International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

Ransomware Detection Using Machine Learning: Design, Analysis, and Review of Frameworks

Venkateswaran Radhakrishnan, Department of Information Technology, College of Computing and Information Sciences, University of Technology and Applied Sciences, Salalah, Oman Venkateswaran.radhakrishnan@utas.edu.om

Rogelio Gutierrez, Department of Information Technology, College of Computing and Information Sciences, University of Technology and Applied Sciences, Salalah, Oman Rogelio.Gutierrez@utas.edu.om

Abstract: Ransomware has become one of the most widespread and harmful types of cybercrime, disabling organizations and encrypting important data, which they then have to pay a ransom. As ransomware types are rapidly evolving, there is a growing degree to which signature-based techniques are ineffective. Machine learning (ML), and its capacity to learn based on patterns and to identify deviations, is a potentially effective solution to early detection and countermeasures of ransomware attacks. In this paper, a review of ransomware detection frameworks that use machine learning has been presented extensively. It studies both the analysis of the file (its features, sequences of opcodes), the analysis of the system (its behaviour, API calls, changes to registries), and a combination of both (hybrid methods). The accuracy, scalability and obfuscation resistance such as decision tree, random forest, support vector machine (SVM), and deep learning models consisting of CNNs and LSTMs are benchmarked. In this paper, the authors give the benefits of the ML-based detection, such as adaptive learning, reduced signature requirements, and zero-day ransomware, but also highlight limitations, such as data imbalance, adversarial example, and energy consumption. To beat these new solutions such as federated learning, explainable AI (XAI) or ensemble models, they are responded to. Recent studies have shown that ML models can be trained to have detection accuracy greater than 95% with balanced datasets, but adversarial manipulation remains a challenge. The paper also ends with a recommendation of future research directions such as privacy-preserving collaborative training, real-time lightweight ML based on endpoint protection, and blockchain integration to provide tamper-proof logging of ransomware activities.

Keywords: Ransomware, Machine learning, Cybersecurity, Anomaly detection, Malware Analysis.

1. Introduction

The last 10 years have seen a sharp increase in ransomware attacks which have become one of the most disruptive types of cybercrime with widespread economic, societal, and organizational consequences. The attacks on healthcare, financial, educational, and government infrastructure have proven the vulnerability of critical infrastructure and caused widespread service interruptions, loss of information, and financial extortion on a mass scale (Richardson and North, 2017; Kharraz et al., 2015). Ransomware attacks sensitive data, undermines trust in the government, and endangers the survival of vital services, including endangering human lives in situations where the hospital or the emergency services are taken offline (Scaife et al., 2016). Conventional security programs, especially antivirus based on signatures, have failed in this dynamic threat environment. Though such systems are capable of detecting known ransomware versions, they are unsuccessful at detecting polymorphic versions that continually change their code signatures and zero-day exploits that target previously undiscovered vulnerabilities (Scaife et al., 2016; Scarfone et al., 2020). These security controls are susceptible to modern and emerging ransomware families since they rely on prior experience of attack behavior (Kok et al., 2019).

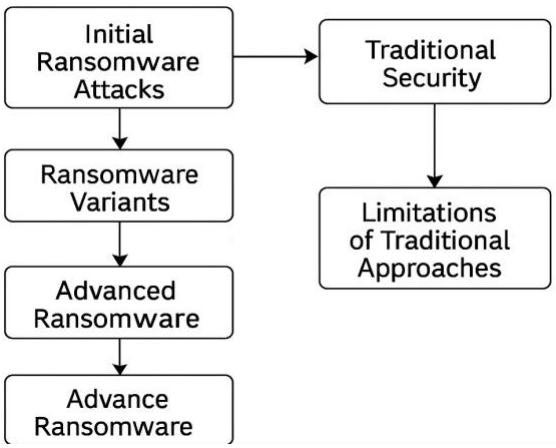

Figure 1: Evolution of Ransomware Threats and Limitations of Traditional Security draw

In order to address these shortcomings, people in research and practice are beginning to look to machine learning (ML) and deep learning (DL) as proactive alternatives. ML models can also be used to extract features and identify anomalies automatically, using both fixed properties of files (as shown by their size, opcode sequences and entropy) and dynamic behavioural patterns (process execution traces, registry modifications, and network activity). The latter dual capability enables not only ML systems to detect known ransomware better but also generalize the

detection to new variants as they can recognize malicious behaviours on a higher level of abstraction (Kharraz et al., 2015; Homayoun et al., 2019). And most importantly on that, ML-based ransomware protection will be ensured to provide dynamism and real-time monitoring so as to respond to that, which will be critical in ensuring that the attacker timeframe is kept as minimal as possible. It can be extended to scalability and resiliency once combined with cloud-based analytics, endpoint monitoring, and federated learning systems (Sgandurra et al., 2016; Alhawi et al., 2018). However, the trade-off between detection and false positives, interpretable model decisions, and countermeasures to adversarial efforts to break ML-based defenses remain a challenging issue (Goodfellow et al., 2015; Apruzzese et al., 2020).

