International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 2 (2025)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 2, 2025
© 2025 IJERST. All Rights Reserved

Research Paper

Cyber Fraud Detection And Analysis Of The Crypto Ransomware

[1] T.RAVALI, [2] CH. DEVI, [3] M. NANDINI, [4] D. SRAVANI, [5] E. ASHWITHA, [6] D. SREEJA

[1] Assistant Professor, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,4,5,6] B. Tech Students, Department of Computer Science and Cyber Security, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

Abstract:

Currently as the widespread use of virtual monetary units (like Bitcoin, Ethereum, Ripple, Litecoin) has begun, people with bad intentions have been attracted to this area and have produced and marketed ransomware to obtain virtual currency easily. This ransomware infiltrates the victim's system with smartly designed methods and encrypts the files found in the system. After the encryption process, the attacker leaves a message demanding a ransom in virtual currency to open access to the encrypted files and warns that otherwise the files will not be accessible. This type of ransomware is becoming more popular over time, so currently it is the largest information technology security threat. In the literature, there are many studies about detection and analysis of this cyber-bullying. In this study, we focused on crypto-ransomware and investigated a forensic analysis of a current attack example in detail. In this example, the attack method and behavior of the crypto ransomware were analyzed, and it was identified that information belonging to the attacker was accessible. With this dimension, we think our study will significantly contribute to the struggle against this threat.

Received: 02-5-2025 Accepted: 09-6-2025 Published: 18-6-2025

I.INTRODUCTION

With the rapid digitization of industries and the exponential growth of online transactions, the digital landscape has become a lucrative target for cybercriminals. Among the most dangerous threats in recent years is crypto-ransomware, a form of malware that encrypts a user's files and demands cryptocurrency payments—typically in Bitcoin—for decryption. Ransomware like WannaCry, Locky, and Ryuk have caused devastating consequences, affecting hospitals, financial institutions, and government agencies

worldwide. These attacks are sophisticated, dynamic, and increasingly automated, exploiting human vulnerabilities, software loopholes, and systemic weaknesses.

Cyber fraud detection—the process of identifying and mitigating unauthorized or malicious cyber activities—has become more crucial than ever. The intersection of machine learning, network analysis, and threat intelligence offers new possibilities for detecting crypto-ransomware based on behavioral patterns, data anomalies, encryption signatures, and attack vectors. This research focuses on analyzing ransomware characteristics and developing robust detection models using machine learning and data analytics to counter the growing menace of crypto-ransomware. By identifying early signs of ransomware behavior and financial traces on blockchain networks, we aim to mitigate damage and assist law enforcement in tracking the origin of attacks.

II.LITERATURE SURVEY

Over the last decade, several research works have explored the detection, analysis, and prevention of crypto-ransomware and cyber fraud. Kharraz et al. (2015) conducted one of the early systematizations of ransomware behavior, highlighting file system activities, encryption techniques, and network interactions. Huang et al. (2017) used dynamic analysis tools to monitor file I/O patterns and detect encryption attempts in real-time. Similarly, Ugarte-Pedrero et al. (2016) introduced CryptoWall analysis, identifying runtime API behavior as an indicator of malicious activity.

In the context of machine learning, Sgandurra et al. (2016) presented EldeRan, an ML-based ransomware detection framework using dynamic features like file modifications, registry access, and system calls. Anderson et al. (2018) proposed deep learning models for behavior-based ransomware detection. Other studies focused on Bitcoin transaction analysis, tracing wallet addresses and blockchain movements to identify criminal revenue chains (Conti et al., 2018). Recent research by Kurniawan et al. (2020) integrates natural language processing (NLP) on ransom notes and graph-based tracing on blockchain data to map attacker infrastructures.

Despite these advancements, most systems either focus solely on technical behavior or financial traceability. Few provide a hybrid view combining machine learning, system behavior, and financial intelligence, which is essential for detecting and stopping crypto-ransomware in real-time and performing post-attack forensics.

III.EXISTING SYSTEM

The existing systems for crypto-ransomware detection and cyber fraud analysis are largely reactive, relying heavily on signature-based antivirus software, heuristic rules, and manual interventions. Signature-based systems scan binaries for known ransomware patterns or cryptographic libraries. However, they are easily bypassed by obfuscation, polymorphism, or packing techniques, allowing newer variants to go undetected.

Other tools use sandboxing and dynamic analysis, but these are resource-intensive, and many ransomware variants now detect virtual environments and delay execution to avoid detection. Moreover, most fraud detection mechanisms rely on rule-based systems that monitor network traffic or transaction thresholds. These approaches lack adaptability and fail to generalize to new or evolving attack vectors.

There is also limited use of real-time financial analysis in tracing cryptocurrency flows post-ransom payment. While blockchain offers transparency, most tools lack integration with ML models that can analyze wallet clustering, transaction graph analysis, and money-laundering patterns. Overall, current systems are fragmented, lacking a unified, intelligent, and automated detection approach.

IV.PROPOSED SYSTEM

The proposed system introduces an intelligent and comprehensive machine learning-based framework for detecting and analyzing crypto-ransomware and associated cyber fraud. The solution consists of three major components: Ransomware Behavior Detection, Cryptocurrency Transaction Analysis, and Fraud Classification.

Ransomware Detection Module: This module uses static and dynamic feature extraction from suspicious executables. Features include system API calls, entropy changes in files, file renaming patterns, encryption indicators, and registry modifications. These are fed into ML classifiers such as Random Forest, SVM, Gradient Boosting, and Deep Neural Networks trained on labeled ransomware and benign data.

