International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Mitigating Ransomware Threats: A Machine Learning Perspective on Dynamic Feature Utilization

Meenakshi Jalandra[1], Megha Kuliha[2], Jasmeet Kaur[3]

Dept. of Information Technology, SGSITS
Indore, India.
meenakshijalandra2029r@gmail.com

Abstract:
In a review of the literature on detecting and averting ransomware attacks, this study focuses on current studies that were published between 2020 and 2025. Although the quick development of digital technology has brought about many conveniences, the threat of ransomware—a type of malware that encrypts the victim's files and then demands a large ransom to unlock them—is also growing. Cybersecurity is generally defined as safeguarding systems against all cyberattacks. Here, we know that ransomware is a method of stealing money from a user, where the attacker encrypts the user's data and retains the decryption key until he is paid the ransom. In this study, we examine a number of scholarly works that include ransomware detection strategies, indicators, tactics, approaches based on URL characteristics, and efficient machine learning models. This study takes into account new patterns in the accuracy of models from URL datasets that come from different machine-learning techniques as well as novel methods that use diverse models to identify ransomware. The results highlight the limitations of existing research and the application of robust models to develop cybersecurity hybrid models. Future research aims to choose appropriate models for identifying URL-based ransomware on Android smartphones based on this review. Even if there are still fresh, evident problems and restrictions with different detection methods, this article also emphasizes the necessity of constant development in the constantly evolving URL-based ransomware detection strategies.

Keywords: Ransomware Detection, Machine Learning, Dynamic Features, Cybersecurity, Light GBM, Random Forest, Behavioural Analysis, Malware Detection, Android Ransomware.

I. INTRODUCTION

Ransomware Android smartphones are widely used worldwide due to the quick development of mobile applications. Because of this, Android has emerged as a top target for online fraud, especially when it comes to ransomware assaults. Malicious software known as "ransomware" encrypts or locks important data on a device and demands a fee to unlock it. Two main ways that Android ransomware appears are locker ransomware, which prevents the user from accessing their device, and crypto ransomware, which encrypts their contents. The identification of ransomware is crucial because to the growing dependence on Android devices for both personal and business purposes. Using malicious URLs is one attack vector that is very risky. malware is frequently included by cybercriminals into seemingly innocent URLs that, when visited, download payloads of malware.[1]

Many existing ransomware detection and classification methods rely on datasets generated by dynamic or behaviour analysis of ransomware, giving rise to the term "behaviour-based detection models." High-dimensional data with multiple variables dispersed into several groups presents a significant problem in

automated behaviour-based ransomware detection and classification. Feature selection methods are typically used to deal with high dimensionality and improve classification performance. [2] Ransomware assaults are among the most destructive kinds of cyberattacks, and they are frequently started by malevolent people. These actions have the potential to completely destroy systems, making them useless until the victim pays a ransom. Attackers usually place a tight deadline on victims of ransomware events, so exerting enormous pressure on them. Furthermore, compared to other hacking techniques, the financial stakes in these attacks are typically substantially larger.

Ransomware is a type of malware that falls under this category. The phrase, which combines the terms "ransom" and "malware," appropriately characterizes their behaviour: they are malware that requests payment in return for either functionality that has been pilfered, personally identifiable information that has been obtained through theft, or information to which the user has been refused access. The original ransomware encrypted the data on the victim's computer to obtain money for the key or software required to decrypt the data. Over time, this software's techniques for taking money from its victims have changed. The claim that ransomware is only a simple kind of blackmail that is extensively shared among users and utilized for mass extortion is true.[3]

