A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model

Umara Urooj
School of Computing
Universiti Teknologi Malaysia
Johor Bahru, Malaysia
umaraurooj@gmail.com

Mohd Aizaini Bin Maarof
School of Computing
Universiti Teknologi Malaysia
Johor Bahru, Malaysia
aizaini@utm.my

Bander Ali Saleh Al-rimy
School of Computing
Universiti Teknologi Malaysia
Johor Bahru, Malaysia
bander@utm.my,
bnder321@gmail.com

2021 3rd International Cyber Resilience Conference (CRC) | 978-1-6654-1844-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/CRC50527.2021.9392548

Abstract— **Crypto-ransomware is a malware that uses the system's cryptography functions to encrypt user data. The irreversible effect of crypto-ransomware makes it challenging to survive the attack compared to other malware categories. When a crypto-ransomware attack encrypts user files, it becomes difficult to access these files without having the decryption key. Due to the availability of ransomware development tool kits like Ransomware as a Service (RaaS), many ransomware variants are being developed. This contributes to the rise of ransomware attacks witnessed nowadays. However, the conventional approaches employed by malware detection solutions are not suitable to detect ransomware. This is because ransomware needs to be detected as early as before the encryption takes place. These attacks can effectively be handled only if detected during the pre-encryption phase. Early detection of ransomware attacks is challenging due to the limited amount of data available before encryption. An adaptive pre-encryption model is proposed in this paper which is expected to deal with the population concept drift of crypto-ransomware given the limited amount of data collected during the pre-encryption phase of the attack lifecycle. With such adaptability, the model can maintain up-to-date knowledge about the attack behavior and identify the polymorphic ransomware that continuously changes its behavior.**

Keywords— security, ransomware, crypto-ransomware, pre-encryption, detection

I. Introduction

Cybersecurity is an area aimed at protecting data, devices, and networks from digital attacks. Cyberattacks are launched having an intention to access, alter, or destroy user data or create intrusion in user's business processes. Implementation of cybersecurity becomes crucial and challenging as there are fewer people and more devices. Attackers are usually evil minds interested in accessing, altering, or destroying user data and reputation. Cybersecurity cannot be ensured without paying attention to malware attacks [1]. With the development of anti-viruses and intrusion detection systems adversaries also developed more advanced and powerful malware that can evolve, causing severe infection and can mutate [2]. Malware is a piece of code designed to damage a computer network, server, client, a computer, or any other user's resources. It disables or cause damage to computer resources without user knowledge and violates user rights. Malware has different variants including Rootkit, Viruses, Trojan, Worms, and Ransomware, etc [3].

Ransomware attacks are an evolving area of the current age. It becomes a serious attack due to the severity of the damage it causes [4]. Ransomware is an advanced malware that is executed once and takes privileges on your system resources usually user data by encrypting all files and ask the victim to do what the creator demands, for having the access to computer resources. It exploits user rights. Usually, a ransom is demanded in the form of money [5]. The major risk attached to such attacks is that the attacker does not always keep his promise and after payment does not provide the decryption key. Apart from money loss, the creator can incur other losses such as loss of life or reputation and loss of data. Ransomware attracts evil minds and acts as a motivation for gaining profit. Ransomware can also perform many other activities such as shutting down or kill commands to processes. It can also generate a virtual desktop to stop the user from doing his work [6, 7]. These attacks got risen due to money motivation. Ransomware files that initiate attack are usually spread by Drive-by download, exploiting vulnerabilities in internet-accessible systems, phishing emails, and strategic web compromise [6].

Ransomware evolved with time. Its different variants are being developed day by day. Many ransomware families are developed along with different variants of ransomware. New variants are developed by utilizing various obfuscation strategies such as junk code insertion, variable renaming, polymorphism, metamorphism, and packing. Evolution, Growth rate, and sheer volume highlighted the need for adaptive and pre-encryption crypto-ransomware detection systems [8]. Easy-to-use kits and money are the main driving forces that boost the crypto-ransomware. Even attackers with limited skills can launch a strong crypto-ransomware attack, thanks to Ransomware as a Service (RaaS). Although existing solutions tried to detect ransomware early during the pre-encryption phase, these solutions do not consider the dynamic nature of ransomware attacks. Zero-day attacks evolution makes detection work more challenging [9]. Therefore, an adaptive pre-encryption detection system is required to detect crypto-ransomware attacks immediately before it starts extortion [10]. To this end, this study is devoted to address the lack of adaptive pre-encryption ransomware detection.

