ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1623

Machine Learning for Cybersecurity: Ransomware Detection with SVM

[1]Wira Zanoramy Ansiry Zakaria; [2]Muhammad Nasim Abdul Aziz; [3]Sharifah Roziah Mohd Kassim

Cyber999, Cybersecurity Malaysia
GC-STKYT-160924-804

Publication Date: 2025/03/17

Abstract: Ransomware attacks pose a significant threat to digital security, necessitating the development of effective detection mechanisms. This paper explores the utilization of Application Programming Interface (API) calls as a pivotal feature in ransomware detection systems. By analyzing the sequence and nature of application API calls, we can discern patterns indicative of malicious behavior. This paper also discusses the challenges associated with API-based detection, including the potential for benign applications to exhibit similar behaviors. Overall, the findings underscore the importance of API calls in developing robust ransomware detection frameworks and highlight ongoing research efforts to improve detection methodologies through innovative feature extraction and machine learning techniques.

Keywords: *Ransomware Detection, Machine Learning, Support Vector Machines (SVM), API Call Analysis, Cybersecurity Threat Mitigation*

How to Cite: Wira Zanoramy Ansiry Zakaria; Muhammad Nasim Abdul Aziz; Sharifah Roziah Mohd Kassim (2025) Machine Learning for Cybersecurity: Ransomware Detection with SVM. *International Journal of Innovative Science and Research Technology*, 10(2), 2173-2180. https://doi.org/10.38124/ijisrt/25feb1623

I. INTRODUCTION

Ransomware has emerged as one of the most pressing threats in the landscape of cybersecurity, characterized by its ability to encrypt victims' data and demand ransom for its release. The evolution of ransomware has seen it transition from simple encryption schemes to sophisticated attacks that exploit vulnerabilities across various platforms, affecting individuals, businesses, and government entities alike (Razaulla et al., 2023; Oz, 2021). The financial implications of such attacks are staggering, with losses amounting to billions of dollars annually, alongside significant reputational damage and operational disruptions (Gunuganti, 2022; Oz, 2021). The proliferation of ransomware is fueled by the increasing accessibility of ransomware-as-a-service (RaaS) models, which enable even less technically skilled criminals to launch attacks (Lee, 2023). This democratization of ransomware has led to a surge in the number of attacks, making it imperative for organizations to adopt robust cybersecurity measures. Understanding the phases of a ransomware attack—from initial infiltration to data encryption and extortion—is crucial for developing effective detection and response strategies (Yamany, 2024; Kang, 2023). over, the dynamic nature of ransomware necessitates continuous research and innovation in detection methodologies. Traditional signature-based detection methods are often inadequate against the evolving tactics employed by ransomware, prompting a shift towards machine learning and behavioral analysis techniques (Hammadeh, 2023; Gurukala, 2023). These advanced approaches leverage data from API calls, system behaviors, and other indicators to identify potential ransomware activities before they can cause significant harm (Mahboubi et al., 2022; Silva & Hernández-Álvarez, 2023). In conclusion, the threat posed by ransomware is multifaceted and ever-evolving, requiring a comprehensive understanding of its mechanisms and the implementation of proactive measures to mitigate risks. As the landscape of cyber threats continues to change, ongoing research and collaboration among cybersecurity professionals will be essential in fortifying defenses against this formidable adversary (Razaulla et al., 2023; Oz, 2021; Shaikh, 2024).

II. MACHINE LEARNING FOR CYBERSECURITY

Machine learning (ML) has emerged as a pivotal technology in the realm of cybersecurity, particularly in the detection and mitigation of cyber threats. The integration of ML techniques into cybersecurity frameworks has significantly enhanced the capabilities of intrusion detection systems (IDS) and other security measures. Various studies have highlighted the effectiveness of both supervised and unsupervised ML approaches in identifying and classifying a wide array of cyber-attacks, thereby addressing diverse cybersecurity concerns (Abushark et al., 2022; Alharbi et al.,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1623

2021; Nazir, 2023). These ML models can analyze vast amounts of data, learning from patterns and anomalies that may indicate potential threats, which is particularly crucial given the increasing complexity and volume of cyber threats today (Fakiha, 2023; Ahsan et al., 2022).

The application of ML in cybersecurity is particularly relevant in the context of the Internet of Things (IoT), where the proliferation of connected devices presents unique security challenges. As the number of IoT devices continues to rise, the need for scalable and effective security solutions becomes paramount. Machine learning-based anomaly detection and predictive analytics have shown promise, enabling real-time threat detection and response (Ling, 2023; More, 2020). The ability of ML algorithms to adapt and learn from new data makes them well-suited for the dynamic nature of IoT security ("Artificial Intelligence with Respect to Cyber Security", 2023).The proactive nature of AI and ML technologies has been instrumental in minimizing the impact of cyberattacks. By providing real-time responses and automating threat detection processes, these technologies enhance the overall security posture of organizations ("Leveraging AI and ML for Advance Cyber Security", 2022; Mustafa, 2023). However, it is important to acknowledge that while ML offers significant advantages, it also presents challenges, such as the need for continuous algorithm retraining and the potential for adversarial attacks that can exploit vulnerabilities in ML systems (Zhang et al., 2020). Thus, a comprehensive understanding of both the capabilities and limitations of ML in cybersecurity is essential for developing robust security frameworks.

