Blockchain Security Framework for Ransomware in IOT Healthcare

Mr. CHANDRU R[1], Ms. G. FATHIMA[2]

[1] Mr. CHANDRU R, M.Sc CFIS, Department of Computer Science Engineering, ramchandru372@gmail.com, ,
Dr.MGR UNIVERSITY, Chennai, India

[2] Ms. G. Fathima Faculty ,Centre for Cyber Forensics and Information Security, University of
Madras, Chepauk, Chennai

---***---

Abstract: Ransomware is a malicious software or program that encrypts the data on a hard disc and denies the users access to it unless an amount is paid. Ransomware attacks majorly target the majority of the organizations like financial institutions and healthcare organizations. Ransomware attacks are one of the scariest forms of cyber-attacks, and they are not limited to a particular industry or the nations. Blockchain is an untamperable technology, which is stronger, more secure and decentralized in nature. Characteristics of blockchain can provide additional security for ransomware detection and mitigation more effectively. In this paper, we introduce a new blockchain-based security framework to identify and protect the ransomware attacks for smart healthcare (briefly, BSFR-SH). The security analysis performed in this paper establishes the security of the proposed BSFR-SH against the ransomware attacks. Performance of BSFR-SH is much superior compared to other existing similar mechanisms because it has better accuracy and F1-score compared to other mechanisms under comparison.

Keywords: Blockchain tamper-proof technology, Encrypts data, Malware Identification, Detection, Automated Detection Systems, Ransomware, Untamperable technology.

I. INTRODUCTION

Ransomware attacks have become one of the most destructive and widespread types of cybercrime in recent years. These malicious software encrypt important files or data on an infected computer and ask for a ransom to release them. The healthcare industry, as well as other sectors like finance and government, has been especially susceptible to ransomware attacks because of the sensitive and priceless nature of the information they process. As ransomware is becoming more and more advanced and sophisticated, there is a pressing need to come up with new and efficient measures to identify, counteract, and recover from such attacks [1].

Conventional security controls, including antivirus software and intrusion detection systems (IDS), usually fall behind the changing tactics of ransomware attackers. Consequently, there is an urgent need for stronger, real-time detection and defense technologies that can actively counter ransomware attacks. In this regard, new technologies such as blockchain and machine learning provide promising solutions [2] .

The pairing of blockchain and machine learning to strengthen cybersecurity is in increasing focus as a means to fortify against ransomware and other malevolent activities. Blockchain offers a distributed ledger that maintains the integrity of information by keeping it immutable and tamper-proof. Blockchain can be used to lock backups for key data so that victims will be able to retrieve their files without having to pay a ransom. This hybrid method, which combines blockchain and machine learning, could transform ransomware defense by delivering prevention and recovery capabilities [3] .

A novel framework referred to as the Blockchain-Enabled Security Framework for Smart Healthcare (BSFR-SH), which relies on blockchain technology to protect data and machine learning methods to identify ransomware attacks. The BSFR-SH is designed to yield an end-to-end solution for the smart healthcare industry, where sensitive patient data and system integrity are the top priority. Through the integration of blockchain's capability to provide data integrity and machine learning's capacity to identify unusual patterns, our framework offers an effective defense system against ransomware attacks while retaining the efficiency and dependability of healthcare processes [4] .

The rest of this paper is structured as: Section II provides a background in related work on ransomware detection and blockchain security frameworks with existing solutions and limitations. Section III outlines the proposed method of implementing BSFR-SH, including system architecture and the application of machine learning to ransomware detection. Section IV explains the experimental outcome and performance assessment of the given framework, and how it compares with other available techniques. Last but not least, Section V concludes the paper and suggests future research directions for this area [5].

II. LITERATURE SURVEY

Y. Zhang et al., [6] Systematic Literature Review and Metadata Analysis of Ransomware Detection Mechanisms provides an extensive analysis of ransomware attacks and detection mechanisms, categorizing existing techniques and evaluating their effectiveness. The paper addresses the evolution of ransomware and the challenges posed by obfuscation techniques that hinder detection. It emphasizes the importance of preventive measures, such as regular data backups, and explores the use of honeypot systems for identifying ransomware. The authors suggest that combining traditional and modern techniques can enhance detection rates. The paper serves as a benchmark for future research in this field.

