RENTAKA: A Novel Machine Learning Framework for Crypto-Ransomware Pre-encryption Detection

Wira Z. A. Zakaria[1], Mohd Faizal Abdollah[2], Othman Mohd[3]
S. M. Warusia Mohamed S. M. M Yassin[4], Aswami Ariffin[5]
MyCERT, Cybersecurity Malaysia, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia[1]
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia[2, 3, 4]
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia[2, 3, 4]
Cyber Security Response Services, Cybersecurity Malaysia, MyCERT, Cybersecurity Malaysia[5]
Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia[5]

***Abstract*—Crypto ransomware is malware that locks its victim's file for ransom using an encryption algorithm. Its popularity has risen at an alarming rate among the cyber community due to several successful worldwide attacks. The encryption employed had caused irreversible damage to the victim's digital files, even when the victim chose to pay the ransom. As a result, cybercriminals have found ransomware a lucrative and profitable cyber-extortion approach. The increasing computing power, memory, cryptography, and digital currency advancement have caused ransomware attacks. It spreads through phishing emails, encrypting sensitive data, and causing harm to the designated client. Most research in ransomware detection focuses on detecting during the encryption and post-attack phase. However, the damage done by crypto-ransomware is almost impossible to reverse, and there is a need for an early detection mechanism. For early detection of crypto-ransomware, behavior-based detection techniques are the most effective. This work describes RENTAKA, a framework based on machine learning for the early detection of crypto-ransomware. The features extracted are based on the phases of the ransomware lifecycle. This experiment included five widely used machine learning classifiers: Naïve Bayes, kNN, Support Vector Machines, Random Forest, and J48. This study proposed a pre-encryption detection framework for crypto-ransomware using a machine learning approach. Based on our experiments, support vector machines (SVM) performed with the best accuracy and TPR, 97.05% and 0.995, respectively.**

***Keywords*—Ransomware; crypto-ransomware; ransomware early detection; pre-encryption; pre-attack; ransomware lifecycle**

I. INTRODUCTION

Ransomware is a relatively new type of malware that targets users in an attempt to extort money. Ransomware is malware that encrypts or locks files on an infected computer and demands payment to unlock and decrypt the files. Ransomware was a relatively new intrusion attack that used encryption to extort money from its victim. The victim must follow the ransom note's instructions to pay the ransom in Bitcoin to decrypt and recover the original files. The attacker frequently uses Bitcoin due to its anonymity, as its identity is difficult to trace. On the other hand, paying the ransom does not guarantee that the victim will receive the decryption key necessary to recover the files [1], [2].

Ransomware employs a variety of attack vectors, including social engineering, spam email, botnets, detection evasion, and self-propagation via vulnerabilities. After successfully infecting the victim's machines, it will lock files and directories and encrypt files with the following extensions: .docx, .xslx, .odt, .zip, .pdf and .jpg. As a result, the victim cannot access their files or computer until the attacker receives the ransom payment within a specified time [3], [4].

Ransomware attacks have grown in sophistication, posing a significant threat to education, health, business, and government organizations. Cybercriminals created hundreds of ransomware variants as a result of lucrative incentives. As a result, ransomware has recently dominated the cyberthreat landscape. Individuals, businesses, government agencies, universities, and hospitals, are targeted by ransomware attacks. For instance, in 2017, the Wannacry ransomware infected over 300,000 victims in 150 countries via the Shadow Brokers APT EternalBlue exploit. Petya ransomware was the first targeted ransomware attack, with most infections occurring in Ukraine. However, Petya has spread to over 60 countries. As a result, ransomware attacks continue to dominate the cyber security world, with an expected dramatic increase in targeted attacks. Due to the exponential growth of ransomware attacks, it is necessary to focus on this type of threat. Exploit kits, cryptocurrency, and ransomware-as-a-service (RaaS) are the primary factors accelerating the global crypto-ransomware outbreak. With RaaS, even inexperienced attackers can launch a crypto-ransomware attack against any organization [4]–[7].

The rest of the paper is organized as follows. Sections II, III and IV discussed this research's motivations, scope, and objectives. Finally, Sections V and VI discussed the research contributions and design. Section VII provided the literature review for this study. Section VIII described the dataset used in this work. Section IX described the framework design and development. Next, Section X described the testing and validation done in this study. Finally, Section I concluded the research and explained the possible future work for this research.

II. MOTIVATION

The crypto-ransomware attack is irreversible, and it is almost impossible to recover the files. Therefore, there is a need to identify it before it attacks the system and files. Crypto-

ransomware poses a significant threat, with new varieties and families being regularly discovered on the internet and the dark web. Furthermore, due to the encryption mechanisms utilized by these outbreaks, recovering from ransomware attacks is challenging [8]–[10]. In addition to the costs of downtime and the money that individuals and businesses may be compelled to pay as ransom, victims may suffer other consequences such as data loss, reputation loss, and even death [8], [11], [12].

