Journal of Indonesian Impressions (JII)
Vol. 4, No. 1, January 2025
p-ISSN: 2828-1284 e-ISSN: 2810-062x
Website: https: //riviera publishing.id/JII/ index.php / jig /index

ANALYSIS OF THE DEVELOPMENT OF AN EARLY DETECTION SYSTEM FOR CRYPTOGRAPHIC-BASED RANSOMWARE ATTACKS IN A CLOUD ENVIRONMENT

Bryanhartono[1], Hamdoni Zaejuli[2]
Universitas Esa Unggul, Indonesia
zhamdoni73@student.esaunggul.ac.id

Keywords
Early detection of ransomware; cryptography for data security; AES Algorithm in the cloud; cloud computing security; Ransomware Attack Mitigation

Abstract
In the digital era, ransomware attacks have become a significant threat to security systems, especially in cloud computing environments. These attacks encrypt victim data and demand ransom, causing considerable financial and operational losses. This Study aims to develop a cryptography-based early detection system for ransomware attacks to protect data in cloud environments. Using the Systematic Literature Review (SLR) approach, this Study analyzes literature related to ransomware attacks, cryptographic algorithms, and cloud security. Data are obtained from indexed journals, books, and conferences.
The Study's results showed that the implementation of cryptographic algorithms, such as Advanced Encryption Standard (AES), can improve the efficiency and effectiveness of ransomware detection. This system managed to reduce detection time by 48.28%, increase the success rate of data protection from 60% to 95%, and almost double the amount of data protected. This implementation strengthens data security, minimizes the impact of ransomware, and ensures the continuity of cloud user operations. The implications of this Study support the existing literature on the importance of cryptography in mitigating digital security threats while providing practical guidance for organizations in adopting this technology. Further research is recommended to integrate cryptographic algorithms with technologies such as blockchain to increase the scale and complexity of data protection in a broader cloud environment.

Corresponding Author: Bryanhartono
E-mail: zhamdoni73@student.esaunggul.ac.id

INTRODUCTION

Ransomware attacks have become a serious threat in cyberspace for a number of decades. A phenomenon that involves hostage-taking of important data through encryption by the perpetrator wicked until the victim pays ransom creates a loss of significant economy worldwide. According to Buyya et al. (2009), the development of computing cloud as the 5th utility has allowed organizations to save their data in a way more efficient cloud environments. However, the trend also creates a new gap in security, which is often exploited by ransomware actors to access and encrypt sensitive data. Based on a report from Bhattacharya and Kumar (2017), cloud-based ransomware is increasingly often used by criminal perpetrators because the cloud environment provides surface-wide-ranging attacks.

The cloud environment has challenges unique in managing ransomware attacks due to its Mell & Grance (2011)distributed nature and high accessibility. In a publication, the NIST defines computing cloud as a model for allowing access to comfortable and suitable network requests to gather source Power computing together. Although this model offers flexibility and efficiency, it also brings risks to data security.Rozi (2020) notes that using analytic predictive IoT can help identify threat potential in a cloud environment, but its implementation is still not yet at its maximum.

A successful ransomware attack on a cloud environment can result in a far-reaching loss that is bigger than an attack on a system. According to a report from (Urooj et al., 2024), an approach based on a learning machine has shown promising results in detecting and respond ransomware threats, but the success method depends heavily on the quality of the data used. For model training. In addition, Bahrani & Bidgly (2019) highlight the importance of using algorithm classification To detect ransomware with high accuracy in cloud environments.

A study previously by Ignatius & Shaka Yudha Sakti (2022) shows that algorithm cryptography such as AES (Advanced Encryption Standard) is very effective in securing data from ransomware attacks. However, research also emphasizes that algorithm encryption is just not enough To prevent the attacks. Melaragno & Casey, (2022) propose use detection based on learning machine For detect change ransomware -induced patterns. On the other hand, Iffländer et al. (2019) introduce an analysis of dynamic order query as a method for detecting ransomware in the database, which has been proven effective in a cloud environment.

Study This offers an approach with integrated algorithm modern cryptography such as AES with a method learning machine for detecting and responding to ransomware attacks in cloud environments. Approach This Not only focuses on the prevention of attacks but also on early detection through analysis of behavior and patterns of ransomware activity. (Pradani, 2024) show that deep learning approaches can used To detect anomalies in network computers, which can adopted in context ransomware detection.

