet of things, Wireless Communications and Mobile Computing, vol. 2021, Article ID 2109267, pp. 1-9, (2021). \doi{10.1155/2021/2109267}.
[31] R. Malekian, J. Habiyaremye, M. Zennaro, C. Mikeka, E. Masabo, K. Jayavel, and S. Kumaran: A Data-Driven Predictive Machine Learning Model for Efficiently Storing Temperature-Sensitive Medical Products, Such as Vaccines: Case Study: Pharmacies in Rwanda", Journal of Healthcare Engineering, vol. 2021, Article ID 9990552,pp. 1--12, 2021. \doi{10.1155/2021/9990552}.
[32] Sun, S.; Zheng, X.; Gong, B.; García Paredes, J.; Ordieres-Meré, J. Healthy Operator 4.0: A Human Cyber–Physical System Architecture for Smart Workplaces. Sensors 2020, 20, 2011. https://doi.org/10.3390/s20072011
[33] S. Mukherjee, K. Dolui and S. K. Datta, "Patient health management system using e-health monitoring architecture," 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, India, 2014, pp. 400-405, doi: 10.1109/IAdCC.2014.6779357.