III. Research Scope

This research is implemented only for the crypto-ransomware attack. However, this malware category is still persistent and creates massive damage in many crucial sectors [13], [14]. Furthermore, this research focused on crypto-ransomware targeting the Windows operating system since this platform is the most exciting target for the crypto-ransomware operators [15]–[17]. Besides that, most crypto-ransomware targets regular and average computer users, and most of them are running the Windows operating system [18]. The Windows operating system was chosen because it is the most frequently used platform in computer systems and is targeted by most ransomware attacks. The research will focus on crypto-ransomware that uses an encryption algorithm to encrypt its victim's data and files. Crypto-ransomware was chosen because the damage caused by this type of ransomware is often severe and irreversible [19], [20].

IV. Research Objectives

The first objective is to investigate ransomware behavior via Windows API calls. API is the set of instructions that every program uses to communicate with the operating system. Therefore, it is critical to analyze the ransomware's API to understand the ransomware's behavior better. The second goal is to develop an early detection framework for crypto-ransomware attacks. This is to mitigate the ransomware attack's damage. The third objective of this research is to create a dataset to identify crypto-ransomware in its early stages. This dataset contains critical data from the initial stages of a crypto-ransomware attack. The dataset will be used to train and test the machine learning classifier. Furthermore, this dataset can be used for future research in ransomware early detection.

V. Research Contributions

In meeting the above objectives, this research has provided the following contributions. The first contribution is discovering important behaviors of crypto-ransomware attacks with the analysis of API produced. The second contribution is developing the RENTAKA framework to detect crypto-ransomware before triggering the mass unauthorized file encryption. The third contribution is an algorithm for determining the pre-encryption boundary and assists in extracting the required features. The fourth contribution is the crypto-ransomware early-stage behavior dataset that can aid future research using a machine learning approach. This research also filled the gap from previous research in focusing on the pre-encryption stage of the crypto-ransomware attack, which is a critical point; recovery is impossible after encryption happens. In addition, this research also provided a unique solution by combining the signature matching approach and machine learning approach, which provided two levers of detection that can complement each other. Listed below are the contributions of this research:

- Identification of crypto-ransomware behavior during the early stages.
- Proposed a framework for crypto-ransomware early using a machine learning approach.
- Proposed an algorithm for pre-encryption features.
- Crypto-ransomware behavior dataset.

VI. Research Design

The framework within which a researcher chooses the research methods and techniques is the research design. The design enables researchers to focus on appropriate research methods for the subject matter and establish a foundation for success in their studies. Therefore, this study is divided into four phases, as depicted in Fig. 1:

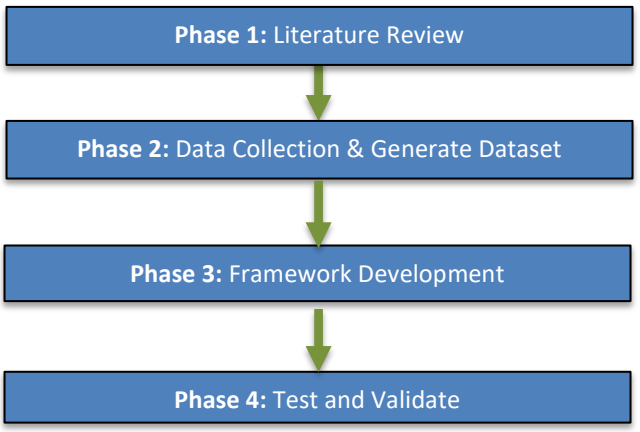

Fig. 1. Research Design.

VII. Phase 1: Literature Review

A. Ransomware

Locker and crypto-ransomware are the two types of ransomware. The Locker ransomware merely affects the user interface, leaving the system and files intact. The Locker ransomware encrypts files and disables operating system features, including desktop apps and input/output utilities. Meanwhile, cryptographic ransomware, often known as crypto-ransomware, tries to extract money from victims by encrypting their files [21].

Crypto-ransomware encrypts user-related files using the cryptography features in the host operating system. The consequences of such ransomware are reversible only through the cryptographic keys possessed by a distant adversary, which sets it apart from other types of malware. Files that have been encrypted are renamed and given new extensions. Some of the most common ransomware encrypted file extensions are ".ccc", ".cerber", ".cerber2", ".cerber3", ".crypt", ".cryptolocker", ".cryptowall", ".ecc", ".ezz", ".locky", ".micro", ".zepto", and ".encrypted". It substitutes a fresh wallpaper with a ransom note for the original desktop background. Cryptolocker,

CryptoDefense, KeRanger, ZCryptor, Crysis, zCrypt, Locky, and WannaCry are just a few examples of crypto-ransomware [5], [8], [22].