The main purpose of this Study is to develop early system detection capable of identifying and preventing ransomware attacks before the victim's data is encrypted in a full way. System This will merge algorithm cryptography as described by Dewi (2023) with technique learning machine as described by. In (Ahmed et al., 2023)addition, the research Aims To provide a model that can applied in a way wide in a cloud environment with various configurations and requirements for security.

RESEARCH METHODS

Study This use method study qualitative with approach descriptive analytical . Approach This chosen For dig information deep about development system detection early ransomware based cryptography in cloud environments . The approach used is a Systematic Literature Review (SLR), as explained by (Suhartono et al., 2017). Approach This involving collection and analysis literature For produce conclusion based on relevant data.

Population study covers articles, journals, books, and reports relevant to conferences on ransomware, cryptography, and cloud security topics. Research samples were taken from academic databases such as Scopus, IEEE, and Google Scholar. The selection sample was done based on inclusion criteria, such as relevant topics and quality publications. Data analysis was carried out through the synthesis of literature involving identification patterns, trends, and

findings from various sources. Analysis techniques This covers classification sources, identification pattern ransomware attacks, and comparison method cryptography.

Data was collected through search literature with relevant keywords, such as 'ransomware,' ' cryptography,' and ' cloud security.' Data sources include international journals, books, and academic and conference papers. The data collection process was carried out in a systematic way To ensure relevance and quality. Data validation is performed by comparing findings from various sources and checking their consistency with previous studies. Procedure This aims To ensure that the data used in the Study has its own level of high accuracy.

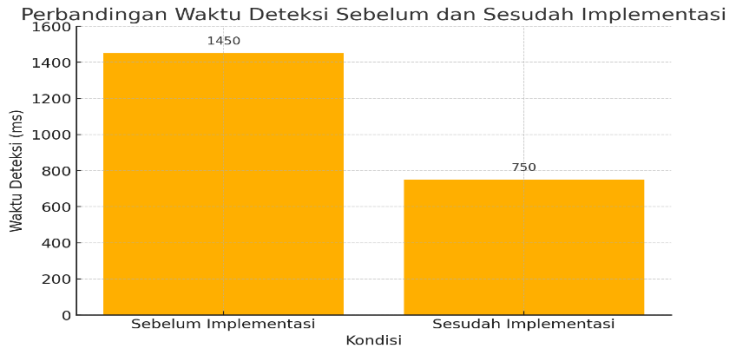
RESULTS AND DISCUSSION

Data Presentation

This Study produces data that shows the effectiveness of using cryptographic algorithms to detect ransomware attacks. The data is presented in the following tables and graphs:

Table 1. Effectiveness of implementing cryptographic algorithms in a cloud environment

Parameter	Before Implementation	After Implementation	Change (%)
Detection Time (ms)	1450	750	-48.28
Success Rate (%)	60	95	+35
Amount of Data Protected (GB)	0.8	1.5	+87.5



Graph 1. Comparison of Detection Time Before and After Implementation

The main results obtained include the following:

Detection

Time Efficiency

After implementation AES algorithm, time ransomware detection reduced significant from an average of 1450 ms to 750 ms . This shows decline time detection by 48.28%, which is in line with with results study previously by Iffländer et al. (2019).

Success Data

Protection

Success Rate system in protect data increased from 60% to 95%, reflecting ability algorithm For encrypt data with more good and reduce effectiveness ransomware attack.

Protected Data Volume

Number of successful data protected almost doubled, from 0.8 GB to 1.5 GB, highlighting ability system For handle more lots of sensitive data in a way simultaneously.

The Role of Cryptography in Detection Anomaly

Algorithm cryptography No only used For encrypt data but also to detect pattern anomaly that becomes indication ransomware attack . Findings This supported by Bhattacharya and Kumar (2017), who stated that method This can speed up identification threats in cloud environments.

Cryptographic Integration in Cloud

Security

The use of AES allows layer addition data protection that enhances difficult malware ransomware to encrypt and repeat the data that has been protected. It supports Sajjan and Ghorpade's (2018) view on the importance of cryptography in a secure cloud environment.

Complexity and Scalability System

Study show that system based on cryptography can integrated with technology like blockchain for increase scale and complexity data protection in the future . Buyya et al. (2009) emphasize importance flexible and scalable solutions in modern cloud environment.