The rest of the paper is organized as follows. Section II discusses the motivation of this study. The contribution of the study is introduced in Section III. Related works are detailed in Section IV. In Section V the proposed methodology is described, and the paper is concluded by Section VI.

978-1-6654-1844-7/20/$31.00 ©2021 IEEE

II. THE MOTIVATION

Benign like behaviour of crypto-ransomware attack is challenging to deal with while designing a model for the detection of such attacks [11]. If a model does not make the distinction between a benign program and a crypto-ransomware attack [12, 13], then it will generate a high ratio of false alarms [14].

Crypto-ransomware attacks are irreversible, which makes them significant to study in the field of cybersecurity [15]. Crypto-ransomware has long-lasting effects. User files cannot be dealt with, without the decryption key once attacked by crypto-ransomware [7, 13]. Existing solutions tried to address the detection of ransomware attacks in the early phase before encryption starts. However, these solutions lack to deal with the dynamic nature of ransomware attacks.

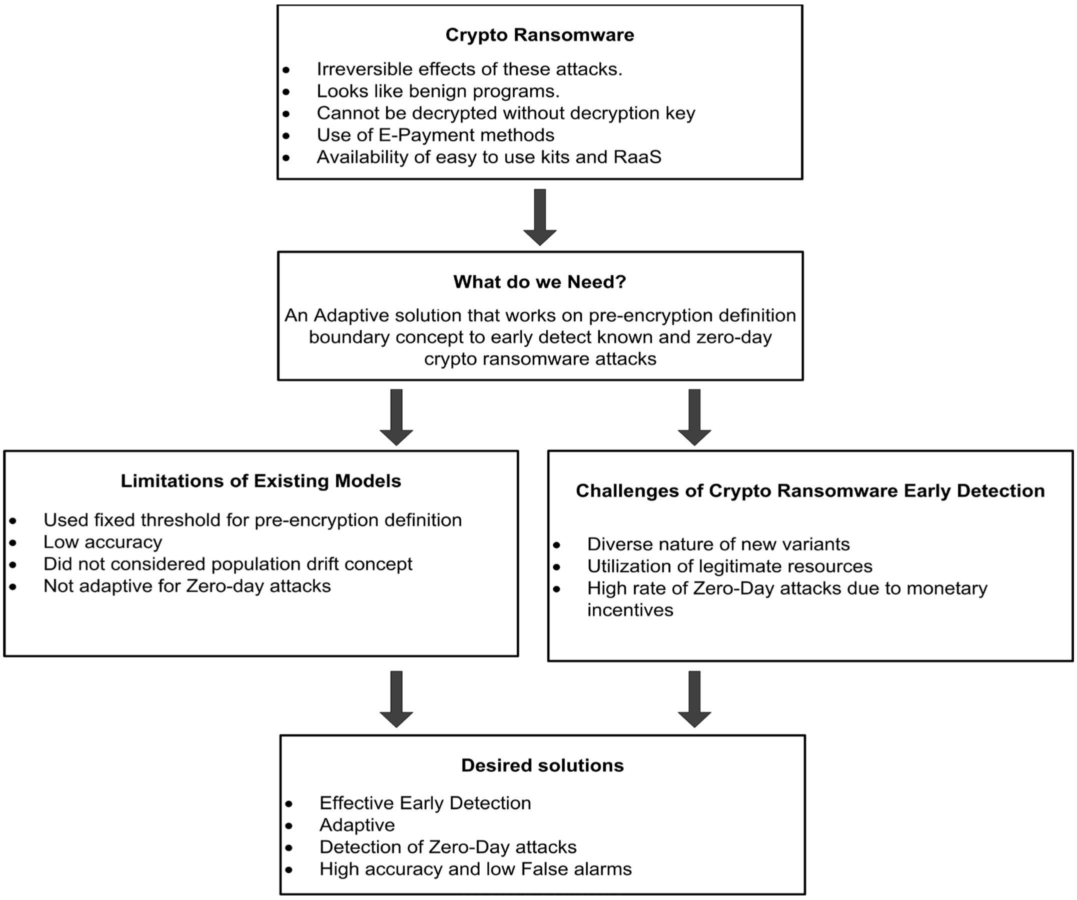
Crypto Ransomware
Irreversible effects of these attacks.
Looks like benign programs.
Cannot be decrypted without decryption key
Use of E-Payment methods
Availability of easy to use kits and RaaS
What do we Need?
An Adaptive solution that works on pre-encryption definition boundary concept to early detect known and zero-day crypto ransomware attacks
Limitations of Existing Models
Used fixed threshold for pre-encryption definition
Low accuracy
Did not considered population drift concept
Not adaptive for Zero-day attacks
Challenges of Crypto Ransomware Early Detection
Diverse nature of new variants
Utilization of legitimate resources
High rate of Zero-Day attacks due to monetary incentives
Desired solutions
Effective Early Detection
Adaptive
Detection of Zero-Day attacks
High accuracy and low False alarms