The availability of development toolkits and the ease with which ransomware assaults can be traced from victims to attackers are the key factors driving the surge in ransomware attacks today. Before a ransomware attack can occur, it must first get access to the victim's computer [23]–[25].

Ransomware is commonly distributed using spear-phishing and exploit kits. Spear-phishing is a sophisticated email assault designed to deceive people or corporations into accessing a malicious website infected with malware. These emails frequently include attention-getting content from reputable sites to attract recipients to click on the offered link. Furthermore, it is common for an attacker to employ a series of commands or code to exploit the capabilities of a susceptible program. Finally, exploit kits, which can be used manually or automatically, assist hackers in finding flaws in software that would otherwise be impenetrable [26]–[28].

Ransomware has developed throughout time. Its many variations are being produced daily. As a result, there are a lot of ransomware families and their variants. Various obfuscation tactics are used for creating new versions, including garbage code insertion, variable renaming polymorphism, metamorphism, and packing [29].

Crypto-ransomware is malware that encrypts a victim's data and holds it hostage in exchange for money. Cybercriminals collect the ransom in the form of crypto-currency, typically Bitcoins, to hide their identity. There are two types of ransomware: locker and crypto-ransomware. Crypto-ransomware is more common and offers a more significant threat than locker ransomware [30], [31].

WannaCry, Cryptolocker, Cryptowall, and Locky are examples of ransomware that have progressed from low-impact assaults like PC-Cyborg (also known as AIDS) to high-impact attacks like WannaCry, Cryptolocker, Cryptowall, and Locky. In addition, the number of ransomware variations has been rising since 2012. For example, ransomware variations increased from one to 193 between 2012 and 2016. As a result, ransomware became a significant threat to cybersecurity during this period. In addition, ransomware-as-a-Service (RaaS) families like Cryptolocker, CryptoWall, Locky, and TeslaCrypt also appeared in 2017, causing significant financial losses worldwide [32].

Crypto-ransomware assaults have become increasingly prevalent, allowing attackers to make millions of dollars per month. Around 180 million non-technical individuals were victimized by ransomware in 2017. In 2018, there were approximately 850 million ransomware assaults. In 2019 and 2020, ransomware is expected to have caused around $11.5 billion and $20 billion in global damage, respectively.

B. Crypto-ransomware Lifecycle

- Deployment: The crypto-ransomware must be able to install itself on the targeted system successfully. Phishing emails are the most typical way for ransomware to propagate. Cybercriminals use social engineering techniques to persuade people to believe the email message and open the malicious file attached to it. Social engineering approaches include executables with appealing icons, Microsoft Office macros, and phishing files. Furthermore, ransomware spreads using malicious websites or exploit kits like Angler and Magnitude.
- Installation: The infection begins after a malicious payload successfully lands on the victim's platform. The malicious components are built using scripts, procedures, batch files, and other resources. Ransomware will make configuration changes to a Windows-based system, such as establishing unique registry keys in the registry to ensure harmful malware runs every time the computer reboots. Payload persistence, restricted system restoration, stealth mode, environment mapping, and privilege escalation are all features of more complex crypto-ransomware.
- Command and Control: After the ransomware has been installed, it begins interacting with its command and control server. This server provides ransomware with further instructions and a public encryption key. Next, the crypto-ransomware will try to connect to its C&C server, which the ransomware operator controls. Once the link has been established, it will provide information about the victim's computing platform and the encryption key.
- Destruction: The encryption stage begins after establishing effective contact with the targeted computer. The files are encrypted once the ransomware gets the encryption code and the location of the victim files. The encrypted files are renamed with a different extension when the original files are erased. Some ransomware variations add their name to any file as an extension. A list of the files that will be encrypted is included in the ransomware payload. Essential files like "WINDOWS," "Application Data," and "Temp" are excluded to keep the Windows operating system functioning. By erasing the volume shadow copies, ransomware prohibits the user from restoring them. Instead, it uses administrator rights to erase shadow copies of the Windows drive using the cmd.exe command.
- Extortion: The ultimate stage of a crypto-ransomware assault is extortion. Once the data have been fully encrypted, the next step is to inform them and persuade them to pay the suggested ransom. At this point, a windows pop-up or a desktop wallpaper with the ransom note appears on the screen. The directions on proceeding with the ransom payment are included in the ransom note. All ransomware has a different look and various texts in the ransom note. Finally, the crypto-ransomware final stage shows an extortion message demanding a ransom in exchange for the decryption key. Fig. 2 shows the steps in the crypto-ransomware lifecycle.

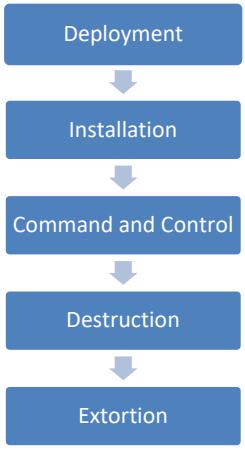

Fig. 2. Crypto-ransomware Lifecycle.