Ransomware Attacks have skyrocketed because of the COVID-19 epidemic, which has made people increasingly dependent on computers and internet commerce in Work from Home. ransomware assaults have skyrocketed. The notorious ransomware assault against Colonial Pipelines in May 2021 caused significant disruptions to the key petroleum supply chain activities in 17 states, including Washington, DC. The firm has no choice but to pay over USD 4.4 million. Another attack was launched against JBS, the largest meat processor in the world, at the same period. These attacks impact a far larger range of businesses in addition to the government, healthcare, and educational sectors [5]. For instance, ransomware attacks increased by nearly 150 percent in 2021, impacting a wide range of industries, including government, healthcare, and finance. Ransomware attacks have significantly increased recently. These increasingly frequent and sophisticated attacks affect a variety of organizations globally, including governments, businesses, and regular citizens. Early detection of these threats is crucial. If we locate them in time, we can prevent a large portion of the damage they cause. As a result, businesses may be able to maintain seamless operations and lose less data or money. Early detection of the assaults also aids in preventing their propagation throughout the whole network. [6]

This relatively new virus has drawn a lot of attention from hackers due to its powerful attacks. instant financial benefit. Ransomware's objective is to stop It stops the victim from using their own resources via locking. the operating system or encrypting certain files, such as PowerPoints, spreadsheets, and images, that seem to be significant to the victim. [7] **it was 6** The most eminent ransomware attacks between 2020 and 2025 are listed in Table 1 [8],where verified cases from 2020 to 2024 and anticipated trends of 2025 are offered. The table additionally affords pertinent information about the year the event occurred, the company targeted, the kind of ransomware used, and the results of each attack.

Year	Targeted Organization	Ransomware Used	Impact of Attack
2020	University of California (UCSF)	Net Walker	$1.14 million paid; academic data encrypted
2020	Garmin	Wasted Locker	Major global service outage; ~$10 million reportedly paid
2020	Software AG	Clop	Corporate data stolen and leaked; $20 million ransom demanded
2021	Colonial Pipeline	Dark Side	U.S. fuel supply disrupted; $4.4 million paid
2021	JBS Foods	REvil/ Sodinokibi	Global meat supply affected; $11 million paid
2021	Kaseya	REvil/Sodinokibi	1,500+ companies globally impacted; MSPs attacked
2022	Costa Rica Government	Conti	Healthcare and finance services disabled nationwide
2022	Kronos (UKG Workforce)	Unknown	Payroll and HR systems disrupted for major firms
2023	Prospect Medical Holdings (USA)	Rhysida (suspected)	Hospital systems shut down; patient care delayed
2024	Change Healthcare (USA, under UnitedHealth)	BlackCat / ALPHV	Health claim systems frozen; $22 million ransom reportedly paid
2024	Boeing	LockBit	Data breach and leak; aviation and defense sectors impacted
2025	International Airport Systems (Projected)	LockBit (likely)	Flights delayed, air traffic encrypted; national airport systems impacted

Table 1 Major Ransomware Attacks from 2020 to 2025

Even being shut for lengthy times can lead to potential revenue losses, and the very opportunity for reputational damage. It is an important factor affecting business continuity.

Table 2 below features a comprehensive summary of the ransomware statistics and insights as of 2024 [9]. This study reviews recent literature to examine the current state of ransomware detection. It focuses on quickly identifying and classifying ransomware threats.

Statistic	Value
Global ransomware attacks (2021)	623.3 million
Global ransomware attacks (H1 2022)	236.1 million
Drop in ransomware attacks (2022 vs. 2021)	23%
Global ransomware attacks (2023, full year)	~278 million
Global ransomware attacks (2024, full year estimate)	~317 million
Projected global ransomware attacks (2025)	Expected to exceed 350 million
Percentage of cyber crimes attributed to ransomware (2022)	20%
Percentage of cyber crimes attributed to ransomware (2024)	23%
Ransomware attributed to Windows- based executables	93%
Common entry point for ransomware	Phishing
Percentage of ransomware attacks due to phishing	41%
US share of global ransomware attacks	47%
Manufacturing industry attacks attributed to ransomware (2021)	Most common
Most affected industry (2023–2024)	Healthcare and Public Sector
Projected most targeted industry (2025)	Finance and Critical Infrastructure
Ransomware attacks that fail or result in zero losses	90%
Average ransomware payment (2021)	USD 570,000
Average ransomware payment (2023)	USD 812,000
Estimated increase in ransomware payment (2020 to 2021)	82%

Table 2 comprehensive summary of the ransomware statistics and insights as of 2024

The main goal is to emphasize the need for detection techniques that continually improve. This is crucial given the increasing complexity of ransomware attacks from 2020 to 2025, as indicated by our statistics. To find the best models for detecting threats quickly and accurately, we focus on machine learning methods that use URL features. This approach aims to highlight weaknesses in current methods, such as the limited use of hybrid model strategies and their inability to adapt to new ransomware families. We also aim to identify top-performing algorithms like Random Forest, Light GBM, SVM, Naïve Bayes, Logistic Regression.