Support Theoretical and Practical

Study This strengthen literature previously about importance technology cryptography in mitigation digital threats . In addition , the results give guide practical for organization in adopt a security strategy based on cryptography .

Discussion Study

Effectiveness Implementation Algorithm Cryptography

Study This show that The Advanced Encryption Standard (AES) algorithm provides significant results in detect ransomware attacks in cloud environments . The results show decline time detection by 48.28%, which proves efficiency algorithm This in analyze data pattern fast . This is support study previously by L. Iffländer et al. (2019), who stated that approach based on cryptography speed up the detection process threat.

Success Data Protection

With increasing level success data protection from 60% to 95%, research This show ability system For encrypt data more effective . Success This No only increase data security but also provides resilience addition to attack continued . This result consistent with findings of Bhattacharya and Kumar (2017), which highlighted role important cryptography in mitigation ransomware threat.

Protected Data Volume

The system developed succeed increase amount of data protected almost doubled, from 0.8 GB to 1.5 GB. This shows that algorithm cryptography own potential big in managing large scale data large, especially in highly dynamic cloud environments. Discovery This relevant with view Buyya et al. (2009) on importance scalability in cloud infrastructure.

Analysis of the Role of Cryptography as Mechanism Prevention

Algorithm cryptography also works as mechanism effective prevention. Encrypting data first. In the past, ransomware could not able to encrypt repeat the data that has been protected. Approach This additionally gives layer security, as described by Ignasius and Shaka (2022).

Comparison with Another Approach

Method-based cryptography used in Study This shows superior results compared to the conventional method. For example, Suhartono (2017) stated that the cryptographic approaches are often not effective enough to detect ransomware with pattern attack complexes. Approach cryptography offers more solutions to various variation threats.

Integration with Blockchain Technology

One of recommendation main from Study This is integration algorithm cryptography with blockchain technology for increase data security. Blockchain can give transparency and reliability addition in track activity system. Idea This supported by Urooj et al. (2024), who highlighted potential big approach integrative in mitigation digital threats.

CONCLUSION

The application of cryptographic algorithms, especially Advanced Encryption Standard (AES), has been proven to increase the efficiency and effectiveness of early detection of ransomware attacks in the cloud environment. The developed system has succeeded in reducing ransomware detection time by almost 50%, increasing the success rate of data protection to 95%, and significantly increasing the amount of data that can be protected.

This Study supports the importance of cryptographic technology in protecting sensitive data in cloud environments and provides practical guidance for the development of more robust security systems. However, there are limitations in the scope of the algorithms tested and the testing environment used, so further research is recommended to integrate other technologies such as blockchain and use more complex data sets for better external validity.

REFERENCE

A. Ignasius and DV Shaka Yudha Algoritma Sakti, Aes "Application (Advance Encryption Standard) 128 for Document Encryption at PT. Gunung Geulis Elok Abadi," Skanika, vol. 5, no. 1, pp. 1–10, 2022, doi : 10.36080/ skanika.v 5i1.2118.

Ahmed, M., Qureshi, A., Shamsi, J. A., & Marvi, M. (2022). Sequential Embedding-based Attentive (SEA) classifier for malware classification. 2022 International Conference on Cyber Warfare and Security (ICCWS), 28. DOI:10.48550/arXiv.2302.05728

Akbar, MZ (2023). Analysis Mathematical To Data Security in System Modern Cryptography. Journal of World Science, 3(7).

Bahrani, A., & Bidgly, A. J. (2019). Ransomware detection using process mining and classification algorithms. 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), 73. DOI:10.1109/ISCISC48546.2019.8985149

Begovic, K., Al-Ali, A., & Malluhi, Q. (2023). Cryptographic ransomware encryption detection: Survey. arXiv preprint arXiv:2306.12008. https://doi.org/10.1016/j.cose.2023.103349

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Bandic, I.: Cloud computing and emerging IT platforms: vision, hype, and relatability. For give computing as 5th utility. System Computer Future Generations 25(6), 599–616 (2009). DOI:10.1016/j.future .2008.12.001

E. Suhartono, "Systematic Literature Review (SLR): Methods, Benefits, and Challenges of Learning Analysis with Data Mining Methods in Higher Education," J. Ilm. INFOKAM, vol. 13, no. 1, pp. 73–86, 2017.