C. Early Detection

Crypto-ransomware is a type of malware that is relatively new. To our knowledge, only a few studies have been conducted on early detection. However, the emerging threat of crypto-ransomware piqued the interest of numerous researchers worldwide, who sought to develop a method for detecting it. Additionally, due to crypto-encryption ransomware's capability, this distinct characteristic can be used as a critical indicator for its early detection during the pre-encryption stage.

Crypto-ransomware pre-encryption detection detects it even before the encryption process begins. Due to the critical nature of detecting crypto-ransomware early in the attack lifecycle, several studies on pre-encryption detection of crypto-ransomware have been proposed.

It is more difficult to detect in the pre-encryption phase due to a lack of evidence that crypto-ransomware is present. Simultaneously, no unauthorised encryption activity occurs. The benefits of successfully detecting a crypto-ransomware infection at this level are that no files are lost and the ransomware is prevented from infecting additional hosts or networks.

In the case of crypto-ransomware, detecting it during the pre-encryption stage is very valuable. Due to the irreversible and irrecoverable nature of a crypto-ransomware attack, it is critical to detect it early, even before it begins encrypting the files. Several studies have proposed methods for detecting crypto-ransomware infections before encryption. Pre-encryption detection occurred before the start of file encryption activity. Detection is critical at this stage to prevent any files from being encrypted. The benefits of detecting crypto-ransomware activity at this level are incredibly beneficial for an organization's file, system, and network security. Apart from preventing any files from being encrypted, detection at this stage may alert system administrators to the infection as soon as possible, allowing security precautions to be taken in time.

Additionally, this proactive measure can help prevent the spread of crypto-ransomware to other endpoints or networks. Finally, detection enables system owners and administrators to respond to an attack as soon as possible before significant damage is caused.

The basic steps in most crypto-ransomware lifecycle, as shown in Fig. 2 are further grouped into three sub-phases of attack: Pre-encryption, encryption, and Post-encryption. These sub-phases are depicted in Fig. 3.

- Pre-encryption – because any crypto-ransomware objective is to encrypt files in bulk, it is frequently designed to avoid detection by making a series of pre-attack API requests. Fig. 4 shows a list of activities during this stage.
- Encryption – at this attack level, unauthorized mass file encryption is taking place.
- Post-encryption – this is where the extortion takes place, by strategically notice the victim of the fate of the encrypted files and luring the system owner to execute the ransom payment.

Crypto-ransomware is a dreaded type of malware that has gained notoriety because of its fatal and irreversible effects on its victims. Due to the irreversible damage caused by ransomware, it is critical to notice these assaults quickly. The following is a list of the reasons why early detection of crypto-ransomware is critical:

- To avoid file loss and the need to pay the ransom (Kok et al., 2019).
- To detect ransomware attacks as early as possible to prevent data loss and stop ransomware self-propagation (Roy & Chen, 2019).
- Early detection can help users protect confidentiality and availability while limiting the probability of an attack and minimizing losses (Moussaileb, 2018).
- The value of detecting cryptographic ransomware is at the pre-encryption stage. It is useless after the encryption activity is completed because data loss has already happened.
- The damage done by crypto-ransomware is irreversible (Al-Rimy & Maarof, 2018).

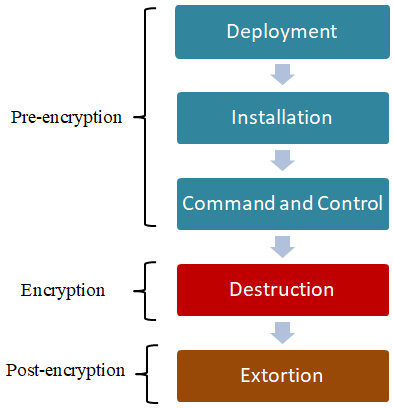

Fig. 3. Pre-encryption, Encryption and Post-encryption Stages.

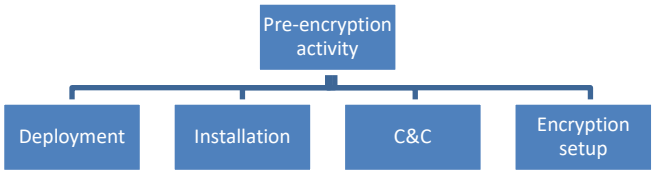

Fig. 4. Activities of a Crypto-ransomware during the Early Stage.

D. Related Work

Early detection and prediction are advantageous for varieties of malware where recovery is difficult and costly. Crypto-ransomware, for example, encrypts user files and withholds the decryption key until the perpetrators are paid a ransom. Unfortunately, as the frequency of crypto-ransomware attacks has grown in recent years, so has the research community's attention to this issue. As a result, few studies examining various threat detection strategies have been conducted. Table I provided a summary of the related works.