Machine learning is critical in enhancing cybersecurity measures through its ability to detect, classify, and respond to cyber threats effectively. The ongoing research and development in this field continue to push the boundaries of what is possible, making ML an indispensable tool in the fight against cybercrime (Handa et al., 2019; Musser & Garriott, 2021). As organizations increasingly adopt these technologies, it is crucial to remain vigilant about the evolving landscape of cyber threats and the corresponding advancements in machine learning methodologies.

A. Machine Leaning for Ransomware Detection

Machine learning (ML) application in ransomware detection has gained significant traction in recent years, driven by the increasing sophistication and prevalence of ransomware attacks. Ransomware, a type of malicious software that encrypts a victim's files and demands a ransom for their release, poses a critical threat to both individuals and organizations. Traditional detection methods, such as signature-based approaches, often fall short in identifying new or variant strains of ransomware, necessitating the adoption of ML techniques that can analyzebehavioral patterns and adapt to evolving threats ("Machine Learning Classifier Algorithms for Ransomware Lockbit Prediction", 2024; Gong, 2024; Smith et al., 2022). Machine learning algorithms have been effectively employed to enhance ransomware detection capabilities through various methodologies. For instance, studies have demonstrated that classifiers such as Decision Trees, Random Forests, and Support Vector Machines can be utilized to categorize and detect ransomware based on their dynamic behaviors (Masum et al., 2022; Almomani et al., 2021; Khalil & Khammas, 2022). These algorithms analyze features extracted from files and system behaviors, allowing for the identification of ransomware even before it executes its payload. In particular, dynamic analysis approaches, which monitor the behavior of software during execution, have shown detection rates exceeding 96% when combined with ML techniques (Park & Razak, 2022; Alhawi et al., 2018). over, recent advancements in ML have led to the development of hybrid models that integrate multiple algorithms to improve detection accuracy and reduce false negatives. For example, the use of Generative Adversarial Networks (GANs) has been proposed to enhance the classification of ransomware by adapting to the changing landscape of malware (Gong, 2024). Additionally, the incorporation of entropy-based features has been explored as a means to identify encrypted files characteristic of ransomware, although this method can be circumvented by sophisticated ransomware variants that avoid high entropy values (Davies et al., 2022; Lee, 2024). The evolution of ransomware detection methodologies also includes the exploration of ensemble learning techniques, which combine the strengths of various ML models to achieve superior performance (Zhang, 2024). These approaches not only improve detection rates but also enhance the interpretability of the models, allowing security professionals to understand the underlying decision-making processes of the algorithms (Marcinkowski, 2024). Furthermore, the application of few-shot learning techniques has emerged as a promising avenue for addressing the challenges posed by limited training data in ransomware classification tasks (Wang, 2023). In conclusion, machine learning has proven to be a transformative force in the field of ransomware detection. By leveraging advanced algorithms and dynamic analysis techniques, ML enhances the ability to identify and mitigate ransomware threats effectively. As ransomware continues to evolve, ongoing research and development in ML methodologies will be crucial for staying ahead of these cyber threats and protecting sensitive data from malicious actors ("Machine Learning Classifier Algorithms for Ransomware Lockbit Prediction", 2024; Smith et al., 2022).

B. SVM for Ransomware Detection

Support Vector Machines (SVM) have emerged as a prominent technique for ransomware detection, leveraging their ability to classify complex data patterns effectively. SVM is a supervised machine learning algorithm that excels in both linear and nonlinear classification tasks, making it particularly suitable for identifying the diverse behaviors exhibited by ransomware (Park & Razak, 2022; Ngirande, 2024). The application of SVM in ransomware detection typically involves training the model on features extracted from various data sources, such as API calls, file attributes, and behavioral patterns, to distinguish between benign and malicious software (Almomani et al., 2021). Research has demonstrated the efficacy of SVM in detecting ransomware across different platforms, including Android and Windows. For instance, a study focused on Android ransomware utilized SVM to classify and analyze ransomware samples,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1623