Fig. 1. Challenges encountered and limitation of existing solutions.

Benign like behaviour and irreversible nature of ransomware attacks made them more challenging for detection [16]. The available detection solutions lack in making the distinction between legitimate processes and malicious code due to developing variants of ransomware [13].

Many studies utilized a fixed threshold for data extraction for crypto-ransomware attacks. These studies built an early detection model using a fixed threshold which was the limitation of these studies. Fixed threshold sometimes precedes encryption [17, 18].

The use of cryptographic relates APIs is also challenging as the APIs are also used by legitimate benign programs which leads to the generation of high false alarms. The utilization of cryptographic APIs made detection more difficult [14].

Low accuracy occurs when the designed system is facing difficulty to classify the encounter process in legitimate benign programs and malicious programs. A model presents low accuracy when it is unable to detect zero-day attacks, unable to deal with the evolved and changing behaviour of crypto-ransomware attacks [15].

The effectiveness of zero-day aware adaptive crypto-ransomware early detection is twofold i.e. generation of an adaptive technique and accurately detecting the crypto-ransomware attacks by using adaptive online classifier [16].

Currently, available solutions do not address the adaptation along with pre-encryption detection. Figure 1 gives a pictorial representation of encounter challenges in crypto-ransomware detection along with the limitation of existing solutions.

Adaptive, zero-day aware pre-encryption early detection is the main distinction of the proposed model with respect to available solutions. To effectively detect the novel and zero-day variants of crypto-ransomware while maintaining the adaptiveness using the limited amount of data is crucial [19]. These attacks are challenging because of the limited amount of data, redundant, diverse nature of features [20, 21], early detection, and adaptation [21, 22]. The available solutions lack in terms of dealing with the limited amount of pre-encryption data [23] and do not provide adaptiveness to the developing variants of crypto-ransomware [24, 25].

We address the problem of ransomware population drift by proposing a novel pre-encryption crypto-ransomware detection framework that will deal with the population drift concept and limitations of existing research work. It will be unique work in terms of its working mechanisms. It is an imperative solution to all the existing detection systems for crypto-ransomware attacks that encrypt user files and making them inaccessible for legitimate users.

III. CONTRIBUTION

Many research work in the field of ransomware detection assuming that these attacks are stationary in nature and not evolved with time, which is the limitation of all the existing research works [26]. Some of the authors dealt with the non-stationary nature of these attacks but still possess limitation in their work that is addressed in the proposed model. The proposed research model deals with the limitation of existing research work by developing an up-to-date and evolutionary model that can work well with developed variants of crypto-ransomware [27].