EldeRan is a machine learning framework for detecting ransomware early in its lifecycle. As far as this research is concerned, it is the first of its kind in ransomware early detection. The framework looked at dynamic analysis data from ransomware samples. It also keeps track of events throughout the ransomware's installation phase to capture ransomware features. As a result, EldeRan can operate without requiring advanced access to a ransomware family. The first restriction is that it is difficult to analyze and identify crypto-ransomware samples that have been silent for a long time or are waiting for a user-initiated trigger action [33].

As a ransomware early detection framework, the Pre-encryption Detection Algorithm, or PEDA, was proposed [34]. The framework has two phases: PEDA-Phase-I and PEDA-Phase-2. API calls were collected after examining the samples for 30 seconds in the Cuckoo sandbox. PEDA-Phase-I will use the learning algorithm (LA) to collect and analyze the Windows API calls generated by a suspicious sample. The LA can then assess whether the suspicious program was ransomware or not using API pattern recognition. This method ensures the most thorough identification of known and unknown ransomware, but it may lead to many false positives. PEDA implemented a signature database for the samples and placed it in the Phase-II signature repository if the prediction was for ransomware.

Meanwhile, in PEDA-Phase-II, the signature repository uses the signature matching method to detect ransomware at a far earlier level, namely the pre-execution step. Yet this approach only detects known ransomware, though it is proven accurate and quick despite its rigidity. PEDA's two phases resulted in two layers of early ransomware detection, guaranteeing that the victim's data was not lost. This technique, however, was unable to detect ransomware that employed its encryption code and inherited the disadvantages of a signature-based approach [24].

For the early detection of crypto-ransomware, Alqahtani introduced the CRED framework [35]. Their study focuses on the flaws in currently existing ransomware early detection tools. They also presented a model capable of accurately characterizing the attack lifecycle's pre-encryption phase. This strategy is superior because it can overcome data insufficiency gathered during the pre-encryption phase by giving enough time before stopping data collection and using two categories of data: process-centric and data-centric. However, they did not present experimental data to indicate that their approach is superior to others because their study is preliminary.

A group of researchers used file system data to detect ransomware, including whether the contents appear to have been encrypted and the number of modifications made to the file type. As a result, the researchers recognized all 492 ransomware strains tested and prevented, with less than 33% of user data destroyed in each case [36].

TABLE I. DIFFERENCES OF CURRENT PRE-ENCRYPTION DETECTION FRAMEWORK

Framework	Elderan	PEDA	CRED
Pre-encryption boundary identification	Dynamic analysis runtime limited to first 20 seconds.	Identify first occurrence of CryptoAPI.	Using temporally correlated IRP-API based pre-encryption delineation method
Features	30967 features. (API, registry key operations, file operations, dropped files, embedded strings)	232 API calls	API calls and IRP
Dataset	RISS	RISS	Process-centric Data-centric

E. Challenges in Pre-encryption Detection

Crypto-ransomware operations are often disguised as legal user actions, mainly when crypto-ransomware does not require special rights and depends on cryptographic functionality similar to benign applications. Because most crypto-ransomware either implements cryptography or uses existing libraries, this is the case. Apart from that, all they have to do is read and write files.

Detecting ransomware is a race between the bad guys and the creators. New countermeasures push ransomware creators to improve their ransomware, resulting in new countermeasures. For ransomware scenarios, it may, for example, act more like legitimate software or a human user.

There are few strong evidence indicators during the early stages of a crypto-ransomware attack. For example, there is no evidence that many files were encrypted during these early stages. Furthermore, no encryption action is taking place. Strange file extensions, unauthorized changes to the desktop wallpaper, the appearance of a ransom letter, increased CPU utilization, or system slowdown are not visible symptoms of ransomware infection. As a result, the evidence available during the early stages of the investigation is inadequate to evaluate whether the described behaviors are crypto-ransomware-like. It's impossible to tell whether the listed current activity belongs to a benign program or a crypto-ransomware because there was no significant unintended encryption activity during the early phases [20], [34], [37].

There are few significant indicators during the early phases of a crypto-ransomware assault. The fundamental reason is that

there is no indication of illicit file encryption during the early stages [38], [39]. Furthermore, there is no encryption operation in progress. Strange file extensions, unauthorized desktop wallpaper changes, the appearance of a ransom letter, increased CPU use, and system slowdown are not indicative of a ransomware infestation. As a result, the information supplied at the investigation's outset is insufficient to determine whether the described actions are crypto-ransomware-like. Determine whether the related current activity is owned by benign software or crypto-ransomware due to the lack of significant illegal encryption activity in the early stages. The data on the victim's PC is encrypted using a robust encryption method in any crypto-ransomware attack.

