International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Impacts of Ransomware Attacks on Edge Computing Devices: Challenges and Research Opportunities

Goteng Kuwunidi Job
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

Atiku Baba Shidawa
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

Gital Abdulsalam Yau
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

Adamu Muhammad Tukur
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

Nehemiah Musa
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

Ismail Zahraddeen Yakubu
Department of Computer Science & Engineering
SRM Institute of Science and Technology
Kattankullathur, India

Abstract—Internet of Things (IoT) devices generates a huge volume of data that needs to be processed at real time. Cloud computing paradigm has been a requisite part of this process, consequently, the physical distance between users and cloud increases transmission latency which makes cloud computing not too suitable for real time applications. To address this issue, Edge Computing (EC) which collaborates with the cloud computing allows the processing and storage of applications and data in real time from different geographical locations. As EC is being accepted in the ICT environment, it is also faced with a lot of security issues. In this paper, an investigation on the impacts of ransomware attacks on EC devices is conducted and presents some ransomware families that target edge devices. The study presented some solutions proposed in the literature on securing EC devices against ransomware attacks, however there is a need to provide proactive measures and also apply more robust methods such as, deep learning than the traditional signature based or shallow machine learning approaches which are not recommendable and robust enough in handling complex malwares like ransomware. Thus, the researchers proposed a deep learning framework for the detection of ransomware on EC devices.

Keywords—Edge Computing; Edge Devices; Ransomware; Crypto-Currency; Internet of Things.

I. INTRODUCTION

Information and technologies in recent years have increased exponentially, people now live more convenient and comfortable lives and things are coordinated together and with information, it is expected that even more volume up to 500 Zettabytes will be created in 2019 by people and machines as predicted by Cisco [1]. Internet of Things (IoTs) refers to various devices that are connected to the internet; the data generated by these devices needs to be processed at real time[2]. Cloud computing has been a part of this process but with the huge and large volume of data produced by IoTs devices which increases transmission latency, increasing response time and also stressing the user has made cloud computing inefficient. Edge Computing (EC) paradigm has proven to be a better solution to tackle these problems[3]. EC is positioned between cloud computing andIoTs devices; this allows data and applications to be processed and stored at the edge of the network which reduces the transmission latency [4]. In the year 2016, ransomware continue to spread as found in McAfee Lab report, which entails that edge devices needs a proactive preventive measure against the emerging attack. Ransomware locks or encrypt the victims data or system and limit the victim from accessing it until a ransom is paid, bitcoin account is mostly used for payment.

The subsequent sections of this paper is organized as follows: In Section 2, we gave a general background of the study to include overview of edge computing and ransomware, Section 3 presents related work on the security of edge computing and ransomware in Section 4 we present a framework for the proposed system, in Section 5 we gave a discussion and presented future research direction, and finally in Section 6 the conclusion.

II. GENERAL BACKGROUND

Here we present a general idea of edge computing (edge server, edge network, and edge devices) and also outlined the definition of ransomware, types, how it operates, medium for accepting ransom and also edge devices targeted by ransomware.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

A. About Edge Computing

The traditional cloud computing model is not in conformity with the massive data generated and the continuous demand by real time applications, hence the need to offload the computation, networking and storage near the user. Edge computing is a novel model that allows processing and storing data at the edge of the network, also providing smart services near the source of the data by collaborating with cloud computing. [5]

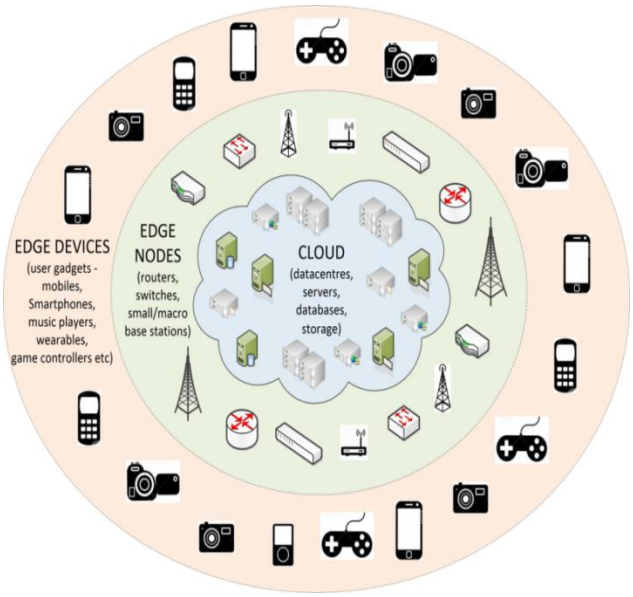

Fig.1. Architecture of Edge computing[6]

EC paradigm is encouraged by its possibility to reduce latency, increase bandwidth and scalability over cloud computing model [7]. Fig. 1 described as edge computing; here the traditional cloud data centers and servers are connected to edge nodes where computations are directed to the edge devices which include routers, switches or base stations, smart phones, wearable, gadgets, and personal computers in different geographical locations are connected very close to the edge nodes for easily computation and storage.