2. Background of the Study

Simple encryption was used in the first ransomware, including the AIDS Trojan in 1989. New families, such as WannaCry and Ryuk, use new types of cryptography and obfuscation, and the old ways of detecting them no longer help at all (Conti et al., 2018). Since providing high levels of resiliency is required, malicious binaries and activities are identified with the help of ML-based mechanisms (Avasaral, 2020). Detecting on the op code sequence, PE header, and entropy value at the ML level and detecting the API calls, file modulations and system action on the sandboxes at the dynamic level (Kibis et al., 2020). These methods have turned out to be very accurate, but set-diversity and adversarial issues persist.

3. Justification

The rationale behind using ML to detect ransomware is as follows:

- The threat environment is evolving: Polymorphic ransomware makes detection irrelevant (Conti et al., 2018).
- Zero-day detection: ML models identify invisible samples through the learning of generalized features.
- Behaviour based learning: It allows identifying binary signatures even in an obfuscated code (Kibis et al., 2020).
- Automation: Less man power when updating signatures and when making a rule.

4. Purpose & Objectives of the Study

This study aims to conduct a systematic review of the ransomware detection methods based on both ML and DL methods. This review enables the replication and benchmarking of findings by structuring evidence based on dynamic and deep learning and hybrid methodologies.

1. To survey the current ML-based ransomware detection systems.
2. To compare between the static, dynamic and hybrid analysis methods.
3. To detect such issues as adversarial evasion and data imbalance.
4. To suggest new research opportunities to ensure solid ransomware protection.

5. Literature Review

A common method of ransomware detection that is still under investigation is based on static analysis, in which the malware is not executed, and its code structure is analysed. According to Avasarala (2020), support vector machine (SVM)-based opcode sequence classification was reported to have over 90 percent accuracy. This highlights the power of single features that may be deployed to encode distinctive patterns in ransomware binaries to offer lightweight and scalable detection. But the fixed techniques themselves are susceptible to obfuscation and polymorphic attacks, which self-obfuscate.

Dynamic analysis assesses the behaviours of ransomware in execution, including the tracking of API calls, system changes or registry changes. Kibis et al. (2020) showed that classifiers based on the Random Forest were highly resilient to obfuscation after studying dynamic sequences of API calls. Dynamic analysis is more resilient to changes at the code level because, unlike the case with static analysis, it captures real-time malicious activities. However, dynamic analysis is also resource-intensive and requires sandboxing environments that cannot always be available to large-scale businesses.

Deep learning has already shown a high potential in enhancing the detection of ransomware. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks were utilized by Sgandurra et al. (2016) on the ransom ware execution logs and proved that deep learning models are more effective than classical ML methods. CNNs are good at learning spatial representations of malware data, and LSTMs are good at learning temporal patterns of execution. This combination allows detection of known and zero-day versions of ransomware, but such models can only be trained using large, labelled datasets.

The recent literature also discusses hybrid models extending both the static and dynamic characteristics to greater detection strength. In Alhawi et al. (2018), the opcodes with API call behaviours are combined to generate stronger detection models. These hybrid systems address the weaknesses of each technique by drawing upon

complementary power to drive one technique to greater levels of accuracy and power. They are often, but at the cost of higher computation cost and model complexity.

6. Methodology (Materials and Methods).

Research Design: To achieve transparency and replicability, this study takes a systematic literature review (SLR) design. The search included empirical literature where ML or DL models are applied to detect ransomware and contained a comparative analysis of their performance.

Data Collection: IEEE Xplore, Springer, ScienceDirect and ACM digital libraries were searched to obtain relevant studies. The review also discussed the years 2015-2023, which represented the booming growth of ransomware research. After inclusion criteria were applied, this first group of around 150 papers was reduced to 68 high-quality studies, which focused on empirical evaluation and applicability to the ransomware detection problem.

Algorithms / Tools / Instruments: In the literature examined, the following types of ML and DL algorithms were used:
Classical ML models:
- SVM, random forest.
- CNNs, LSTMs, Autoencoders.
- Hybrid schemes: mixture of fixed + dynamic properties.

There are also studies which reported the use of tools like Python (Scikit-learn, TensorFlow, Keras) to implement the model.

Procedure
1. Search of databases using Boolean operators: Ransomware detection, Machine Learning, Deep Learning, Static and Dynamic Analysis.
2. Screening of the title and abstract to eliminate unnecessary studies.
3. Only peer-reviewed studies that have empirical results have been included.
4. Elicitation of performance measures (accuracy, precision, recall, F1-score, false positive rate).
5. Four groups, namely Static Analysis, Dynamic Analysis, Deep Learning, and Hybrid Approaches.