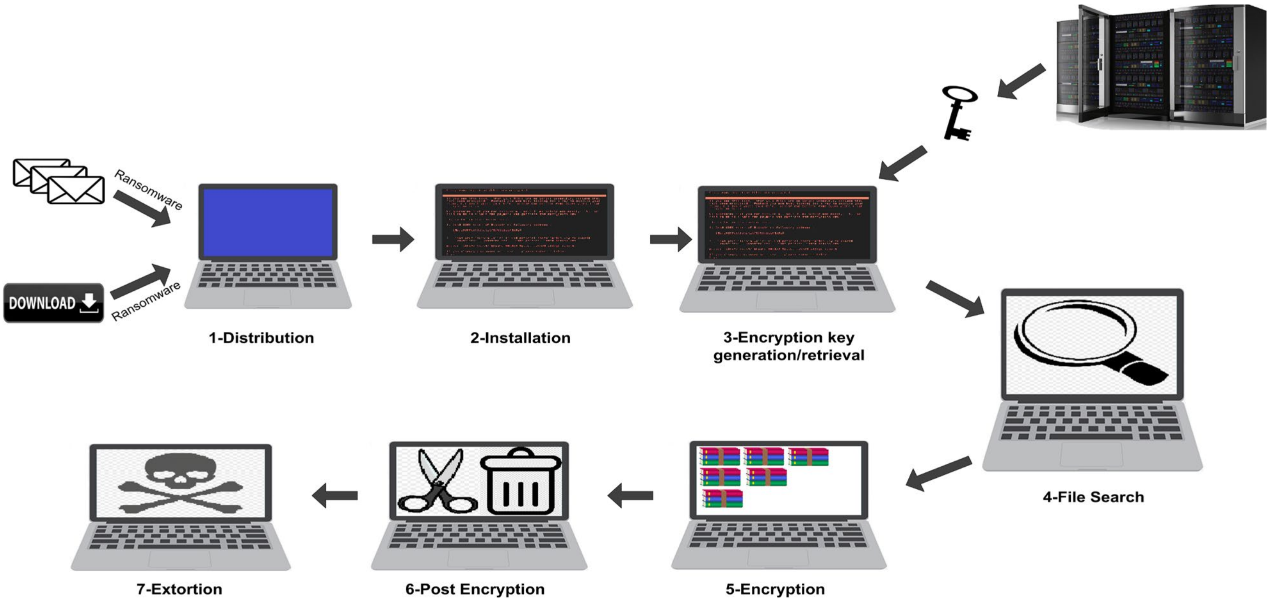

Fig. 2. Ransomware attack launch phases

Accuracy is the main concern in the field of detection. A strong detection system will detect ransomware in less time with high accuracy. We address the problem of ransomware population drift by proposing a novel adaptive pre-encryption crypto-ransomware early detection framework that will deal with the population drift concept and limitations of existing research work. It will be unique work in terms of its working mechanisms. It is an imperative solution to all the existing detection systems for crypto-ransomware attacks that encrypt user files and making them inaccessible for legitimate users. The contribution of the proposed study is described below:

1. An enhanced pre-encryption boundary definition and features extraction scheme to weight the pre-encryption features more accurately.
2. An adaptive pre-encryption crypto-ransomware early detection model by training an online classifier with data and features extracted and selected from pre-encryption boundary definition to increase the detection accuracy of both known and zero-day attacks.

IV. RELATED WORK

Different studies were carried out relating to the pre-encryption and population drift concepts. Some of them are briefly explained below:

A study given by [17] deals with the detection of malware using early data of execution but this study was having low accuracy and a high false alarm rate.

Another approach was followed for ransomware detection by monitoring user files. User files were observed for malicious changes done to these but studies including this approach cannot distinguish between changes done by a benign program and malicious program [25]. So these studies also carried high false alarm generation [14, 16].

In [18] a machine learning-based ransomware classifying approach named EldeRan was proposed. It selects the features which help to find ransomware. This work also discussed the limitations of Dynamic analysis.

An obfuscation detector named ANDRODET for crypto-ransomware was proposed in [28]. The system was developed for the android platform thus working in an incremental and online manner. Identifier renaming, control flow obfuscation, and string encryption obfuscation issues were addressed.

A feature extraction scheme was proposed in [29]. presented scheme DPBD-FE presented the dynamic threshold for defining the boundary definition. The proposed work was able to accurately extract the related APIs for the early detection of crypto-ransomware.

A feature selection approach was discussed in [30] which deals with feature redundancy and overfitting issues. An integration of redundancy gradual up weighting and mutual information was done to get the most relevant feature selection.