B. Edge Server

An edge server also known as edge data center is referred to a computer that exists at the extreme or " edge" of a network. An edge server serves as a connection point between two different usually private and internet networks; an edge server is an edge device such as routers and routing switches, thus this devices reduce latency and improve page access[5]. Depending on the content, edge server can serve different purposes which include: (i) Security context (ii) Application context (iii) Mail context and (iv) Content distribution context.

C. Edge Network

The heterogeneous nature of edge computing has led to the interconnection of numerous devices including sensors by the incorporation of several communications, such as mobile basic network, wireless network and the internet. The main aim of edge network is to transfer network tasks, contents and resources closer to the end user; here network resources mean caching or storage, computation and communication resources[8]

D. Edge Devices

From Fig 1, end user devices such as smartphones, wearable gadgets, tablets, mobile, personal computer are all considered as edge devices. There is estimated that in the year 2020, about 20 and 50 billion edge " smart" devices will be connected to the internet which include actuators, sensors etc[9].

E. Ransomeware

Ransomware is a malware that take advantage of the vulnerabilities in users system and maliciously hijack the system and encrypt files or any related resources and render them inaccessible, it then shows a warning message to the user demanding a ransom before releasing the hijacked files/resources[10]. Most victims end up paying the ransom because of the fear of losing or exposing valuable files or information. Cases where victims refused to pay, ransomware may increase payment time and also increase the amount of ransom or delete the files from the device [11]. Payment of ransom is based on crypto currency technology (Bitcoin) as transaction in this technology is anonymous, hence the details of the recipient is not available. Ransomware attack started way back 1989 when the author of the AIDS Trojan " Joseph Popp" , spread over 51/4 floppy and replaced the autoexec.bat file. The victims computer when rebooted 90 times the virus will initiate and begin the encryption of files before displaying a message on the desktop, requesting for ransom [12].

In 2016, ransomware destruction has said to have increased exponentially, according to Trend Micro Laboratories, about 247 ransomware families are discovered, which is far more than the 29 families discovered in 2015 while the attackers are rate US$1billion mostly generated from large organizations or enterprises that don't have backups and had to pay the ransom than loose valuable files. Attackers find writing ransomware codes lucrative. With the advancement in technology; such as the emergent of enormous evolution in internet of things devices, connectivity of devices and end users, accessibility of valuable information on social media and the commonness of crypto-currency allows attackers to easily penetrate user's device and collect ransom from device owners[11].

a) Types of Ransomeware

There are two major types of ransomware namely; Locker and crypto ransomware.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

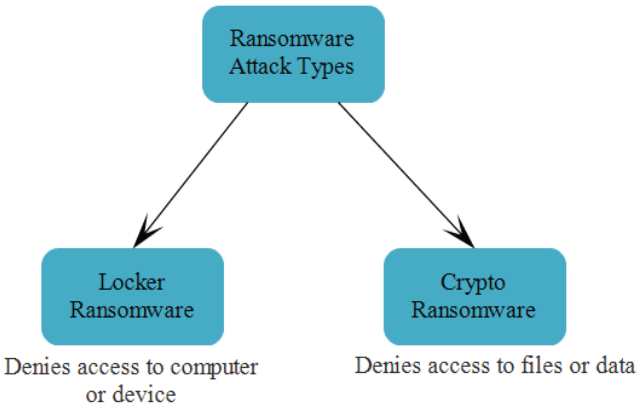

Fig.2. Types of Ransomware[13]

1) Locker Ransomware: This type of ransomware which is also known as computer locker is designed to mainly lock users PC, the attack does not harm the files in the system; after locking the system the attack gives a limited access to the system strictly payment interface, the attacker keeps pressurizing victims to pay ransom with short time notices. This type of attack affects devices with limited or no access of removing them, such devices includes smartphones and emergent Internet of Things devices [13]. Ransomware of this category uses fear technique imposed on victims into paying of ransom, its major tricks to victim is to send copyright infringements or a claim of criminal activities. Fortunately, this type of ransomware can be successfully removed from the victim's device since the attack does not harm the files locked.