achieving significant detection accuracy (Ngirande, 2024). Similarly, another study highlighted the use of SVM in a hybrid evolutionary approach to enhance ransomware detection, where the algorithm was optimized through Particle Swarm Optimization (PSO) to improve feature selection and classification performance (Almomani et al., 2021). These findings underscore the adaptability of SVM in addressing the challenges posed by ransomware's evolving nature. over, SVM has been compared with other machine learning algorithms in various studies, often demonstrating competitive performance. For example, in a comparative analysis of different classifiers, SVM achieved high accuracy rates, often surpassing other models such as Decision Trees and Random Forests (Dendere, 2024). In one notable study, SVM was reported to achieve an area under the ROC curve (AUC) of 0.987, indicating its robustness in detecting high-survivable ransomware attacks (Ahmed et al., 2020). This high performance is attributed to SVM's capability to construct hyperplanes that effectively separate data points in high-dimensional spaces, allowing for precise classification of ransomware behaviors. The integration of SVM with advanced feature extraction techniques has further enhanced its detection capabilities. For instance, the use of entropy-based features has been explored to identify encrypted files characteristic of ransomware, with SVM demonstrating a detection rate exceeding 85% in some cases (Hsu et al., 2021). Additionally, the application of the Lapranove function to improve feature extraction has shown promise in boosting SVM's performance in identifying ransomware (Zhong, 2024). These advancements highlight the ongoing research efforts aimed at refining SVM methodologies to keep pace with the rapidly evolving ransomware landscape. In conclusion, Support Vector Machines represent a powerful tool in the arsenal against ransomware, offering effective classification capabilities that can adapt to the complexities of modern cyber threats. The continued exploration of SVM in conjunction with innovative feature extraction and optimization techniques is essential for enhancing ransomware detection systems and ensuring robust cybersecurity measures (Park & Razak, 2022; Ngirande, 2024; Almomani et al., 2021; Dendere, 2024; Ahmed et al., 2020).

C. Feature Selection

Feature selection is a critical component in developing effective ransomware detection systems, as it directly influences the accuracy and efficiency of machine learning models. Selecting relevant features helps improve detection rates while reducing computational overhead and the risk of overfitting. Various approaches have been proposed in the literature to optimize feature selection for ransomware detection, employing techniques such as mutual information, evolutionary algorithms, and ensemble methods. One notable method is mutual information criteria for selecting dynamic features, as demonstrated in the EldeRan framework. This approach focuses on features such as registry key operations, API calls, and file system activities, which are crucial for identifying ransomware behavior. The study found that the proposed technique outperformed existing methods, highlighting the importance of selecting relevant features for effective ransomware detection (Zahoora et al., 2022; . Similarly, another study introduced the Ransomware Feature Selection Algorithm (RFSA), which utilizes Gini Impurity and Mutual Information to identify essential features that capture the unique characteristics of ransomware activity (Nkongolo, 2024). This algorithm enhances the understanding of ransomware dynamics through correlation matrices and temporal analysis. In addition to mutual information, other feature selection techniques have been explored. For instance, the incremental mutual information-selection technique proposed by aims to adaptively select relevant features during the early stages of ransomware attacks, thereby improving detection capabilities in real-time scenarios (Gazzan, 2024). This method processes data in smaller batches, reducing computational load and allowing for quicker adaptation to new ransomware variants. over, the application of Particle Swarm Optimization (PSO) has been employed to enhance feature selection in conjunction with ensemble classifiers. This approach helps identify a crucial feature subset that significantly improves detection accuracy (Gurukala, 2023). Integrating PSO with machine learning models has shown promise in addressing the high dimensionality of feature spaces commonly encountered in ransomware detection tasks. Furthermore, advanced techniques such as the Lapranove function have been proposed to improve feature extraction and enhance the performance of machine learning models, including Support Vector Machines and Random Forests (Zhong, 2024). This novel approach aims to refine the feature set used for training, ultimately leading to more reliable ransomware detection. In conclusion, effective feature selection is paramount for the success of ransomware detection systems. The ongoing research into various feature selection methodologies, including mutual information, PSO, and advanced statistical techniques, continues to enhance the capabilities of machine learning models in identifying and mitigating ransomware threats. As ransomware evolves, the development of robust feature selection strategies will be essential for maintaining effective cybersecurity defenses (Zahoora et al., 2022; Nkongolo, 2024; Gazzan, 2024; Gurukala, 2023; Zhong, 2024).