In [24] an ensemble learning-based early detection model was proposed. They utilized the ibagging technique for early detection. This work was presented to overcome the shortcoming of limited data before the encryption process. An enhanced selection technique for the selection of most infomative features was also proposed which helps to increase accuracy and low false alarms. These relevant features were used for the training of the detection model.

A context-aware and adaptive malware detection study was presented in [25] for android systems. This study considered the concept of malware population drift. Graph kernel was used to find malicious programs.

In [31] an IRP-API-based pre-encryption method correlation cannot be true all the time. Cryptography related API cannot correlate with the IRP of the interacting process at the same time. If multiple processes are loaded then an API can be from one process while an IRP can be from any other process. Secondly, an API can be generated at time t1 and IRP at time t2 so in that case correlation can be undescribed.

V. THE PROPOSED METHODOLOGY

Given the irreversible effect of CRW attacks, the effectiveness is tackled from two perspectives: an adaptive approach to detect CRW attacks in time, i.e. before the encryption, and the accuracy of these models. Detection accuracy is measured with respect to the detection rate and false alarm rate. The detection rate indicates the model's ability to correctly identify the crypto-ransomware attack, whether known or zero-day. On the other hand, false alarms resulted from feature misrepresentation and the model's rigidness due to the inelasticity to deal with the change of malicious code's behavior with time as well as the emergence of new variants of crypto-ransomware attacks.

Several factors have an impact on CRW Early detection. Unclear definition of pre-encryption phase, inability to distinguish the legitimate from malicious cryptography utilization, inability to detect novel attacks, and outdated models are among these issues that render any detection solution ineffective.

Ransomware attack involves several steps, which can be combined into three phases, pre-encryption, encryption, and post-encryption. From the distribution of the malicious code to demanding the ransom, an attack launch phases through seven different stages. These stages include malicious software distribution, installation, encryption key generation/retrieval, file search, encryption, post-encryption, and extortion. Using different exploitation techniques, a malicious code reaches the victims' machine where it starts self-installation. The encryption key is either generated locally or delivered by the command-and-control server to encrypt the desired data. The targeted data which is being encrypted is either copied to a new place or deleted permanently. The last stage of extortion includes the display of ransom demand messages a pictorial representation of ransomware attack launch and execution is given in figure 2 [22].

The proposed model consists of four important processes that play a vital role in the outcome of this model. These important processes include Pre-Encryption boundary definition, Feature Extraction, Feature Selection, and Online classifier. All these four components work in a cascade manner. The output of one process becomes the input of the succeeding process.

A. Pre-Encryption Boundary Definition

The model starts its working by performing the dynamic analysis on the feed sample. Pre-encryption boundary definition is defined by using the trace files generated after running the dynamic analysis. This pre-encryption boundary definition will help to detect the ransomware in the first place i.e., before the encryption starts. The first cryptography API will trigger the model to start work. This first API will distinguish the pre-encryption phase from the actual encryption process. A pre-encryption boundary definition is a collection of cryptography related APIs. The pre-encryption boundary will be defined by using the pseudo rocchio relevance feedback technique. This technique utilizes the term frequency-inverse document frequency [29].

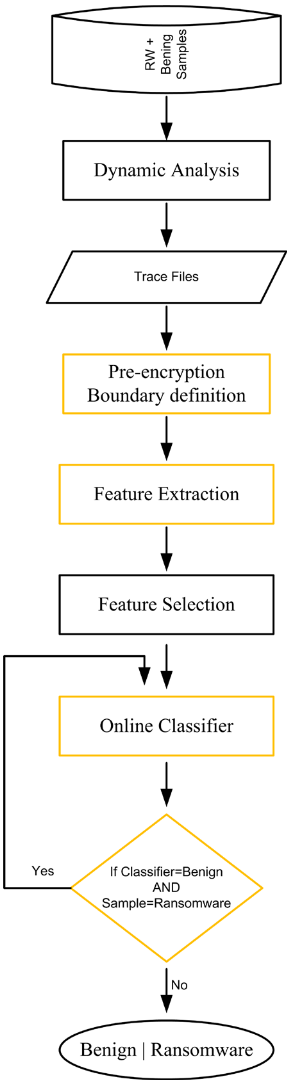

Fig. 3. Design for Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model

B. Pre-Encryption Feature Extraction

After defining the pre-encryption boundaries, the feature extraction process begin. Feature extraction plays vital role in labelling the samples in benign or ransomware. This phase extracts the related features from pre-encryption phase. An annotated term frequency inverse document frequency (aTF-IDF) technique will be utilized for the extraction of relevant features. An aTF-IDF works well for pre-encryption data. Extracted features will be processed to remove the noise and missing entries. This stage is crucial to deal while having an online environment.