2) Crypto-Ransomware: This type of ransomware aims at encrypting the users file with a strong cryptography technique. Immediately after the encryption the victim receives a message that their files are encrypted and the need to pay a ransom, usually crypto-currency (Bitcoin) for decryption and relief of files [12]. Crypto-ransomware is harmful on valuable files, according to a report in [10], crypto-ransomware damages has increased within the January to March of 2016 due to its ability to enforce dangerous harm and its lucrative nature.

III. RANSOMEWARE ATTACKS ON EDGE COMPUTING DEVICES

According to a report by Symantec 2016 disclosed that the targeted systems are not only Personal Computer and mobile devices but also targets edge computing environment. In the same vain McAfee 2016 report made it clear that Linux and MAC operating systems are also vulnerable to ransomware attack. Some vulnerable devices include:

- Personal Computer (PC): Operating systems running on PCs(Windows, Linux, Mac, Android) are also targeted by ransomware. 89% of the market is shared by Microsoft Windows while the rest is shared among Linux, Mac and Android [13]. Ransomware attacks to PC includes: Filecoder, CryptoFortress, and TeslaCrypt[14]. In May 12, 2017 attackers took advantage of the vulnerability of the Windows Operating system and takes access of the system to inject and run a novel modification of ransomware called WannaCry[15]. Personal computers at the edge of the network are faced with these categories of ransomwares and other families of the threat.
- Mobile Devices: With the massive growth and widespread of mobile, smartphones and tablets, they became a big target to ransomware attack. Most mobile ransomware are locker ransomware due to their inability to maneuver capabilities to bypass the attack and reinstate previous state of the system; Ransom.AndroidOS.Small and Trojan-Ransom.AndroidOS.Fusob are some examples of mobile ransomware [10]. Other examples include: Android. Fake Defender,Android.Lockdroid.E, Android.Simplocker[13].
- Server: Servers are responsible for keeping critical and valuable information of any organizations, keeping data in data servers. According to Symantec Lab reports, this type of ransomware secretly and gradually grabs control of the data in the organizations servers and terminals. Example of such ransomware includes PHP.Ransomcrypt.A which secretly and gradually hijacks and locks all online files.
- IoTs Devices: With the increase in IoTs devices and the amount of data they produce and consume the devices includes smart TV, smart cars, smart watches, smart cities which are all targets of ransomware attacks. Example of IoTs based ransomware includes Android.Lockdroid.E[10].
- Wearable Devices: Wearable devices like smart watches which come with internet capabilities are also target of ransomware attack, example of such ransomware is called Ransomware example is Android.SimpleLocker which target smart watches and disconnect the smart watch with other devices[10].

IV. RECENT WORKS ON SECURING EDGE COMPUTING

Touceda et al. [16] proposed an attribute based authentication for permission in to peer-to-peer network; the proposed system is aimed at allocating privileges without third party. In [17] proposed a system that allow mobile device users to move from one geographical location to the other with intractability, authentication is based on handover, clients identity and location are kept with the aid of the elliptic curve algorithm cryptography. In another work conducted by Yang et al. [17]they proposed a cross domain authentication technique that allows different patients to establish sessions securely without interference in e-health social systems. Another handover authentication was proposed for mobile network security by He et al. [18]. A lightweight ciphertext-policy scheme to provide secure data access control in mobile cloud computing was proposed in [19].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

A. Works on Ransomeware Attack

Andronio et al.[20], investigated ransomware on Android devices, they proposed a model known as HellDroid to detect malicious applications, the solution observes the behavioral activities of ransomware at the application layer. In [14] a ransomware recognition approach known as Crypto Drop was proposed, this approach is based on file structure layer to identify a usual ransomware behavior, the model makes use of similarity-preserving hash functions to measure the difference between the encrypted content of every file and the original file. One limitation of the approach is lack to identify cryptographic primitives. Still, [21]proposed ShieldFS, the authors model is actually an add-on driver that guarantees Windows operating system native file system resistant to ransomware attack. ShieldFS observe all low-level file system activities to update a set of adaptive models that profile the file system over time. In [22] they came up with a framework called EldRan using ML algorithms, they used heuristic analysis in sandboxed environment to analyses the dynamic Behaviour of ransomware.