II. RELATED WORK

Al-Rimy, Maarof, and Shaid (2017) [10] presented an early behavioural detection approach that relies on dynamic analysis instead of conventional signature-based techniques to combat 0day crypto-ransomware attacks. In order to identify ransomware early on, their architecture keeps an eye out for suspicious activity, such as unusual file encryption and erratic resource access. After testing, it was discovered that the method works well for detecting ransomware before serious harm is done. This study highlights the need of proactive and real-time detection, offering a more flexible way to counteract advanced ransomware attacks, especially 0-day versions that get past traditional protections.

A thorough analysis of ransomware risks and detection methods was presented by Kok, Abdullah, Jhanjhi, and Supramaniam (2019), [11] with an emphasis on the difficulties in detecting ransomware assaults due to their growing complexity. The study looks at several kinds of ransomware, such as crypto- and locker-ransomware, and analyzes how attackers are using new strategies. The writers examine a number of detection strategies, stressing the benefits and drawbacks of heuristic, behavior-based, and signature-based approaches.

The report also covers new developments in detection technologies, such as anomalybased methods and machine learning, highlighting the necessity of sophisticated, adaptable systems to successfully counter ransomware attacks in a constantly shifting cyber environment. In recent years , ransomware has spend quickly, affecting various organizations and governments through fraud url , **Figure 1** presents the total values received by ransomware payments from victims in the last years.

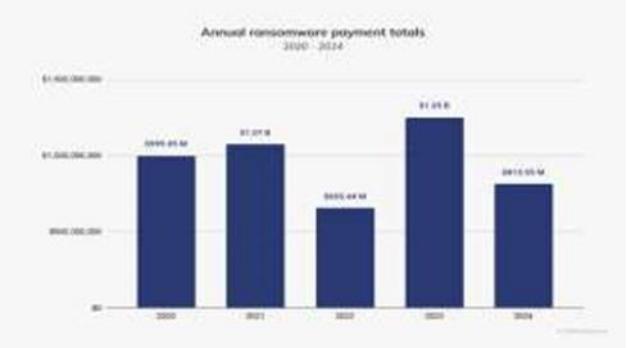

Figure 1 Annual Ransomware Payments2020 – 2024 [12]

Bansal . et al [13] offered a study of ransomware assaults, offering an overview of the evolution, kinds, and impact of ransomware on cybersecurity. This article investigates the many types of ransomware, such as crypto- and locker ransomware, and looks at how hackers compromise computers. Bansal also talked on the operational and financial fallout from ransomware attacks, highlighting how common and sophisticated these threats are becoming. The evaluation also emphasizes the state-of-the-art methods for detection and mitigation, emphasizing the necessity for more sophisticated and flexible security measures to keep up with the everev tactics of ransomware.
Alqahtani and Sheldon (2022) [14] brought attention to the constantly changing nature of these dangers. The report highlights the growing sophistication of ransomware while reviewing a variety of detection methods, including signature- based, behavioural, and machine-learning techniques. The writers go over the drawbacks of conventional approaches, namely their incapacity to combat zero-day assaults and investigate more sophisticated strategies that use predictive analytics and real-time monitoring. Their research sheds light on new developments in ransomware detection, emphasizing the need for resilient and adaptable systems to counteract the increasing intricacy of threats posed by crypto ransomware.