VIII. Phase 2: Dataset

The dataset was from the Resilient Information System Security (RISS) research group from Imperial College London in 2016. This dataset was selected because it has API data for ten ransomware families and a good selection of goodware. The dataset was created using a dynamic analysis approach for 582 samples of ransomware and 942 samples of benign program. The data are captured in five main categories with 30,067 features. API calls have 232 features. Two groups of researchers used this dataset for works on crypto-ransomware early detection frameworks [33], [34].

As far as this research is concerned, the dataset on crypto-ransomware behavior is still lacking. However, the RISS dataset is by far the best dataset available for ransomware behavior, and this is shown by the works done by Elderan and PEDA [33], [34]. Tables II and III provided some information about the RISS dataset used in this study.

TABLE II. Ransomware Families in RISS Dataset

No.	Sample name	Count
1	Critroni	50
2	Cryptlocker	107
3	Cryptowall	46
4	Kollah	25
5	Kovter	64
6	Locker	97
7	Matsnu	59
8	Pgpcoder	4
9	Reveton	90
10	Teslacrypt	6
11	Trojan-ransom	34

TABLE III. Categories of Data in RISS Dataset

Category	Count
API	232
Registration key	346
Dropped file	6622
Files and directory operation	7500
Embedded string	16267
Total	**30967**

These researchers successfully used the RISS dataset from different institutions and produced acceptable results. Another dataset is from The Zoo malware repository, which provides ransomware binaries that can be downloaded and analyzed into dynamic analysis sandboxes such as Cuckoo Sandbox.

IX. Phase 3: Framework Development

Given the size and variety of threats we face today, having solutions to detect unknown crypto-ransomware attacks before unauthorized mass file encryption takes place seems necessary. In addition, it is essential to protect user data from any variants of crypto-ransomware attacks with zero data loss.

Monitoring API calls made by crypto-ransomware makes it possible to design an early detection framework to halt crypto-ransomware attacks, including those using sophisticated encryption capabilities.

We proposed a pre-encryption detection framework for crypto-ransomware using a machine learning approach, RENTAKA, to protect user data from being encrypted. The framework is depicted in Fig. 5. Based on detailed investigations of most cases, ransomware-specific events and processes are heavily related to Application Programming Interface (API) calls for the Windows platform. User-level malware like ransomware requires the invocation of system calls to interact with the operating system (OS) to execute its malicious actions. Application Programming Interface (API) calls are the functions that a program utilizes in its execution. In other words, API calls are a set of routines provided by the OS for building applications in which each API call performs a specific task. The API calls is extracted through dynamic analysis after executing the ransomware sample in a sandbox environment. We demonstrate that our proposed solution can detect crypto-ransomware in the pre-attack stage and achieve zero data loss against current ransomware families. Furthermore, as shown in Table IV, we also proposed an algorithm to extract the data related to the pre-encryption stages.

TABLE IV. Pseudocode for Pre-encryption Boundary Algorithm

1. Sample executes in sandbox
2. Run dynamic analysis
3. Extract the behavioral log
4. Locate APIstat cluster
5. Find encryption API
    a. If found encryption API, flag it as "ENC"
    b. Extract all API before the ENC flag
    c. Store in a file
    d. Kill sample execution, repeat with next sample

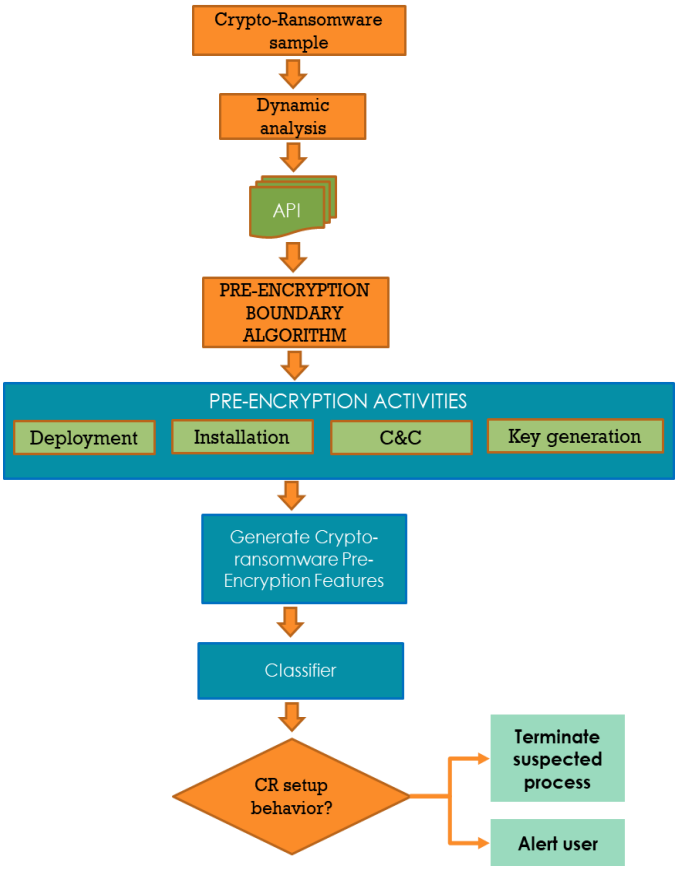

Fig. 5. The Proposed RENTAKA Framework.