Ransomware solutions are more of the existing solutions of other malwares; these solutions are designed to make use of a black list written based on characteristics (signature). To determine the signature of ransomware, existing solutions make use of trust party which scans ransomware codes on a user device, examples of such solutions are in [21, 23]. Another solution was proposed by Kim et al.[24], the solution is a real time ransomware detection technique without the inclusion of a trust party, the proposed method increase access control policy to the task process of an OS on users device, which will disallowed unauthorized application from initiating or editing in the device, it is white list based, applications are opened or edited if and only if they belong to the white list. Another solution was proposed in[25], the authors used machine learning algorithm for classification of malware, this solution prevent ransomware from penetration at its initial stage using its distribution channels like Exploit kits, the solution scans the heaving patterns like dropped file, listing of file path, ransom note of the victims device. In [26], a Ransom Wall, a layered based defence mechanism for defense against cryptographic ransomware by monitoring a set of features that characterize the behavior of a ransomware was proposed. The layers are: Strong Trap layer takes care of the early detection of ransomware, machine learning ensure a zero-day intrusion, and finally a File Backup layer for maintaining user files, with these layers Ransom Wall attain a detection rate of 98.25% with a near zero false positive using the Gradient Tree Boosting algorithm but the model has not been evaluated on a large scale real setup which is a limitation of the work. A lot of ransomware solutions are designed using machine learning approach, they include [27, 28]. Fig.3 depicts the categories of ransomware solution strategies as discussed in this section. The file based approached takes 43%, the solutions that applied machine learning takes 36% while 21% solution strategies came from deep learning.

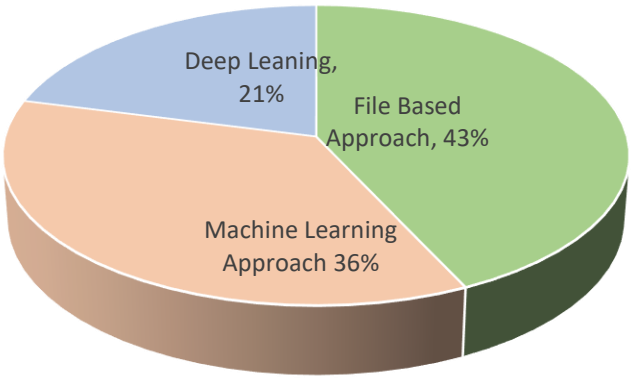

Fig. 3. The percentage of categories of ransomware solution strategies

V. CHALLENGES AND OPPORTUNITIES

Despite the results obtained by the existing methods i.e file based and machine learning approaches, there are several issues that are related to these methods as seen below:

- File Based Approach also known as the antivirus signature based are written for a specific threats or families, traditional file-based detection security is much easier for ransomware authors to penetrate and redistribute hence it can be easily evaded. This makes file-based approach not suitable for the detection of the notorious ransomware.
- Machine learning approach or shallow learning approach, this technique require a training process with a large and representative set of data that have been previously classified by a human expert or through other means, in other words shallow learning approach requires a purview expert (that is, a feature engineer) who can perform the critical task of identifying the relevant data characteristics before executing the shallow learning algorithm. Which involve tedious process and biased feature extraction leading to inefficient classification.

  Our review shows evidence that present machine learning techniques are still affected by several shortcomings that reduce their effectiveness for ransomware detection.

With the challenges befalling the existing methods this creates research opportunities and future research direction for researchers in this domain.

- Deep learning approach, relies on a multi-layered representation of the input data and can perform feature selection autonomously through a process defined representation learning. Deep learning techniques does not require any expert to perform feature

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

engineering of dataset, this method will increase the effectiveness of ransomware detection.

VI. THE PROPOSED FRAMEWORK

In figure 4 below we present architecture of the proposed deep learning method to cumber ransomware attack on edge computing devices.

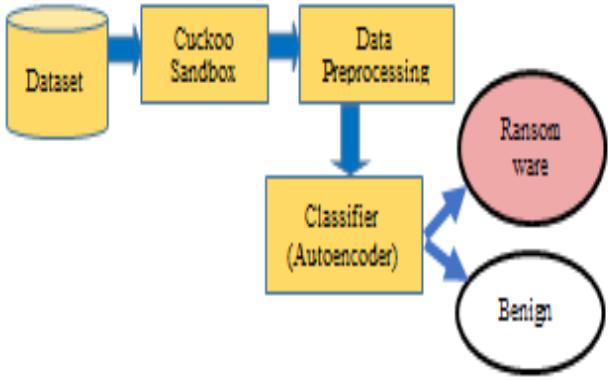

Fig. 4. Architecture of the proposed deep learning technique.

In the proposed architecture, first, the model consist of the dataset; the dataset will include dataset both ransomware and benign to be obtained from any open source dataset repository, to do away with the tedious feature engineering process as it is in shallow machine learning, the dataset will be thrown to automated malware analysis system called cuckoo sandbox which is an open source malware analysis system with this ransomware executable file details will be categorically outlined with their behaviors. For effective classification we will use autoencoder for training of the model, autoencoder is an unsupervised neural network that is used to trained to attempt to copy its input to its output, in other words, the input trained should look more like the output. We are expecting to have an accuracy rate of about 99%. The trained deep learning engine classifies the executables as benign or ransomware.