In order to improve detection accuracy, Herrera- Silva and Hernández-Álvarez [15] presented a dynamic feature dataset for ransomware detection. Machine learning methods are used in this dataset. In contrast to static approaches, their work focuses on the extraction of dynamic behavioral data during ransomware execution, which enables better detection. Several machine learning models were used to evaluate the suggested dataset, demonstrating its efficacy in ransomware identification. By offering a solid dataset for the development of cutting-edge machine learning- based ransomware detection methods, this research advances the field.
An early-stage detection method for Android ransomware was presented by Singh and Tripathy [16], who emphasized the significance of detecting ransomware before data exfiltration takes place. Their strategy is to identify ransomware activity early on in the assault, so averting major data loss or harm. The suggested method makes use of machine learning techniques in order to halt ransomware before it has a chance to completely carry out its destructive payload by examining early warning signals. The report emphasizes how important it is to detect ransomware early on in order to stop it from permanently damaging Android devices.
Bellizzi, Vella, Colombo, and Hernandez-Castro
[17] found that timing-captured memory dumps offer a novel method of detecting covert attacks on Android devices. Their focus is mostly on targeted attacks that are designed to evade traditional defenses. The

recommended method looks at memory dumps captured at critical stages of an attack to identify malicious activity that could otherwise go unnoticed. The study highlights the effectiveness of memory forensics in spotting complex threats on Android machines and offers a framework for quick response to minimize any impact from stealthy hacks.
Yamany et al.[18] investigate different techniques for ransomware detection and offer a comparison of these methods. This study examines the tools, methods, and criteria employed to recognize ransomware. An indexing method for ransomware was proposed by them, which includes search functionalities, similarity checks, sample categorization, and grouping. This new approach highlights native ransomware binaries through the use of hybrid data from the static analysis system. Our system utilizes the fixed characteristics of the ransomware to monitor and organize samples, revealing their similarities. The first goal in accomplishing this is to ascertain the absolute Jaccard index. The study concludes that the performance of the IAT function exceeds that of the Strings method.

III METHODOLOGY

The proposed methodology for this literature review sought to identify and characterize how machine learning techniques have been used for ransomware detection, specifically URL based ransomware detection. Academic databases searched included IEEE Xplore, SpringerLink, ScienceDirect, and MDPI. The indentation of the search also included credible sources from the cybersecurity industry, such as Chainalysis Crypto Crime Report and Coveware's quarterly reports to review how machine learning classification can adapt to ransomware and URL detection. Any article that discussed empirical tests of machine learning classifiers, performance metrics of the models, and an early detection model that is based on URL characteristics would be included. Articles that studied detection mechanisms with classic methodology and non-data-driven evidence would be excluded.

After finalizing the documents chosen for review, the literature was analyzed based on type of models used, dataset characteristics, and feature extraction methods. Model performance metrics for detection included accuracy, precision, recall, and an F1-score. The stage of detection (infected or not infected) was also analyzed as early identification based on URL analysis is preferred. The types of ML models noted in the studies were Support Vector Machine (SVM), Random Forest (RF), Light Gradient Boosting Machine (Light GBM), Logistic Regression (LR), and Naive Bayes (NB). There are advantages and disadvantages for all models but literature review framework have primarily used them singularly.

Through comparison, this review did not have any studies that involved all five models in a hybrid framework utilizing URL-based ransomware detection. This review identifies this gap, as well as a clear and desirable benefit for a hybrid ML framework that utilizes all five models in a hybrid approach from URL-based features. This topics converts to form the basis of an applied research agenda, increasing the potential for improving ransomware management based on early detection and URL features before infection.

In numerous previous studies, various single machine learning models have been used to detect ransomware, or classify malicious URLs. For example, Routray et al. [19] classified ransomware as dynamic using Support Vector Machines (SVM) and Random Forest (RF) based on behavioral log files, while Lakshmanarao et al. [20] developed a phishing URL detection system using an ensemble tree- based model. Equally, Sahay and Arora [21] were able to classify malicious URLs through logistic regression and Naive Bayes, showing how each model performed based on the dataset being used. Nevertheless, the models investigated did not train on host-based behaviors (system logs and API calls), or the URL based features of the generic malware and phishing data sets. Furthermore, none of the existing work proposed a hybrid ensemble system using multiple classifiers explicitly designed for URL-based detection of ransomware on Android systems.