D. API Calls as Feature

API calls serve as a crucial feature in the detection of ransomware, as they provide insights into the behavior of applications during execution. By analyzing the sequence and nature of API calls made by software, researchers can identify patterns indicative of ransomware activity. This approach has gained traction due to API calls' ability to reveal the software's underlying intentions, particularly in distinguishing between benign and malicious behaviors. Several studies have highlighted the effectiveness of using API calls as features for ransomware detection. For instance, demonstrated that analyzing Windows API calls, particularly file-related I/O calls, can significantly enhance the detection of ransomware. Their method involved extracting API call sequences from a dataset comprising benign and malicious samples, generating n-grams of API calls to capture the contextual behavior of the software (Bold et al., 2022). This approach underscores the importance of sequence analysis, as ransomware typically

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1623

employs a series of API calls to execute its malicious actions rather than relying on isolated calls. over, the work by Al-Rimy et al. emphasizes the role of API calls in delineating the pre-encryption boundaries of ransomware attacks. Their pseudo feedback-based technique monitors cryptography-related API calls during an attack, allowing for the identification of critical moments when ransomware begins to encrypt files (Al-rimy et al., 2020). This capability is vital for early detection and prevention, as it enables security systems to intervene before significant damage occurs. The integration of machine learning with API call analysis has further enhanced ransomware detection capabilities. For example, utilized Support Vector Machines (SVM) to train models on API call features, demonstrating the algorithm's effectiveness in recognizing patterns associated with ransomware (Park & Razak, 2022). Similarly, noted that many machine learning-based detection solutions focus on API calls, highlighting their relevance in identifying abnormal behaviors characteristic of ransomware (Mahboubi et al., 2022). Additionally, the research conducted by found that API calls achieved a balanced accuracy of 96.49% in distinguishing ransomware from benign applications. Their findings indicated that while native encryption APIs were not crucial for classification, features related to thread/process handling and physical memory operations were significant indicators of ransomware behavior (Moreira et al., 2022). This suggests that a comprehensive analysis of API calls, beyond just encryption-related functions, is essential for effective detection. Furthermore, the use of advanced techniques such as n-grams and Term Frequency-Inverse Document Frequency (TF-IDF) for API sequence data has shown promise in enhancing detection accuracy. 's study on early detection methods for ransomware demonstrated the effectiveness of these techniques in generating feature vectors from API sequences, which were then used to train machine learning classifiers (Zhang, 2023). This approach illustrates the potential for leveraging API call data to improve the robustness of ransomware detection systems. In summary, API calls represent a vital feature in the detection of ransomware, providing valuable insights into application behavior. The ongoing research into the analysis of API call sequences, combined with machine learning techniques, continues to enhance the capabilities of ransomware detection systems, making them more effective in identifying and mitigating threats before they can cause significant harm (Al-rimy et al., 2020; Bold et al., 2022; Park & Razak, 2022; Mahboubi et al., 2022; Moreira et al., 2022; Zhang, 2023).

III. RESEARCH METHODOLOGY

Research methodology refers to the systematic framework that guides researchers in the planning, execution, and analysis of their studies. It encompasses the theoretical underpinnings, research designs, and specific methods employed to collect and analyze data, ensuring that the research is valid, reliable, and applicable to the intended context. Various methodologies exist, including qualitative, quantitative, and mixed methods approaches, each serving distinct purposes and addressing different research questions. For instance, qualitative methodologies focus on exploring phenomena in-depth, while quantitative methods emphasize statistical analysis and generalizability (Caldas, 2003; Barella, 2023; Abutabenjeh & Jaradat, 2018). The choice of methodology is influenced by the research objectives, the nature of the research question, and the context in which the research is conducted, leading to ongoing discussions about the appropriateness and effectiveness of different methodologies (Kalolo, 2015; Johnson & Onwuegbuzie, 2004; Alise & Teddlie, 2010). Ultimately, a well-defined research methodology not only enhances the credibility of the findings but also contributes to the advancement of knowledge within a given field (Monson, 2021; Steen et al., 2021).