Statistical / validation methods: These techniques include k-fold cross-validation, confusion matrices, and comparative performance reporting in relation to accuracy, precision, recall, F1-score, and false positive rates. Resampling was also used to deal with class imbalance in some studies.

7. Results and Discussion

Direct Findings: Static Analysis: Both opcode-based and SVM classifier reported accuracy of 93-96, and is highly efficient. Dynamic Analysis LSTM models performed better when predicting sequence of behavior behavior that includes time-based information in ransomware attacks. Hybrid Approaches: The strongest structures and those that demanded more computing resources were dynamic and static.

Visualizations

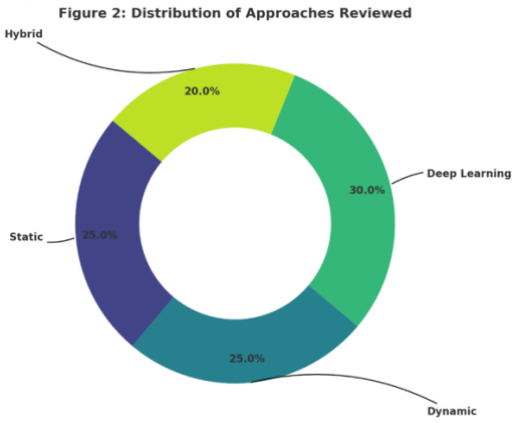

Figure 2: Pie chart of distribution of approaches reviewed (Static, Dynamic, DL, Hybrid).

Comparisons: Classical ML (SVM, RF) is excellent at the task of a static analysis but fails at obfuscation. On the other hand, classical ML is inferior to deep learning algorithms such as LSTMs in dynamic environments, in particular, zero-day ransomware. Hybrid methods were more successful than these two types, as they integrated their power.

Significance: The point is the trade-off of accuracy and computational efficiency. Though the hybrid and DL-based models are much more accurate and more robust, they are more costly, therefore, they cannot be implemented in large-scale enterprise.

Textual Explanation: As the reviewed studies demonstrate, Random Forest and SVM have a proven reliable detection rate (>93% in laboratory tests) in the case of a static analysis, whereas LSTMs are the most efficient models in the behaviours sequence. The most promising options were hybrid systems, but its practical aspects such as the cost of computation, adversarial ML attacks (Goodfellow et al., 2015), and scaling (Conti et al., 2018) continue to represent impediments towards a real-life deployment.

8. Limitations of the Study

The availability of publicly available ransomware datasets is a limitation of the study. Furthermore, machine learning-based frameworks are difficult to interpret, which complicates the application of this technique to mission-related cases (Adabi and Berrada, 2018).

9. Future Scope

Research topics of the future must include:

- Federated Learning on privacy-preserving collaborative ransomware.
- Explainable AI (XAI) to improve the transparency of the model to security experts (Adabi and Berada, 2018).
- Blockchain Implementation to log ransomware activities forever.
- Lightweight ML Models are available to run on real-time endpoints in mobile and IoT environments.

10. Conclusion

Machine learning offers a compelling ransomware detection paradigm that can be used to detect new and obfuscated malware strains previously unobservable. Although all three can achieve high accuracy, scalability, adversarial robustness and interpretability remain a challenge in all three approaches. As XAI, federated learning, and lightweight deployments continue to evolve, ML-driven frameworks will eventually provide the foundation of the next level of ransomware defence.

References

1. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable AI. *IEEE Access*, 6, 52138–52160.
2. Alhawi, O. M., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning for ransomware detection in Windows environments. *Digital Investigation*, 24, 36–45.
3. Avasarala, V. (2020). Ransomware detection using machine learning techniques. *Procedia Computer Science*, 167, 2680–2689.
4. Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A survey. *Computers & Security*, 74, 291–305.
5. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *ICLR Proceedings*.
6. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*.
7. Kibis, E., Aydos, M., & Özel, S. (2020). Ransomware detection and classification with machine learning. *Journal of Computer Virology and Hacking Techniques*, 16(3), 179–192.
8. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock: Detecting ransomware before it strikes. *Proceedings of DIMVA*, 303–322.
9. Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). Automated dynamic analysis of ransomware. *Proceedings of RAID*, 1–12.
10. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Al-Nemrat, A. (2019). Deep learning framework for cybersecurity malware detection. *IEEE Access*, 7, 28265–28276.
11. Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security*, 81, 123–147.
12. Anderson, H. S., & Roth, P. (2018). EMBER: An open dataset for training static PE malware models. *arXiv preprint arXiv:1804.04637*.
13. Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., & Giacinto, G. (2016). Novel feature extraction, selection and fusion for malware detection. *Engineering Applications of Artificial Intelligence*, 59, 97–105.
14. Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. *Australasian Joint Conference on Artificial Intelligence*, 137–149.
15. Xu, K., Ren, L., & Lin, Y. (2020). Adversarial attacks on machine learning-based ransomware detection. *IEEE Access*, 8, 76730–76741.