Niall Mahony et al., [7] Deep Learning (DL) has gone a long way in advancing Digital Image Processing, making those solutions that were previously impossible possible. Yet, those classic computer vision approaches remain valid and are far from outdated. This paper contrasts the advantages and limitations of both DL and traditional methods. It promotes continuous learning and implementation of classic approaches in addition to DL. The argument brings home the importance of retaining classical knowledge in today's AI world. The paper also investigates blending both methods for improved results. Hybrid techniques are discussed that surpass single DL in certain aspects.

Eduardo Berrueta et al., [8] Ransomware is a significant threat to businesses, particularly in a shared server environment. A single compromised host can block access to any shared files. This article suggests a detection tool using file-sharing network traffic analysis. The tool employs machine learning to learn patterns of ransomware behavior, including reading and overwriting of files. It handles clear text and encrypted protocols. Three ML models were analyzed and compared, with the top-performing one chosen. The model was trained on over 70 samples of ransomware from 26 strains and 2500+ hours of clean traffic. The model was able to detect all ransomware binaries, even unseen ones. False positive rates were also evaluated, as well as data loss before detection. The results supported the effectiveness and accuracy of the tool.

Maad Ebrahim et al., [9] Blockchain, which was primarily associated with cryptocurrencies, can now accommodate various advanced technologies such as the Internet of Things (IoT). Integration with IoT allows the creation of smart environments such as smart homes, transport, industries, and supply chains. Blockchain eliminates the necessity for centralized control, providing secure, decentralized communication among devices. It provides security, privacy, and authentication in trustless systems. Other technologies such as SDN, Fog, Edge, and Cloud Computing also have important roles to play in facilitating IoT applications. The integration of AI and Machine Learning enables smart devices to take independent decisions. This paper covers the integration of these technologies for building futuristic smart environments. It emphasizes the increasing synergy between Blockchain, IoT, and AI. The paper also emphasizes the importance of flexible Blockchain platforms for various applications. A simplified architecture for smart environments of the future is introduced to illustrate the potential of this integration.

Hong-Ning Dai et al., [10] The Internet of Things (IoT) is revolutionizing industries into smart, data-driven systems. IoT, however, is confronted with challenges such as decentralization, poor interoperability, privacy concerns, and security threats. Blockchain technology presents solutions to these issues by allowing secure, decentralized communication. This paper discusses the integration of IoT with blockchain, known as Blockchain of Things (BCoT). It offers a comprehensive survey of BCoT, starting with IoT challenges and an overview of blockchain. The study introduces a BCoT architecture for this convergence. It also investigates how blockchain can enable 5G and industrial IoT usage. Central issues and challenges of the integration are addressed. The paper emphasizes the growing importance of BCoT in contemporary tech ecosystems. Finally, it provides future research directions to progress BCoT.

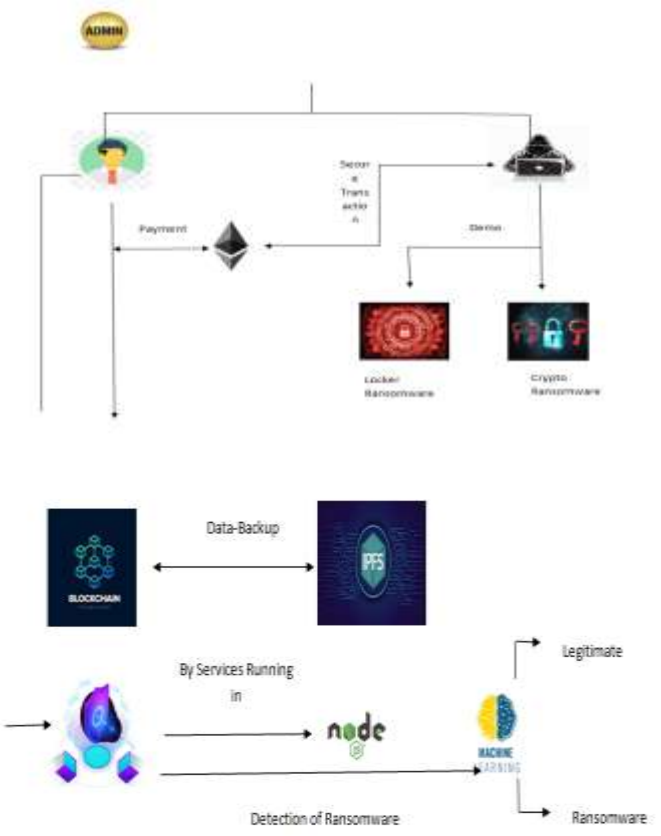
V. Dedeoglu et al., [11] The swift proliferation of IoT devices with sensing, processing, and communication capabilities has opened doors to smart environments and new business models. The devices collect, process, and exchange information through interactions, but security, privacy, and reliability concerns remain. Blockchain technology has come forward as a potential answer, providing immutable distributed ledgers, tamper-proof records, cryptocurrency support for transactions, and smart contracts to facilitate automated action under certain conditions. These aspects improve IoT data privacy and security. Nevertheless, combining blockchain with IoT also presents challenges, such as scalability issues in designing blockchains specific to IoT requirements. In spite of this, blockchain has potential for the development of IoT applications. This chapter discusses the advantages, disadvantages, and potential applications of blockchain in the IoT environment.