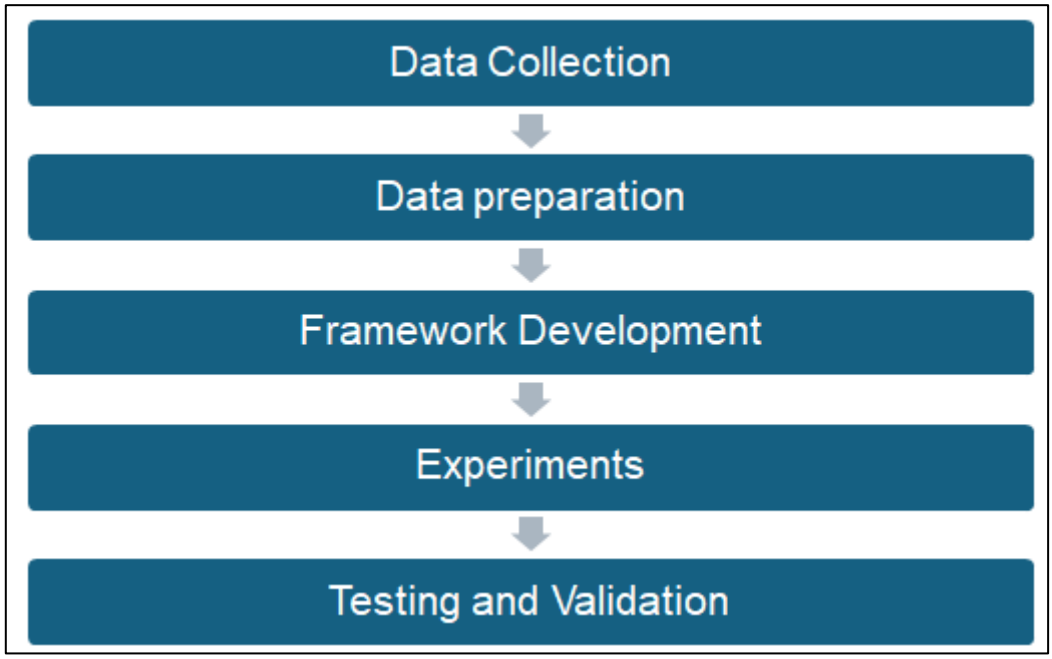

Fig 1. Research Methodology for this Study.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1623

IV. RESULTS

The performance of five classifiers—SVM, Random Forest, kNN, J48, and Naïve Bayes—was evaluated based on Accuracy, True Positive Rate (TPR), and False Positive Rate (FPR). SVM outperformed the others with the highest accuracy of 97.05%, the highest TPR of 0.995, and a low FPR of 0.071, making it the most reliable choice. Random Forest also showed strong performance with an accuracy of 96.39%, TPR of 0.984, and a similarly low FPR of 0.071, closely followed by kNN, which had an accuracy of 96.07%, TPR of 0.979, and FPR of 0.071. J48, while still effective, had a slightly lower accuracy of 94.75% and a higher FPR of 0.106, indicating more false positives. Naïve Bayes had the lowest accuracy of 80.98%, the lowest TPR of 0.781, and the highest FPR of 0.142, making it the least reliable classifier in this context. Overall, SVM is the best performer, with Random Forest and kNN as strong alternatives, while J48 and Naïve Bayes show moderate to lower effectiveness for this problem. Table 1 shows the results of five classifiers.

Table 1 Results from Five Classifiers

Classifier	Accuracy	TPR	FPR
Random Forest	96.3934%	0.984	0.071
Naïve Bayes	80.9836%	0.781	0.142
SVM	97.0492%	0.995	0.071
kNN	96.0656%	0.979	0.071
J48	94.7541%	0.979	0.106

V. FUTURE WORKS

Future research in ransomware detection using machine learning should focus on enhancing the adaptability and robustness of detection models to cope with evolving ransomware tactics. One promising direction is the integration of deep learning models with advanced feature extraction techniques, such as sequence-based API call analysis and entropy-based features, to improve detection accuracy and reduce false positives. Additionally, exploring the potential of few-shot learning and transfer learning methods could help overcome challenges related to limited labeled data for new ransomware variants. Collaborative efforts between academia, industry, and government agencies to develop standardized datasets and benchmarks for ransomware detection could also facilitate the advancement of more effective and generalizable detection models.

VI. CONCLUSION

This study highlights the significant potential of machine learning, particularly Support Vector Machines (SVM), in detecting ransomware based on dynamic behavioral analysis. The results demonstrate that SVM outperforms other classifiers such as Random Forest and k-Nearest Neighbors, achieving the highest accuracy and true positive rate in distinguishing between benign and malicious behaviors. By leveraging features such as API calls and file attributes, SVM can effectively detect ransomware activities with minimal false positives. As ransomware continues to evolve, the continuous improvement of machine learning models and feature selection techniques will be crucial in enhancing the resilience of cybersecurity systems against these ever-evolving threats.

REFERENCES

[1]. (2022). Leveraging AI and ML for advance cyber security. Design of Single Chip Microcomputer Control System for Stepping Motor, 1-3. https://doi.org/10.47363/jaicc/2022(1)142
[2]. (2023). Artificial intelligence with respect to cyber security. JAAI, 1(2), 96-102. https://doi.org/10.18178/jaai.2023.1.2.96-102
[3]. (2024). Machine learning classifier algorithms for ransomware Lockbit prediction. Journal of Applied Data Sciences, 5(1), 24-32. https://doi.org/10.47738/jads.v5i1.161
[4]. (2024). Machine learning classifier algorithms for ransomware lockbit prediction. Journal of Applied Data Sciences, 5(1), 24-32. https://doi.org/10.47738/jads.v5i1.161
[5]. Abushark, Y., Khan, A., Alsolami, F., Almalawi, A., Alam, M., Agrawal, A., … & Khan, R. (2022). Cyber security analysis and evaluation for intrusion detection systems. Computers Materials & Continua, 72(1), 1765-1783. https://doi.org/10.32604/cmc.2022.025604
[6]. Abutabenjeh, S. and Jaradat, R. (2018). Clarification of research design, research methods, and research methodology. Teaching Public Administration, 36(3), 237-258. https://doi.org/10.1177/0144739418775787
[7]. Ahmed, Y., Koçer, B., & Al-rimy, B. (2020). Automated analysis approach for the detection of high survivable ransomware. Ksii Transactions on Internet and Information Systems, 14(5). https://doi.org/10.3837/tiis.2020.05.021