X. Phase 4: Test and Validate

The proposed model is tested and validated on a real-world corpus of ransomware samples. The results show that API call features accurately distinguish between ransomware binaries and benign ones. Furthermore, the relevant feature selection process can improve the model building time without compromising the accuracy of the malware detection system.

This study experimented with 80 features using five different classification algorithms: Random Forest, Naïve Bayes, SVM, kNN, and J48. Based on our experiments, support vector machines (SVMs) performed with the best accuracy and TPR, 97.05% and 0.995, respectively. The second-best result is the Random Forest classifier, with 96.39% accuracy. Finally, J48 performs with the lowest accuracy, which is 94.75%. The overall results from our experiments are listed in Table V.

TABLE V. Results from Machine Learning 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

XI. Conclusion and Future Work

This paper discussed the ransomware categories, attack lifecycle, analysis approaches, detection techniques, and related works in its detection. This paper also provided the challenges of crypto-ransomware early detection. We proposed a ransomware detection scheme using a machine learning classifier. Based on our experiments, support vector machine (SVM), one of the supervised machine learning algorithms, performed the best accuracy and TPR. Crypto-ransomware attacks are very dynamic, and it is moving toward becoming a kind of targeted attack. Therefore, early detection systems with machine learning-based classification algorithms are needed to mitigate crypto-ransomware attacks. For future work, we will test with more extensive samples and improve the pre-encryption boundary algorithm. The encryption boundary identification algorithm is a crucial part of this research. It defines the number of features to be used for building the machine learning model.

References

[1] S. Bistarelli, M. Parroccini, and F. Santini, "Visualising bitcoin flows of ransomware: WannaCry one week later," CEUR Workshop Proc., vol. 2058, pp. 1–8, 2018.

[2] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware, Threat and Detection Techniques: A Review," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 2, pp. 136–146, 2019.

[3] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," J. Comput. Virol. Hacking Tech., vol. 15, no. 4, pp. 277–305, 2019, doi: 10.1007/s11416-019-00338-7.

[4] A. Zimba and M. Chishimba, "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems," Eur. J. Secur. Res., vol. 4, no. 1, pp. 3–31, 2019, doi: 10.1007/s41125-019-00039-8.

[5] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," J. Telecommun. Inf. Technol., no. 1, pp. 113–124, 2019, doi: 10.26636/jtit.2019.130218.

[6] J. A. H. Silva, L. Isabel, and B. López, "A Survey on Situational Awareness of Ransomware Attacks — Detection and Prevention Parameters," 2019, doi: 10.3390/rs11101168.

[7] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware," IEEE Access, vol. 7, pp. 47053–47067, 2019, doi: 10.1109/ACCESS.2019.2907485.

[8] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," Comput. Secur., 2018, doi: 10.1016/j.cose.2018.01.001.

[9] A. Alqahtani and F. T. Sheldon, "A Survey of Crypto Ransomware Attack Detection Methodologies : An Evolving Outlook," pp. 1–19, 2022.

[10] M. Rhode, P. Burnap, and K. Jones, "Distillation for run-time malware process detection and automated process killing," pp. 1–12, 2019, [Online]. Available: http://arxiv.org/abs/1902.02598.

[11] M. Wojnowicz, G. Chisholm, B. Wallace, M. Wolff, X. Zhao, and J. Luan, "SUSPEND: Determining software suspiciousness by non-stationary time series modeling of entropy signals," Expert Syst. Appl., vol. 71, no. March 2017, pp. 301–318, 2017, doi: 10.1016/j.eswa.2016.11.027.

[12] Z. A. Genç, G. Lenzini, and P. Y. A. Ryan, "The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware," 2017, [Online]. Available: http://orbilu.uni.lu/bitstream/10993/32574/1/GLR 2017.pdf.

[13] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence," IEEE Trans. Emerg. Top. Comput., vol. 6750, no. c, pp. 1–1, 2017, doi: 10.1109/TETC.2017.2756908.

[14] S. Homayoun et al., "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," Futur. Gener. Comput. Syst., vol. 90, pp. 94–104, 2019, doi: 10.1016/j.future.2018.07.045.

[15] N. Hampton, Z. Baig, and S. Zeadally, "Ransomware behavioural analysis on windows platforms," J. Inf. Secur. Appl., vol. 40, pp. 44–51, 2018, doi: 10.1016/j.jisa.2018.02.008.