Cryptocurrency Transaction Analysis Module: Once a ransom note is found or a crypto wallet is identified, the system uses blockchain APIs (like BlockCypher or Chainalysis) to analyze transaction flows. It builds transaction graphs, identifies patterns like peel chains, mixers, or exchange endpoints, and applies graph clustering algorithms to trace potential laundering routes or actor connections.

Integrated Threat Intelligence Dashboard: All modules feed into a dashboard that visualizes ransomware detection, victim IPs, payment wallets, transaction timelines, and known attack signatures. It also allows analysts to submit new samples and view predictions in real-time. Integration with a threat intelligence feed updates the system with the latest ransomware campaigns and TTPs (Tactics, Techniques, and Procedures). By combining behavior-based ML models with blockchain analytics, this system offers a multi-dimensional defense mechanism, enabling both real-time protection and post-event forensic tracking of cybercriminal activities.

V.SYSTEM ARCHITECTURE

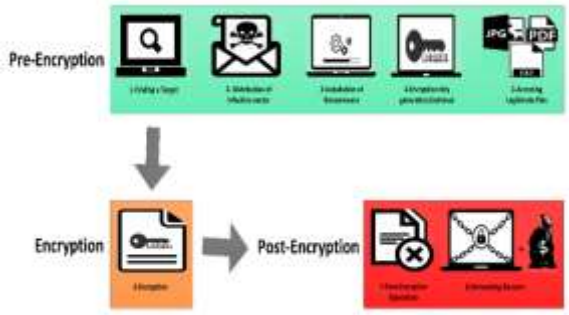


Fig 5.1 System Architecture

The image presents a comprehensive visual representation of the lifecycle of a ransomware attack, broken down into three main phases: Pre-Encryption, Encryption, and Post-Encryption. Each stage highlights the critical steps involved in executing a typical crypto-ransomware operation. This diagram effectively outlines the complete kill-chain of a ransomware attack, from reconnaissance to extortion. Understanding each phase is crucial for designing multi-layered security defenses, such as early detection, sandboxing, endpoint protection, and user awareness training. The structured flow also emphasizes the need for prevention, detection, response, and recovery strategies at each stage to mitigate the risk of ransomware attacks.

VI.IMPLEMENTATION



Fig 6.1 User Login



Fig 6.2 User Dashboard



Fig 6.3 Upload Data Files



Fig 6.4 Encrypted Files



Fig 6.5 Secured Files

VII.CONCLUSION

This research presents a robust framework for the detection and analysis of crypto-ransomware and related cyber fraud using advanced machine learning and blockchain analytics. Unlike traditional detection systems that rely solely on signatures or heuristics, the proposed model leverages behavioral features, anomaly detection, and transaction analysis to identify and mitigate ransomware threats early. It provides actionable insights not only into technical infection patterns but also financial footprints on the blockchain.

The integration of multiple data sources and AI techniques leads to higher accuracy, lower false positives, and faster response times. As ransomware continues to evolve with encryption sophistication and stealth techniques, this system ensures proactive defense, real-time alerting, and traceable attribution of attacks. The approach also supports cybersecurity researchers and forensic investigators in tracking and disrupting the financial chains of organized cybercriminal groups.

VIII.FUTURE SCOPE

The future of ransomware detection lies in automation, decentralization, and resilience. This research opens doors for various improvements, such as integrating federated learning where models are trained across distributed endpoints (e.g., enterprise networks) without compromising privacy. The system can be further enhanced by incorporating AI-driven honeypots, which simulate vulnerable systems to attract and study ransomware behavior in real time.

Moreover, the cryptocurrency tracing module can expand to support cross-chain analysis (e.g., Monero, Ethereum mixers) and deploy AI-based wallet attribution techniques to link anonymous wallets with criminal identities. Real-time smart contract analysis, AI-based intrusion detection in networks, and self-healing file systems are additional enhancements that can strengthen ransomware resilience.

This framework can also be scaled and deployed as a cloud-based SaaS (Security as a Service) solution or integrated into national-level cybersecurity operations centers (CSOCs) for critical infrastructure protection.

IX.REFERENCES

- Kharraz, A., Arshad, S., Mulliner, C., Robertson, W., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. In Proceedings of the DIMVA.
- Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). Automated dynamic analysis of ransomware: Techniques, challenges and research directions. arXiv preprint arXiv:1609.03020.
- Huang, W., Li, J., Liang, B., & Zou, D. (2017). Detecting ransomware with honeypot techniques. Computers & Security, 70, 92–104.
- Ugarte-Pedrero, X., Santos, I., Bringas, P. G., & Alvarez, G. R. (2016). Countering CryptoWall and CTB-Locker ransomware. In Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses.
- Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security, 79, 162–189.
- Anderson, B., Storlie, C., & Lane, T. (2018). Improving malware classification: bridging the static/dynamic gap. ACM Transactions on Information and System Security, 21(1), 1-28.
- Kurniawan, D., Nugraha, F. A., & Wibowo, A. (2020). Tracking Ransomware Bitcoin Payment with Graph Analysis. International Journal of Computer Applications, 177(9), 11–17.
- Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity of critical infrastructures: Recent trends and

future directions. Future Generation Computer Systems, 88, 636–643.

- Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.
- Moser, M., Bohme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In Proceedings of the eCrime Researchers Summit.