[8]. Ahsan, M., Nygard, K., Gomes, R., Chowdhury, M., Rifat, N., & Connolly, J. (2022). Cybersecurity threats and their mitigation approaches using machine learning—a review. Journal of Cybersecurity and Privacy, 2(3), 527-555. https://doi.org/10.3390/jcp2030027
[9]. Al-rimy, B., Maarof, M., Alazab, M., Alsolami, F., Shaid, S., Ghaleb, F., … & Ali, A. (2020). A pseudo feedback-based annotated tf-idf technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction. Ieee Access, 8, 140586-140598. https://doi.org/10.1109/access.2020.3012674
[10]. Alharbi, A., Seh, A., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., … & Khan, R. (2021). Analyzing the impact of cyber security related attributes for intrusion detection systems. Sustainability, 13(22), 12337. https://doi.org/10.3390/su132212337
[11]. Alhawi, O., Baldwin, J., &Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection., 93-106. https://doi.org/10.1007/978-3-319-73951-9_5
[12]. Alise, M. and Teddlie, C. (2010). A continuation of the paradigm wars? prevalence rates of methodological approaches across the social/behavioral sciences. Journal of Mixed Methods Research, 4(2), 103-126. https://doi.org/10.1177/1558689809360805
[13]. Almomani, I., Qaddoura, R., Habib, M., Alsoghyer, S., Alkhayer, A., Aljarah, I., … & Faris, H. (2021). Android ransomware detection based on a hybrid evolutionary approach in the context of highly imbalanced data. Ieee Access, 9, 57674-57691. https://doi.org/10.1109/access.2021.3071450
[14]. Barella, Y. (2023). Analysis on the nature, functions, and process of research: revealing the characteristics of scientific research, types of research, and classification in research. Edumaspul - Jurnal Pendidikan, 7(2), 3866-3871. https://doi.org/10.33487/edumaspul.v7i2.7031
[15]. Bold, R., Al-Khateeb, H., &Ersotelos, N. (2022). Reducing false negatives in ransomware detection: a critical evaluation of machine learning algorithms. Applied Sciences, 12(24), 12941. https://doi.org/10.3390/app122412941
[16]. Caldas, M. (2003). Research design: qualitative, quantitative, and mixed methods approaches. Revista De AdministraçãoContemporânea, 7(1), 223-223. https://doi.org/10.1590/s1415-65552003000100015
[17]. Davies, S., Macfarlane, R., & Buchanan, W. (2022). Comparison of entropy calculation methods for ransomware encrypted file identification. Entropy, 24(10), 1503. https://doi.org/10.3390/e24101503
[18]. Dendere, T. (2024). Ransomware detection using portable executable imports. International Conference on Cyber Warfare and Security, 19(1), 66-74. https://doi.org/10.34190/iccws.19.1.2031
[19]. Fakiha, B. (2023). Enhancing cyber forensics with ai and machine learning: a study on automated threat analysis and classification. International Journal of Safety and Security Engineering, 13(4), 701-707. https://doi.org/10.18280/ijsse.130412
[20]. Gazzan, M. (2024). An incremental mutual information-selection technique for early ransomware detection. Information, 15(4), 194. https://doi.org/10.3390/info15040194
[21]. Gong, W. (2024). Ransomware detection and classification using generative adversarial networks with dynamic weight adaptation.. https://doi.org/10.31219/osf.io/5vju7
[22]. Gunuganti, A. (2022). Ransomware evolution and defense strategies. Journal of Engineering and Applied Sciences Technology, 1-4. https://doi.org/10.47363/jeast/2022(4)261
[23]. Gurukala, N. (2023). Feature selection using particle swarm optimization and ensemble-based machine learning models for ransomware detection.. https://doi.org/10.21203/rs.3.rs-3604834/v1
[24]. Gurukala, N. (2023). Feature selection using particle swarm optimization and ensemble-based machine learning models for ransomware detection.. https://doi.org/10.21203/rs.3.rs-3604834/v1
[25]. Hammadeh, K. (2023). Unraveling ransomware: detecting threats with advanced machine learning algorithms. International Journal of Advanced Computer Science and Applications, 14(9). https://doi.org/10.14569/ijacsa.2023.0140952
[26]. Handa, A., Sharma, A., & Shukla, S. (2019). Machine learning in cybersecurity: a review. Wiley Interdisciplinary Reviews Data Mining and Knowledge Discovery, 9(4). https://doi.org/10.1002/widm.1306
[27]. Hsu, C., Yang, C., Cheng, H., Setiasabda, P., & Leu, J. (2021). Enhancing file entropy analysis to improve machine learning detection rate of ransomware. Ieee Access, 9, 138345-138351. https://doi.org/10.1109/access.2021.3114148
[28]. Johnson, R. and Onwuegbuzie, A. (2004). Mixed methods research: a research paradigm whose time has come. Educational Researcher, 33(7), 14-26. https://doi.org/10.3102/0013189x033007014
[29]. Kalolo, J. (2015). The drive towards application of pragmatic perspective in educational research: opportunities and challenges. Journal of Studies in Education, 5(1), 150. https://doi.org/10.5296/jse.v5i1.7145
[30]. Kang, Q. (2023). A survey on ransomware threats: contrasting static and dynamic analysis methods.. https://doi.org/10.20944/preprints202311.0798.v1
[31]. Khalil, N. and Khammas, B. (2022). An effective and efficient features vectors for ransomware detection via machine learning technique. Iraqi Journal of Information & Communications Technology, 5(3), 23-33. https://doi.org/10.31987/ijict.5.3.205