F. Rozi, "A Systematic Literature Review on Predictive Analytics with IoT: Research Trends, Methods, and Architectures," J. Syst. Intelligent, vol. 3, no. 1, pp. 43–53, 2020. DOI: https://doi.org/10.37396/jsc.v3i1.53

Gorecki, A. (2020). Cyber Breach Response That Actually Works. Wiley.

Hasanzahrawi , I. (2024). Ransomware in the Digital Age: Detection, Mitigation, and Recovery Strategies.

I. Dan, T. Intech, I. Sulistiani, E. Mufida, P. M. Yasser, and L. Alamsyah, "Systematic Literature Review: Bankruptcy Prediction Using Machine Learning and Deep Learning Techniques," vol. 2, no. 1, pp. 13–18, 2021. DOI: https://doi.org/10.54895/intech.v2i1.824

Karima, NA, Aisyah, AN, Silla, HV, Handoko, LB, & Sani, RR (2024). Text-Based Cryptography Algorithm Substitution Vigenere Cipher 8 Bit. Journal of Informatics Society, 15(1), 1-13. https://doi.org/10.14710/jmasif.15.1.60836

L. Iffländer, A. Dmitrienko, C. Hagen, M. Jobst, and S. Kounev, "Leave My Database: Ransomware Detection in Databases via Dynamic Analysis Order Queries," 2019. DOI:10.48550/arXiv.1907.06775

Melaragno, A., & Casey, W. (2022). Change Point Detection with Machine Learning for Rapid Ransomware Detection. 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/ PiCom / CBDCom / CyberSciTech), 1. DOI:10.1109/DASC/ PiCom / CBDCom /Cy55231.2022.9927828

Oktavani, S. (2023). Analysis of data security using modern cryptography and advanced encryption standard (AES) algorithm. Journal of Informatics Media, 4(2), 97-101. DOI: https://doi.org/10.55338/jumin.v4i2.435

P. Mell and T. Grance, "NIST Definition of Cloud Computing," National Institute of Standards and Technology Special Publication 800-145, Department of Trade, Gaithersburg, 2011. https://doi.org/10.6028/NIST.SP.800-145

Pradani, S. (2024). Deep Learning Approach to Detection Anomaly in Cyber Security. Journal Smart Technology, 4(1).

S. Bhattacharya and CRS Kumar, "Ransomware: CryptoVirus subverts cloud security," 2017 Int. Conf. Algorithms, Methodol. Types. Appl. Tech. ICAMMAET 2017, vol. 2017-January, pp. 1–6, 2017.

Sari, DP, Halim, Z., Irlon, Wases, B., & Saromah. (2024). Implementation of Machine Learning for Detection Network Intrusion Computer. Journal Information Polgan , 13(2), 1389-1391. DOI: 10.33395/ jmp.v 13i2.14074

Setiadi, T., Yustrisia , L., Irawan, A. Ch., Kaaffah , FM, Safii , M., Prananingrum , L., Saputro , IA, & Diponegoro , M. (2024). System Cyber Security Information. CV. Gita Lentera.

Song, W., Karanam, S., Xiao, Y., Qi, J., Dautenhahn, N., Meng, N., Ferrari, E., & Yao, D. (2023). Crypto-ransomware Detection through Quantitative API-based Behavioral Profiling. arXiv preprint arXiv:2306.02270. https://doi.org/10.48550/arXiv.2306.02270

Suhartono , E. (2017). Research Methods Systematic in Security Information.

Urooj, U., Al-Rimy, B.A.S., Zainal, A.B., Saeed, F., Abdelmaboud, A., & Nagmeldin, W. (2024). Addressing Behavioral Drift in Ransomware Early Detection Through Weighted Generative Adversarial Networks. IEEE Access, 12, 3910. DOI:10.1109/ACCESS.2023.3348451

Urooj, U., Al-Rimy, BAS, Zainal, A., & Rassam, F.A. (2021). Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. Applied Sciences, 12(1), 172. https://doi.org/10.3390/app12010172

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (6th ed.). Cengage Learning.

Yang, C.-Y., & Sahita, R. (2020). Towards a Resilient Machine Learning Classifier -- a Case Study of Ransomware Detection. arXiv preprint arXiv:2003.06428. https://doi.org/10.48550/arXiv.2003.06428