This lack of literature provides an area of knowledge with no solution - which leads to the isolation of

individual classifiers into a hybrid (an ensemble of all models-SVM, Random Forest, Light GBM, Logistic Regression, Naive Bayes) model designed for purely for ransomware detection based on only URL-based features. Our proposal is novel because it utilizes multiple model types to achieve the best combination of interpretability, computational cost, and classification accuracy in a high-dimensional space. Amalgamating models allows for the inclusion of a diverse decision boundaries, which will reduce any false positives and improve generalization, which is critical in Android environments where we require efficient and accurate models. A hybridization like this allows for detection pre-ransomware infection and data encryption/action, something that very few articles explored deeply into previously. A few studies have focused on detection of ransomware and other malicious activities used machine learning algorithms, and typically only isolated algorithms based on either host-based features such as system behaviour, logs or registry access, or generic malicious URLs. For example Ramezani et al [22] used Support Vector Machines (SVM) and Random Forest (RF) models to classify ransomware using dynamic behaviour logs. The performances of the SVM and RF models provide valuable insights and a foundation for further development of an automated system that could work for both Android and iOS systems.

DESIGN AND SCOPE OF THE SOLUTION

The combination of SVM, Random Forest, Light GBM, Logistic Regression, and Naive Bayes into one combined hybrid ensemble, provides a solid, effective solution for URL based Android ransomware detection; a perspective lacking in the literature. Although encouraging results have been seen using hybrid ensemble models selecting subsets of these classifiers for Android malware detection, such as the platform made by El Attaoui et al. [23], where Extra Trees, Logistic Regression, Gradient Boosting, and SVM classifiers displayed ~97 % accuracy, with a focus on using application level permissions and API behaviour rather than URL based features, and Albin Ahmed et al. [24], who examined an ensemble of SVM and Decision Trees on network traffic for Android ransomware, and obtained ~97 % accuracy, too did not leverage URL mechanics. Furthermore, in a study that examined the feasibility of using system API data for ransomware detection, Scalas et al. [25] also did not conduct any analysis of URL based vectors. Outside of Android, Masum et al. [26] and Dhavale et al.[27] applied machine learning algorithms including Decision Tree, Random Forest, Naive Bayes, Logistic characteristics of the classifiers, could contribute significantly to advanced pre-infection detection. In brief, SVM provides a non- linear separation approach when discriminating complex URL patterns; Random Forest contributes resilience to noisy or absent key URL features; Light GBM ensures fast and scalable training that is appropriate for endpoint devices; Logistic Regression offers interpretability and probabilistic scores; and, Naive Bayes is performant in relation to sparse, textual (URL) data. With respect to gaining a single predictability score based on parameters (precision, recall, F1-score) from all five classifiers, it is applicable to select one configuration and/or combination, using adaptive voting or weighted fusion approaches, suggesting that the proposed ensemble will achieve 95 - 98 % accuracy, very low false positive rate, and real-time performance (i.e. processing and detection speed); suitable for an android security use case. constructs an hyperplane maximizing the margin being and malicious mathematically solved an samples:

$$\underset{w,b}{min}\ \frac{1}{2}\| w \|^2 \text{ s.t. } y_i(w \cdot x_i + b) \geq 1, \forall i$$