[32]. Lee, J. (2024). A study on countermeasures against neutralizing technology: encoding algorithm-based ransomware detection methods using machine learning. Electronics, 13(6), 1030. https://doi.org/10.3390/electronics13061030
[33]. Lee, S. (2023). Hiding in the crowd: ransomware protection by adopting camouflage and hiding strategy with the link file. Ieee Access, 11, 92693-92704. https://doi.org/10.1109/access.2023.3309879
[34]. Ling, M. (2023). Machine-learning-based network sparsificationmodeling for iots security analysis.. https://doi.org/10.1117/12.2690061
[35]. Mahboubi, A., Ansari, K., Camtepe, S., Duda, J., Morawiecki, P., Pawlowski, M., … &Pieprzyk, J. (2022). Digital immunity module: preventing unwanted encryption using source coding.. https://doi.org/10.36227/techrxiv.17789735
[36]. Marcinkowski, B. (2024). Mirad: a method for interpretable ransomware attack detection.. https://doi.org/10.21203/rs.3.rs-3909256/v1
[37]. Masum, M., Faruk, M., Shahriar, H., Qian, K., Lo, D., & Adnan, M. (2022). Ransomware classification and detection with machine learning algorithms.. https://doi.org/10.1109/ccwc54503.2022.9720869
[38]. Monson, M. (2021). Socially responsible design science in information systems for sustainable development: a critical research methodology. European Journal of Information Systems, 32(2), 207-237. https://doi.org/10.1080/0960085x.2021.1946442
[39]. More, P. (2020). Machine learning for cyber threat detection. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.1 S I), 41-46. https://doi.org/10.30534/ijatcse/2020/0891.12020
[40]. Moreira, C., Sales, C., & Moreira, D. (2022). Understanding ransomware actions through behavioral feature analysis. Journal of Communication and Information Systems, 37(1), 61-76. https://doi.org/10.14209/jcis.2022.7
[41]. Musser, M. and Garriott, A. (2021). Machine learning and cybersecurity: hype and reality.. https://doi.org/10.51593/2020ca004
[42]. Mustafa, R. (2023). Subject review: cyber security using machine learning and deep learning techniques. Global Journal of Engineering and Technology Advances, 16(2), 212-219. https://doi.org/10.30574/gjeta.2023.16.2.0161
[43]. Nazir, I. (2023). Impact of machine learning in cybersecurity augmentation., 147-154. https://doi.org/10.48001/978-81-966500-9-4_12
[44]. Ngirande, H. (2024). Detection and analysis of android ransomware using the support vector machines. International Journal for Research in Applied Science and Engineering Technology, 12(1), 241-252. https://doi.org/10.22214/ijraset.2024.57885
[45]. Oz, H. (2021). A survey on ransomware: evolution, taxonomy, and defense solutions.. https://doi.org/10.48550/arxiv.2102.06249
[46]. Park, H. and Razak, M. (2022). Dynamic ransomware detection for windows platform using machine learning classifiers. Joiv International Journal on Informatics Visualization, 6(2-2), 469. https://doi.org/10.30630/joiv.6.2-2.1093
[47]. Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B., … &Assi, C. (2023). The age of ransomware: a survey on the evolution, taxonomy, and research directions. Ieee Access, 11, 40698-40723. https://doi.org/10.1109/access.2023.3268535
[48]. Shaikh, M. (2024). Fortifying against ransomware: navigating cybersecurity risk management with a focus on ransomware insurance strategies. International Journal of Academic Research in Business and Social Sciences, 14(1). https://doi.org/10.6007/ijarbss/v14-i1/20566
[49]. Silva, J. and Hernández-Álvarez, M. (2023). Dynamic feature dataset for ransomware detection using machine learning algorithms. Sensors, 23(3), 1053. https://doi.org/10.3390/s23031053
[50]. Smith, D., Khorsandroo, S., & Roy, K. (2022). Machine learning algorithms and frameworks in ransomware detection. Ieee Access, 10, 117597-117610. https://doi.org/10.1109/access.2022.3218779
[51]. Steen, J., Bloomer, M., & Pereira, S. (2021). The importance of methodology to palliative care research: a new article type for palliative medicine. Palliative Medicine, 36(1), 4-6. https://doi.org/10.1177/02692163211069566
[52]. Wang, F. (2023). A few-shot learning approach with a twin neural network utilizing entropy features for ransomware classification.. https://doi.org/10.31219/osf.io/bzhxu
[53]. Yamany, B. (2024). A holistic approach to ransomware classification: leveraging static and dynamic analysis with visualization. Information, 15(1), 46. https://doi.org/10.3390/info15010046
[54]. Zahoora, U., Khan, A., Rajarajan, M., Khan, S., Asam, M., & Jamal, T. (2022). Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive pareto ensemble classifier. Scientific Reports, 12(1). https://doi.org/10.1038/s41598-022-19443-7
[55]. Zhang, R. (2024). Ransomware detection with a 2-tier machine learning approach using a novel clustering algorithm.. https://doi.org/10.21203/rs.3.rs-4567706/v1
[56]. Zhang, S. (2023). Early detection and defense countermeasure inference of ransomware based on api sequence. International Journal of Advanced Computer Science and Applications, 14(10). https://doi.org/10.14569/ijacsa.2023.0141067
[57]. Zhang, S., Xie, X., & Yang, X. (2020). A brute-force black-box method to attack machine learning-based systems in cybersecurity. Ieee Access, 8, 128250-128263. https://doi.org/10.1109/access.2020.3008433
[58]. Zhong, T. (2024). Ransomware detection with machine learning by applying the lapranove function on bytecode.. https://doi.org/10.31219/osf.io/zk3sw