Shifa, and et al.,[12]*"Ransomware Attacks and Detection Mechanisms: A Systematic Literature Review"* provides a detailed and structured overview of the evolving landscape of ransomware threats and the corresponding detection methodologies. The authors explore the historical development of ransomware, emphasizing its shift from basic lock-screen tactics to more advanced encryption-based attacks that have significantly impacted users and organizations. The review categorizes detection mechanisms into three primary types: signature-based, anomaly-based, and hybrid approaches. It highlights the limitations of traditional methods, such as their inability to detect zero-day threats, and emphasizes the growing reliance on machine learning and artificial intelligence to identify new and sophisticated ransomware variants. The paper also discusses challenges in the detection process, such as obfuscation techniques, the speed of attack execution, and the lack of standardized datasets for training models. Overall, the study serves as a valuable resource for cybersecurity researchers and professionals, offering insights into the strengths and weaknesses of current solutions and identifying areas for further research and innovation in ransomware detection**.**

III. PROPOSED METHODOLOGY

The procedure identified in the diagram provides the step-by-step implementation of a ransomware attack through secure transactions. The process starts with the administrator, who sets the chain of events in motion. The user next conducts a payment transaction on Ethereum, guaranteeing the payment through secure protocols. This step highlights the role of secure transactions as a pivotal aspect of the process. After payment, the process moves on to a demo stage, represented by the icon of a hacker, emphasizing the simulation or starting of ransomware activity. Cybersecurity system with blockchain technology, IPFS (InterPlanetary File System), Node.js, and machine learning for detecting ransomware. Data is first backed up securely with blockchain to make it immutable and maintain its integrity. The backed-up information is then kept in IPFS, a distributed storage system allowing for effective and consistent access. Node.js services are also instrumental in coordinating the detection mechanism [13].

3.1 Research Design



IV. FINDINGS

The results of this study emphasize the potential of integrating blockchain technology and machine learning algorithms to combat the growing menace of ransomware attacks. The suggested Blockchain-Enabled Security Framework for Smart Healthcare (BSFR-SH) utilizes blockchain's intrinsic security characteristics to safeguard sensitive healthcare information, making its integrity intact and tampering impossible. The framework also exhibits better performance in ransomware detection compared to conventional systems, achieving significantly improved accuracy and F1-score. By monitoring the system constantly and deleting suspicious files automatically, BSFR-SH offers a proactive and efficient method of protection against ransomware. The use of machine learning enhances the framework's capabilities in detecting ransomware in real time, limiting damage and ensuring healthcare data is secure [14].

In summary, the Blockchain-Enabled Security Framework for Smart Healthcare (BSFR-SH) presents an encouraging solution to counter the emerging threat of ransomware attacks. The study proves that by fusing the tamper-resistant properties of blockchain with sophisticated machine learning strategies, BSFR-SH is more efficient at detecting and combating ransomware compared to current systems. Its capability to protect sensitive medical information, recover without ransom, and carry out real-time discovery is a major leap forward in cybersecurity, particularly in the healthcare industry. The actual deployment of BSFR-SH also demonstrates its scalability, performance, and low system impact, making it a practical solution for healthcare institutions and other industries that are exposed to similar cyber attacks. Overall, this study underscores the significance of combining new technologies such as blockchain and machine learning to build safer, more resilient, and more efficient systems to counter continually evolving cyber attacks [15].