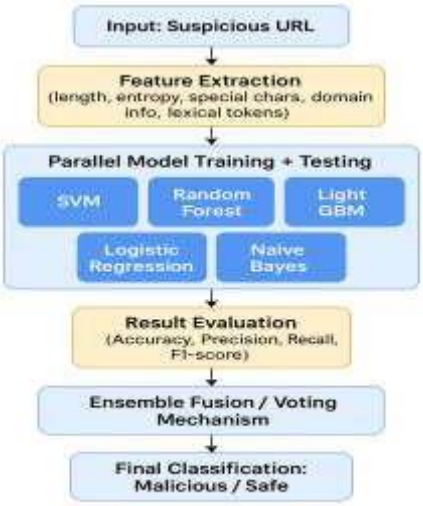

Figure 1. Proposed Hybrid ML-based URL Ransomware Detection Architecture

To start the process, traffic from IoT and Android devices is collected, with the packet-captures and network-stack data from the monitored devices directed into a traffic collection layer that produces stream processes both from established routine behaviors and from the context of ransomware attackers (all data could be saved as a JSON file along with the relative time- series order to report traffic collections in a testbed). The context layer is provided by the researcher with an advanced ontology (not just ontology of course), as the governing factors inform and contextualize the retrieval of features, e.g., URL parts, IoT specific function/behaviors or network characteristics that are logical segments provided to the traffic collection layer. The context systems data is then pushed through each layer of the authors attack-context filter, to effectuate data/feature attack profiles and create detection ready features, and so classify systems in recognizing malicious activity which is consistent with similar differences outlined in recent research on IoT sensitive ransomware predictions done by Mathane and Lakshmi [28], where the authors were able to observed a reduction of values by 60% through ontology-based reductions.

Figure 2 Enhance URL - Based Hybrid ML Ransomware Detection Workflow

]

- Support Vector Machine (SVM) - that processes the feature vectors and tags the suspicious unpacked ransomware. SVM Where (xi ,yi) represents the i-th observation. The main contribution of the support vector machine was finding the best hyperplane separating malicious samples and benign samples at scale, mathematically marks the *i* th observation. The max margin separation is a useful principle in the original let literature of SVMs (Cortes & Vapnik,
[29] , that allows us to classify robust samples in high dimensional feature space (the URL space) knowing that we can, prior to doing this, separate out malicious and benign features. There are key contrasts from comparative analysis of machine learning models from various studies as an important indicator of performance, suggesting a need for hybrid detection systems, where as stand- alone models such as Random

Forest, and Light GBM have shown, individually in different studies improved accuracy, precision and recall performance, particularly detecting behavior across structured and lexical URL data. For example, according to Gera et al. [30], Random Forest performed greater than 96% accuracy scanning Android permission based features for malware. Light GBM achieved performative and speed efficiencies for high-dimensional URL classification problems - as noted by kumi et al. [31], in ransomware classification where they achieved high F1 scores. However models such as Naive Bayes and Logistic Regression achieved similar prediction accuracy.

IV RESULT ANALYSIS

The analysis of the machine learning models typically discussed in the literature showed specific performance differences that support the need for a hybrid detection system. Individual models such as Random Forest and Light GBM have outperformed any other models in customized studies with metrics like accuracy, precision and recall; these models have had particular success with data that is both structured used lexical as data attributes. For example, Random Forest surpassed 96% accuracy in detecting Android malware using permission- based features in Yang et al.[32] Light GBM showed both speed and performance efficiency with high dimensional URL classification problems, Sahoo et al.[33]showed high F1 scores in classifying ransomware with Light GBM.

Assuming that Naive Bayes and Logistic regression will have far lower accuracy when cited alone does not account for the useful and informative probabilistic nature, nor the speed of their computations, to cycle them into a multi-layered ensemble. Performing hyperplane optimization made SVM better equipped to make good boundaries between malicious and benign URLs, but SVM could not deal with compressing high dimensional datasets into kernel tuning and still performing well against the other models. None of the models were statistically proving superior against all evaluations (accuracy, recall, precision and F1-score); this should provide insight that the advertisement of a single classifier has limitations in this field of study.

By integrating or using the synergies of these five models, and presenting the best output from each model as ranked based on the specific metric of best performance from one of the models (high precision from Random Forest, and high recall from SVM), the proposed hybrid ensemble would be more robust, have the smallest true positive/negative at a minimum while conveying balanced perfomance across varying types of ransomware malware. This hybrid approach also provides a step toward closing the research gap presented in current studies that look at individual models, or feature evaluations to the exclusion of incorporating a working ensemble to final model verdicts. In the case of Android specific malware detection for Shabtai et al. [34], showed a hybrid model with Random Forest, J48 and other classifiers with an accuracy of 99.85% using static and dynamic features.