C. Pre-Encryption Feature Selection

Feature selection module will select the most relevant features. Extracted features are usually high dimensional so a careful mechanism should be adopted to select the most related features of pre-encryption phase. An enhanced mutual information features selection technique will be utilized to select the relevant features. Features selected at this stage will be used to train the classifier of the self-learning model.

D. Online Classifier

To make the model adaptive to the developing variants of ransomware an online classifier will be built and trained using the features extracted and selected in the previous stages. A stochastic gradient descent which is an online classifier will be trained to provide an up-to-date detection of zero-day attacks. This classifier will keep on updating itself according to the new variants. If a malicious sample is not correctly classified as ransomware it will update itself by adapting the new changes. Adaptation of an online classifier will help to detect new variants of ransomware. Its ability to deal with new variants will maintain accuracy and low false alarms.

A road map to carry out the proposed research work towards the outcomes is given in the figure 3.

VI. DISCUSSION

By applying the adaptive pre-encryption crypto-ransomware detection model, we can solve the problem of lack of adaptivity in the existing ransomware early detection solutions. The existing works overlook the concept drift for early detection of crypto-ransomware attacks while having a small amount of data. This adaptive approach can effectively deal with the issue of polymorphic ransomware. This proposed model will take the population drift concept introduction in the field of ransomware detection. Existing literature highlighted the issues of available solutions which makes the development of the proposed model vital for the current age. The proposed solution will help to stop the ransomware attack early before the encryption takes place.

VII. CONCLUSION

The concept of early detection and ransomware population drift for crypto-ransomware is limited in terms of defining the pre-encryption boundary. This is the first study that deals with the pre-encryption concept along with the population drift concept. This study meets with the demand of current challenges that deal with evolving concepts of the utilization of evading techniques in advanced variants. Existing work either deal with a fixed threshold for pre-encryption boundary definition or used entire data which is not helpful to stop crypto-ransomware attacks. The existing work does not consider the evolution of advanced variants. In this paper, we proposed an adaptive pre-encryption crypto-ransomware early detection model intended to develop and validate. The proposed model will deal with the pre-encryption concept along with the crypto-ransomware population drift concept. This model will overcome the limitation of existing solutions by accurately defining the pre-encryption boundary definition while dealing with adaptiveness. This is a proposed model based on existing literature and intended to be developed. In our future work, the proposed model will be implemented and evaluated with respect to available solutions.

REFERENCES

[1] M. I. Tariq et al., "A Review of Deep Learning Security and Privacy Defensive Techniques," Mobile Information Systems, vol. 2020, 2020.

[2] A. Gazet, "Comparative analysis of various ransomware virii," Journal in computer virology, vol. 6, no. 1, pp. 77-90, 2010.

[3] M. M. Ahmadian and H. R. Shahriari, "2entFOX: A framework for high survivable ransomwares detection," in 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), 2016, pp. 79-84: IEEE.

[4] B. A. S. Al-rimy, M. A. Maarof, Y. A. Prasetyo, S. Z. M. Shaid, and A. F. M. Ariffin, "Zero-day aware decision fusion-based model for crypto-ransomware early detection," International Journal of Integrated Engineering, vol. 10, no. 6, 2018.

[5] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," International Management Review, vol. 13, no. 1, p. 10, 2017.

[6] A. Liska and T. Gallo, Ransomware: Defending against digital extortion. " O'Reilly Media, Inc.", 2016.

[7] 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," Computers & Security, vol. 74, pp. 144-166, 2018.

[8] Y. A. Ahmed, B. Koçer, S. Huda, B. A. Saleh Al-rimy, and M. M. Hassan, "A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection," Journal of Network and Computer Applications, vol. 167, p. 102753, 2020/10/01/ 2020.