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1623

AUTHORS' INFORMATION FORM

Paper Title: Machine Learning for Cybersecurity: Ransomware Detection with SVM

First Author – Information

First Name	WIRA ZANORAMY ANSIRY	Last Name	ZAKARIA
Designation	SENIOR ANALYST	Department	CYBER999
University	CYBERSECURITY MALAYSIA	Mail ID	wira@cybersecurity.my
Contact No.		ORCID ID	
Residential Address			

Second Author – Information

First Name	MUHAMMAD NASIM	Last Name	ABDUL AZIZ
Designation	SENIOR EXECUTIVE	Department	CYBER999
University	CYBERSECURITY MALAYSIA	Mail ID	nasim@cybersecurity.my
Contact No.		ORCID ID	
Residential Address			

Third Author - Information

First Name	SHARIFAH ROZIAH	Last Name	MOHD KASSIM
Designation	HEAD OF DEPARTMENT	Department	CYBER999
University	CYBERSECURITY MALAYSIA	Mail ID	wira@cybersecurity.my
Contact No.		ORCID ID	
Residential Address			

AUTHOR'S BIOGRAPHY

Wira Z. A. Zakaria is a cybersecurity professional with extensive experience as a senior analyst and lead researcher at Cyber999, Cybersecurity Malaysia. Concurrently pursuing a PhD at UniversitiTeknikal Malaysia Melaka, Wira's research focuses on ransomware early detection using dynamic analysis. With a background that includes roles at MyCERT, Maxis, MIMOS, MEPS, UM, Silterraand HeitechPadu, Wira combines practical expertise with academic insight to advance the field of cybersecurity.

Nasim Aziz is a seasoned Senior Executive at CyberSecurity Malaysia, currently serving in the Cyber999 department. With over a decade of experience at the Malaysia Computer Emergency Response Team (MyCERT), he has played a pivotal role in managing IT security projects critical to the department's operations. Nasim has extensive experience in international CSIRT affiliations, including FIRST, APCERT, and OIC-CERT, and has conducted audits for several CERT/CSIRT organizations to ensure compliance before their inclusion in these global security networks.Nasim is currently pursuing a Doctorate in Information Security at Universiti Teknikal Malaysia Melaka (UTeM), where his research focuses on developing a governance framework to mitigate malware attacks.

Dr. Sharifah Roziah is the Head of Cyber999 at Cybersecurity Malaysia. She is a highly experienced incident response professional and trainer, known for her expertise in managing and mitigating cybersecurity incidents. Dr. Roziah has delivered talks at prominent cybersecurity conferences such as FIRST, APCERT and IEEE conference, sharing her insights on advanced incident response strategies. She also leads the national incident response team, playing a critical role in safeguarding Malaysia's cyberspace by effectively handling and coordinating responses to various cybersecurity threats.