[16] A. K. Maurya, N. Kumar, A. Agrawal, and R. A. Khan, "Ransomware : Evolution , Target and Safety Measures," Int. J. Comput. Sci. Eng. Open Access Res. Pap., no. 1, pp. 80–85, 2018, [Online]. Available: http://www.ijcseonline.org/pub_paper/12-IJCSE-02742.pdf.

[17] A. Tandon and A. Nayyar, A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat, vol. 2, no. Proceedings of ICDMAI 2018. Springer Singapore, 2019.

[18] M. A. Salah, M. Fadzli Marhusin, and R. Sulaiman, "Malware Research Directions: A Look into Ransomware," Asian Journal of Information Technology, vol. 16, no. 6. pp. 458–464, 2017.

[19] S. H. Kok, A. Abdullah, and N. Z. Jhanjhi, "Early Detection of Crypto-Ransomware using Pre-Encryption Detection Algorithm," J. King Saud Univ. - Comput. Inf. Sci., no. xxxx, 2020, doi: 10.1016/j.jksuci. 2020.06.012.

[20] B. A. S. Al-rimy and M. A. Maarof, "A 0-Day Aware Crypto-Ransomware Early Behavioral Detection Framework," 2018, doi: 10.1007/978-3-319-59427-9.

[21] K. Savage, P. Coogan, and H. Lau, "The Evolution of Ransomware," Secur. Response, p. 57, 2015, doi: 10.5437/08953608X5403011.

[22] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics," 2015, [Online]. Available: https://arxiv.org/ftp/arxiv/ papers/1611/1611.08294.pdf.

[23] V. C. Craciun, A. Mogage, and E. Simion, "Trends in design of ransomware viruses," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11359 LNCS, pp. 259–272, 2019, doi: 10.1007/978-3-030-12942-2_20.

[24] U. Urooj, M. Aizaini Bin Maarof, and B. Ali Saleh Al-Rimy, "A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model," 2021 3rd Int. Cyber Resil. Conf. CRC 2021, pp. 7–12, 2021, doi: 10.1109/CRC50527.2021.9392548.

[25] D. Y. Kao, S. C. Hsiao, and R. Tso, "Analyzing WannaCry Ransomware Considering the Weapons and Exploits," Int. Conf. Adv. Commun. Technol. ICACT, vol. 2019-Febru, no. 2, pp. 1098–1107, 2019, doi: 10.23919/ICACT.2019.8702049.

[26] J. Kaur, F. Jaafar, and P. Zavarsky, An Empirical Analysis of Crypto-Ransomware Behavior. 2018.

[27] S. Chadha, "Ransomware : Let ' s Fight Back !," pp. 925–930, 2017.

[28] R. Moussaileb, N. Cuppens, J. L. Lanet, and H. Le Bouder, "Ransomware Network Traffic Analysis for Pre-encryption Alert," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12056 LNCS, pp. 20–38, 2020, doi: 10.1007/978-3-030-45371-8_2.

[29] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of wannacry ransomware," Proc. - 16th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2017, vol. 2017-Decem, pp. 454–460, 2017, doi: 10.1109/ICMLA.2017.0-119.

[30] K. Liao, Z. Zhao, A. Doupe, and G. J. Ahn, "Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin," eCrime Res. Summit, eCrime, vol. 2016-June, pp. 1–13, 2016, doi: 10.1109/ECRIME.2016.7487938.

[31] M. S. Rosli et al., "Ransomware Behavior Attack Construction via Graph Theory Approach," vol. 11, no. 2, pp. 487–496, 2020.

[32] B. N. Giri and N. Jyoti, "The Emergence of Ransomware," doi: 10.1177/0306396801432003.

[33] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection," 2016, doi: 10.15199/48.2015.11.48.

[34] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm," Computers, vol. 8, no. 4, p. 79, Nov. 2019, doi: 10.3390/ computers8040079.

[35] A. Alqahtani, M. Gazzan, and F. T. Sheldon, "A proposed Crypto-Ransomware Early Detection(CRED) Model using an Integrated Deep Learning and Vector Space Model Approach," 2020 10th Annu. Comput. Commun. Work. Conf. CCWC 2020, pp. 275–279, 2020, doi: 10.1109/CCWC47524.2020.9031182.

[36] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2016-Augus, pp. 303–312, 2016, doi: 10.1109/ICDCS.2016.46.

[37] M. Rhode, P. Burnap, and K. Jones, "Early Stage Malware Prediction Using Recurrent Neural Networks," 2017, doi: 10.1016/j.cose. 2018.05.010.

[38] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9148, pp. 3–24, 2015, doi: 10.1007/978-3-319-20550-2_1.

[39] M. Patyal, S. Sampalli, Q. Ye, and M. Rahman, "Multi-layered defense architecture against ransomware.," Int. J. Bus. Cyber Secur., vol. 1, no. 2, pp. 52–64, 2017, [Online]. Available: http://ezproxy.umuc. edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=b th&AN=121205538&site=eds-live&scope=site.