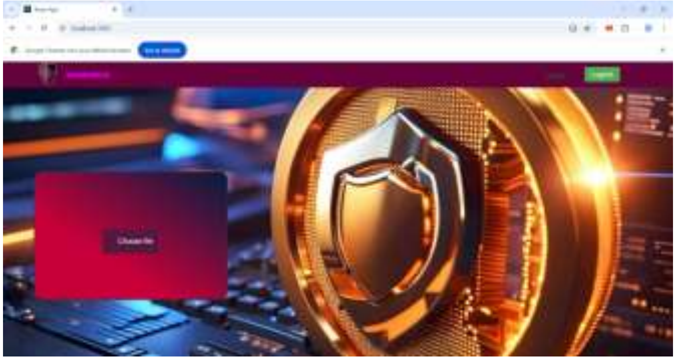


Fig 4.1

It has one button named "Choose file", implying that this page lets users upload files—perhaps for scanning, its shows whether it shows legitimate or not, or safe storage as one of the protective aspects of RANSHIELD.

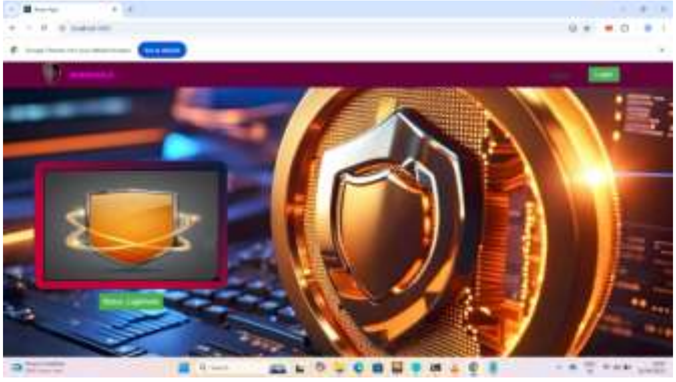


Fig 4.2 - Result

The picture is a web application screenshot called “RANSHIELD”, which looks like it is a prototype or locally hosted utility centered on cybersecurity, ransomware protection. The interface is being executed on “localhost:3000”, so it must be in development or testing on a local system. At the top of the page, a dark purple navigation bar contains a shield logo and the title “RANSHIELD”, representing online security. On the navigation bar's right side, there are navigation links such as a “Home” link and a large green “Login” button, implying access to personalized or secure parts of the app. The foreground of the page features a prominent high-tech shield icon that is glowing in gold and orange colors, against a digital landscape that features a computer keyboard and lines of code. This imagery reinforces the theme of protection within a digital setting. To the left of this image is a floating panel defined in a gradient of red and blue with an image of a second shield in orbit-like rings. This is probably indicative of scanning or monitoring capability. Underneath this shield image is a green status icon with “Status: Legitimate”, which implies that the application has recognized the current state or item as secure and threat-free. As a whole, the interface design and elements suggest RANSHIELD is a cybersecurity software intended to detect or stop ransomware and offer a user-friendly status report on the system's safety that it is tracking.

Figure 4.3

A small status box titled "Balance: Loading…" is displayed, presumably for wallet or token balance, suggesting integration with blockchain or cryptocurrency features. At the center of the page, four red buttons with white labels are present: "Choose File", "Retrieve File", "Store File on IPFS", and "Perform Payment". These buttons imply that users can upload and store files securely, perhaps through IPFS (InterPlanetary File System), a decentralized storage protocol. The presence of a payment button suggests functionality for making secure payments, which may be for paying for services, decrypting encrypted files, or ransomware-related functionality.

V. ACKNOWLEDGEMENTS

I would like to express our sincere gratitude to all those who contributed to the successful completion of this research work. First and foremost, we extend our heartfelt thanks to

Dr. M.G.R. Educational and Research Institute, Chennai, for providing us with the necessary infrastructure and academic environment to carry out this project. I deeply thankful to Ms. Ms. G. Fathima, Faculty. Centre for Cyber Forensics and Information Security, University of Madras, Chepauk, Chennai for her invaluable guidance, continuous support, and insightful feedback throughout the research. Her expertise and mentorship were instrumental in shaping the direction and quality of this work.

I also extend our appreciation to our colleagues and peers who provided constructive suggestions and moral support throughout this journey. Special thanks to the faculty of the Department of Computer Science Engineering for their encouragement and academic assistance.