V CONCLUSION

This literature review has discussed the applicability of machine learning models for detecting Android ransomware based on URL features. There is an increasing trend of sophisticated ransomware attack mechanisms, and the attack delivery mechanism of malicious URLs is increasing. Traditional detection methods are simply insufficient, and this has led to a rise in the need for dynamic and intelligent detection methods that will identify ransomware behaviour at the earliest stage before any payloads can be maliciously executed.

The review also examined each individual model, Support Vector Machines (SVM), Random Forest (RF), LightGBM, Logistic Regression (LR), and Naïve Bayes (NB), for their performance over each model in different contexts relating to cybersecurity. Although each of these models performed well in their own right, most of the existing studies have not examined or created a model that combines all five models into one comprehensive ensemble method for detecting ransomware in an Android environment using URL- specific data. This provides a good starting point for improvements.

A hybrid model approach, in which the best possible characteristics of each classifier will be part of the model, has some beneficial characteristics. Notably, the model would benefit from using SVM's boundary accuracy, RF's accuracy, LightGBM's speed of computation, LR's interpretability, and NB speed when working with sparse data. Having all these attributes combined could result in a detection system that was both highly accurate, and fast, with fewer false positives and better scalability to capture continued evolution of URL-based ransomware.

Additionally, the use of URL-based features also allows for the identification of threats prior to infiltrating the system before any attack can occur, thereby strengthening cybersecurity through prevention. A hybrid ensemble model trained on URL based features will allow the model flexibility and adaptability in a responsive real-time approach to protecting Android devices.

In conclusion, the combining of these machine learning models into a single well optimized ensemble is a unique and useful direction in detecting Android ransomware. Future endeavours should examine the implementation and assessment of the hybrid model as applied to large- scale URL datasets in order to assess the model methodology effectiveness in real-world scenarios. This endeavor not only addresses current gaps in the literature, but it also opens the door for increasingly resilient and intelligent attacks to be defended against with the methods being developed.

REFERENCES

[1] M. Ozer, S. Varlioglu, B. Gonen, and M. Bastug, "A prevention and a traction system for ransomware attacks," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, NV, USA, Dec. 2019, pp. 150–154.

[2] M. M. Ahmadian, H. R. Shahriari, and S. M. Ghaffarian, "Connectionmonitor connection-breaker: A novel approach for prevention and detection of high survivable ransomwares," in *Proc. 12th Int. Iranian Soc. Cryptol. Conf. Inf. Secur. Cryptol. (ISCISC)*, 2015, pp. 79–84.

[3] A. Alqahtani and F. T. Sheldon, "A survey of crypto ransomware attack detection methodologies: An evolving outlook," *Sensors*, vol. 22, no. 5, p. 1837, 2022.

[4] M. Anghel and A. Racautanu, "A note on different types of ransomware attacks," *Cryptology ePrint Archive*, 2019.

[5] A. Alqahtani and F. T. Sheldon, "A survey of crypto ransomware attack detection methodologies: An evolving outlook," *Sensors*, vol. 22, no. 5, p. 1837, 2022.

[6] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput. Secur.*, vol. 111, p. 102490, 2021.

[7] J. A. Herrera-Silva and M. Hernández-Álvarez, "Dynamic feature dataset for ransomware detection using machine learning algorithms," *Sensors*, vol. 23, no. 3, p. 1053, 2023.

[8] N. Singh and S. Tripathy, "It's too late if exfiltrate: Early stage Android ransomware detection," *Computers & Security*, vol. 141, p. 103819, 2024.

[9] A. Alraizza and A. Algarni, "Ransomware detection using machine learning: A survey," *Big Data Cogn. Comput.*, vol. 7, no. 4, p. 143, 2023.

[10] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "A 0-day aware crypto-ransomware early behavioral detection framework," in *Int. Conf. Reliable Inf. Commun. Technol.*, Springer, Cham, 2017, pp. 758–766.

[11] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 136–144, 2019.