[9] M. Alam, S. Sinha, S. Bhattacharya, S. Dutta, D. Mukhopadhyay, and A. Chattopadhyay, "RAPPER: Ransomware prevention via performance counters," arXiv preprint arXiv:2004.01712, 2020.

[10] V. Avdiienko et al., "Mining apps for abnormal usage of sensitive data," in 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, 2015, vol. 1, pp. 426-436: IEEE.

[11] M. Fredrikson, S. Jha, M. Christodorescu, R. Sailer, and X. Yan, "Synthesizing near-optimal malware specifications from suspicious behaviors," in 2010 IEEE Symposium on Security and Privacy, 2010, pp. 45-60: IEEE.

[12] M. Xu et al., "Toward engineering a secure android ecosystem: A survey of existing techniques," ACM Computing Surveys (CSUR), vol. 49, no. 2, pp. 1-47, 2016.

[13] Y. A. Ahmed, B. Koçer, and B. A. S. Al-rimy, "Automated Analysis Approach for the Detection of High Survivable Ransomware," KSII Transactions on Internet and Information Systems (TIIS), vol. 14, no. 5, pp. 2236-2257, 2020.

[14] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, "{UNVEIL}: A large-scale, automated approach to detecting ransomware," in 25th {USENIX} Security Symposium ({USENIX} Security 16), 2016, pp. 757-772.

[15] N. Andronio, S. Zanero, and F. Maggi, "Heldroid: Dissecting and detecting mobile ransomware," in International Symposium on Recent Advances in Intrusion Detection, 2015, pp. 382-404: Springer.

[16] N. Scaife, H. Carter, P. Traynor, and K. R. Butler, "Cryptolock (and drop it): stopping ransomware attacks on user data," in 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 2016, pp. 303-312: IEEE.

[17] S. Das, Y. Liu, W. Zhang, and M. Chandramohan, "Semantics-based online malware detection: Towards efficient real-time protection against malware," IEEE transactions on information forensics and security, vol. 11, no. 2, pp. 289-302, 2015.

[18] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection," arXiv preprint arXiv:1609.03020, 2016.

[19] F. Cuppens, N. Cuppens, J.-L. Lanet, and A. Legay, Risks and Security of Internet and Systems: 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers. Springer, 2017.

[20] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, "Paybreak: Defense against cryptographic ransomware," in Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017, pp. 599-611.

[21] J. K. Lee, S. Y. Moon, and J. H. Park, "CloudRPS: a cloud analysis based enhanced ransomware prevention system," The Journal of Supercomputing, vol. 73, no. 7, pp. 3065-3084, 2017.

[22] B. A. S. Al-rimy et al., "Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection," Future Generation Computer Systems, vol. 115, pp. 641-658, 2021/02/01/ 2021.

[23] F. Mercaldo, V. Nardone, A. Santone, and C. A. Visaggio, "Ransomware steals your phone. formal methods rescue it," in International Conference on Formal Techniques for Distributed Objects, Components, and Systems, 2016, pp. 212-221: Springer.

[24] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection," Future Generation Computer Systems, vol. 101, pp. 476-491, 2019.

[25] A. Narayanan, M. Chandramohan, L. Chen, and Y. Liu, "Context-aware, adaptive, and scalable android malware detection through online learning," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 1, no. 3, pp. 157-175, 2017.

[26] F. Mbol, J.-M. Robert, and A. Sadighian, "An efficient approach to detect torrentlocker ransomware in computer systems," in International Conference on Cryptology and Network Security, 2016, pp. 532-541: Springer.

[27] M. Shukla, S. Mondal, and S. Lodha, "Poster: Locally virtualized environment for mitigating ransomware threat," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1784-1786.

[28] O. Mirzaei, J. M. de Fuentes, J. Tapiador, and L. Gonzalez-Manzano, "AndrODet: An adaptive Android obfuscation detector," Future Generation Computer Systems, vol. 90, pp. 240-261, 2019.

[29] B. A. S. Al-Rimy et al., "A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction," IEEE Access, vol. 8, pp. 140586-140598, 2020.

[30] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection," arXiv preprint arXiv:1807.09574, 2018.

[31] 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," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020, pp. 0275-0279: IEEE.