VI. CONCLUSION

In summary, the suggested Blockchain-Enabled Security Framework for Smart Healthcare (BSFR-SH) effectively combats the escalating menace of ransomware attacks by combining the untamperable and unbreakable qualities of blockchain technology with sophisticated machine learning approaches. The framework proves to have superior performance against ransomware detection compared to current systems in terms of accuracy and F1-score. Its capacity for real-time identification of advanced ransomware strains, while maintaining the integrity and security of vital healthcare information, constitutes a powerful leap in cybersecurity for healthcare. The real-world application of BSFR-SH also demonstrates its scalability, effectiveness, and negligible burden on system performance, establishing it as the perfect solution for healthcare organizations and beyond. In all, this research underscores the need to harness the advantages of cutting-edge technologies like blockchain and machine learning in building stronger and more resilient systems that can protect against continually mutating cyber attacks [16].

REFERENCE :

[1] Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2016). Information security: The moving target. *Computers & Security*,61,97–114. https://doi.org/10.1016/j.cose.2016.06.003

[2] Parveen, K. (2024). *Advanced Techniques of Malware Evasion and Bypass in the Age of Antivirus*. International Journal for Electronic Crime Investigation, 8(3). https://doi.org/10.54692/ijeci.2024.0803200.

[3] Alshamrani, M.; Alzahrani, A.; Alotaibi, M.; Alotaibi, F.; Alghamdi, A. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers* 2024, *13*(3), 60. https://doi.org/10.3390/computers13030060

[4] Jiang JX, Bai G (2019) Types of information compromised in breaches of protected health information. Ann Intern Med 172(2):159. https://doi.org/10.7326/m19-1759

[5] Alqahtani, A., & Sheldon, F. T. (2022). A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook *Sensors*,*22*(5), 1837. https://doi.org/10.3390/s22051837.

[6]Zhang, Y., et al. (2019). Systematic Literature Review and Metadata Analysis of Ransomware Detection Mechanisms. *Journal of Reliable Intelligent Environments*, 5(2), 67–89. https://doi.org/10.1007/s40860-019-00080-3

[7] Niall O' Mahony, Sean Campbell, Anderson Carvalho, Suman Harapanahalli, Gustavo Velasco-Hernandez,

Lenka Krpalkova, Daniel Riordan, Joseph Walsh, Deep Learning vs. Traditional Computer Vision, Advances in Computer Vision, Volume 943, 2019, Pages 128–144, ISBN 978-3-030-17794-2, https://doi.org/10.1007/978-3-030-17795-9_10

[8] Eduardo Berrueta, Daniel Morato, Eduardo Magaña, Mikel Izal, Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic, *Expert Systems with Applications*, Volume 209, 2022, Article 118299, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2022.118299

[9] Maad Ebrahim, Abdelhakim Hafid, Etienne Elie, Blockchain as privacy and security solution for smart environments: A Survey, *arXiv preprint*, arXiv:2203.08901, March 2022, https://arxiv.org/abs/2203.08901

[10] Hong-Ning Dai, Zibin Zheng, Yan Zhang, Blockchain for Internet of Things: A Survey, *IEEE Internet of Things Journal*, Volume 6, Issue 5, October 2019, Pages 8076–8094, ISSN 2327-4662, https://doi.org/10.1109/JIOT.2019.2920987 Academia+7Henry Lab+7arXiv+7

[11] Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal*,*6*(5),8076–8094. https://doi.org/10.1109/JIOT.2019.2920987

[12**]** Shifa, M. S., Hasan *Ransomware Attacks and Detection Mechanisms: A Systematic Literature Review*. In *Proceedings of the International Conference on Cybersecurity and Privacy* (pp.123–145).Springer. https://link.springer.com/chapter/10.1007/978-981-97-7603-0_7

[13**]** Igwe, C. S.-R. (2023). *A secure and scalable blockchain enabled emergency e-health system* [Master's thesis, University of New Brunswick]. UNB Scholar. 10.3390/s22051837

[14] Osama, O. F., Kshetri, N., Rahman, M. M., & Pokharel, B. P. (2025). *healthMLsec: Machine Learning based Vulnerability Assessment in Health Systems: A Framework for Enhancing Cybersecurity and Patient Data* [Preprint]. Preprints.org. https://doi.org/10.20944/preprints202502.2165.v1

[15] Norman G (2016) Drugs and devices: comparison of European and U.S. Approval Processes. JACC 1(5)*:* 399–412. https://doi.org/10.1016/j.jacbts.2016.06.003.