[12] Chainalysis, "Crypto Crime: Ransomware Victim Extortion Continues in 2025," [Online]. Available: https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[13] U. Bansal, "A review on ransomware attack," in *Proc. 2nd Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, 2021, pp. 221– 226.

[14] A. Alqahtani and F. T. Sheldon, "A survey of crypto ransomware attack detection methodologies: An evolving outlook," *Sensors*, vol. 22, no. 5, p. 1837, 2022.

[15] J. A. Herrera-Silva and M. Hernández-Álvarez, "Dynamic feature dataset for ransomware detection using machine learning algorithms," *Sensors*, vol. 23, no. 3, p. 1053, 2023.
[16] N. Singh and S. Tripathy, "It's too late if exfiltrate: Early stage Android ransomware detection," *Computers & Security*, vol. 141, p. 103819, 2024.
[17] J. Bellizzi, M. Vella, C. Colombo, and J. Hernandez-Castro, "Responding to targeted stealthy attacks on Android using timely- captured memory dumps," *IEEE Access*, vol. 10, pp. 35172–35218, 2022.
[18] B. Yamany, M. S. Elsayed, A. D. Jurcut, N. Abdelbaki, and M.
A. Azer, "A new scheme for ransomware classification and clustering using static features," *Electronics*, vol. 11, no. 20, p. 3307, 2022.
[19] S. Routray, D. Prusti, and S. K. Rath, "Ransomware attack detection by applying machine learning techniques," in *Machine Intelligence Techniques for Data Analysis and Signal Processing: MISP 2022*, vol. 1, Springer, Singapore, 2023, pp. 765–776.
[20] A. Lakshmanarao, M. R. Babu, and M. B. Krishna, "Malicious URL detection using NLP, machine learning and FLASK," in *Proc. Int. Conf. Innov. Comput. Intell. Commun. Smart Electr. Syst. (ICSES)*, 2021, pp. 1–4.
[21] M. Scalas et al., "On the effectiveness of system API-related information for Android ransomware detection," *Computers & Security*, vol. 86, pp. 168–182, 2019.
[22] A. Ramezani, "Fusion models for cyber threat defense: Integrating clustering with k-means, random forests, and SVM against windows malware," in *Proc. IEEE World AI IoT Congr. (AIIoT)*, 2024, pp. 465–470.
[23] A. El Attaoui, N. El Hami, and Y. Koulou, "Android malware detection using the random forest algorithm," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 36, no. 3, p. 1876, 2024.
[24] A. A. Albin Ahmed et al., "Android ransomware detection using supervised machine learning techniques based on traffic analysis," *Sensors*, vol. 24, no. 1, p. 189, 2023.
[25] M. Scalas et al., "On the effectiveness of system API-related information for Android ransomware detection," *Computers & Security*, vol. 86, pp. 168–182, 2019.
[26] M. Masum et al., "Ransomware classification and detection with machine learning algorithms," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, 2022, pp. 0316–0322.
[27] N. Rani and S. V. Dhavale, "Leveraging machine learning for ransomware detection," *arXiv preprint arXiv:2206.01919*, 2022.
[28] V. Mathane and P. V. Lakshmi, "Predictive analysis of ransomware attacks using context-aware AI in IoT systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 4, 2021.
[29] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.
[30] T. Gera et al., "Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware," *Security and Communication Networks*, vol. 2021, p. 7035233, 2021.
[31] S. Kumi, C. Lim, and S. G. Lee, "Malicious URL detection based on associative classification," *Entropy*, vol. 23, no. 2, p. 182, 2021.
[32] R. Yang et al., "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, vol. 21, no. 24, p. 8281,
2021.
[33] D. Sahoo, C. Liu, and S. C. Hoi, "Malicious URL detection using machine learning: A survey," *arXiv preprint arXiv:1701.07179*, 2017.
[34] A. Shabtai et al., "'Andromaly': A behavioral malware detection framework for android devices," *J. Intell. Inf. Syst.*, vol. 38, no. 1, pp. 161–190, 2012.