VII. CONCLUSION AND FUTURE DIRECTION

In this study, we conducted a thorough investigation on the impact of ransomware attacks on edge computing devices and presented some ransomware families that targets edge devices. Edge computing is a promising paradigm in which computation and storage are done at the edge of the network in different geographical location which reduces stress on users waiting for services from the cloud hence the security of edge devices needs to be considered and also be protected. At the course of our study we presented some solutions proposed in the literature, however there is a need to provide a proactive and adaptive measures such as using deep learning than the traditional signature based or shallow learning approaches which are not recommendable in handling complex malwares like ransomware.

In future we will use deep learning technique which is an adaptive and proactive strategy to combat the unrest caused by ransomware attacks. Deep learning models have proved effective in handling more complex problems and detecting intricate hidden activities of ransomware. However, from our review, only few deep learning techniques have been used to tackle ransomware attack, there is need for more exploration to use deep learning models to create stronger, adaptive and secure environment for edge devices.

REFERENCES

[1] Bilal, K., Malik, S.U.R Khan, S.U. and Zowaya, A.Y. *Trends and challenges in cloud datacenters.* IEEE cloud computing, 2014. **1**(1): p. 10-20.

[2] Pan, J. and J. McElhannon, *Future edge cloud and edge computing for internet of things applications.* IEEE Internet of Things Journal, 2017. **5**(1): p. 439-449.

[3] Bilal, K. Khalid, O. Erbad, A. and Khan, S.U.*Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers.* Computer Networks, 2018. **130**: p. 94-120.

[4] Mao, Y., J. Zhang, and K.B. Letaief, *Dynamic computation offloading for mobile-edge computing with energy harvesting devices.* IEEE Journal on Selected Areas in Communications, 2016. **34**(12): p. 3590-3605.

[5] Zhang, J. Chen, B. Zhao, Y. Cheng, X. and Hu, F. *Data security and privacy-preserving in edge computing paradigm: Survey and open issues.* IEEE Access, 2018. **6**: p. 18209-18237.

[6] Varghese, B. Wang, N. Barbhuiya,S. Kilpatrick, P. and Nikolopous, D.S. *Challenges and opportunities in edge computing*. in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*. 2016. IEEE.

[7] Hu, W. Gao, Y. Ha, J. Wang, J. Amos, B. Chen, Z. Pillai, P. and Satyanaranan *Quantifying the impact of edge computing on mobile applications*. in *Proceedings of the 7th ACM SIGOPS Asia-Pacific Workshop on Systems*. 2016.

[8] Wang, S. Zhang, X. Zhang, Y. Wang, L. Yang, J. and Wang, W. *A survey on mobile edge networks: Convergence of computing, caching and communications.* IEEE Access, 2017. **5**: p. 6757-6779.

[9] Liu, Z., K.-K.R. Choo, and J. Grossschadl, *Securing edge devices in the post-quantum internet of things using lattice-based cryptography*. IEEE Communications Magazine, 2018. **56**(2): p. 158-162.

[10] Al-rimy, B.A.S., M.A. Maarof, and S.Z.M. Shaid, *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions.* Computers & Security, 2018. **74**: p. 144-166.

[11] Yaqoob, I. Ahmed, E. Rehmen, R.H. Ahmed, A.I.A. Al-garda, M.A. Imran, M. and Guizani, M. *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks, 2017. **129**: p. 444-458.

[12] Gonzalez, D. and T. Hayajneh. *Detection and prevention of crypto-ransomware*. in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. 2017. IEEE.

[13] Sajjan, R.S. and V.R. Ghorpade. *Ransomware attacks: Radical menace for cloud computing*. in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. 2017. IEEE.

[14] Scaife, N. *Cryptolock (and drop it): stopping ransomware attacks on user data*. in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. 2016. IEEE.

[15] Turaev, H., P. Zavarsky, and B. Swar. *Prevention of Ransomware Execution in Enterprise Environment on Windows OS: Assessment of Application Whitelisting Solutions*. in *2018 1st International Conference on Data Intelligence and Security (ICDIS)*. 2018. IEEE.

[16] Touceda, D.S. Camara, J.M.S. Zeadally, S. and Sodriano, M. *Attribute-based authorization for structured Peer-to-Peer (P2P) networks.* Computer Standards & Interfaces, 2015. **42**: p. 71-83.

[17] Yang, X., X. Huang, and J.K. Liu, *Efficient handover authentication with user anonymity and untraceability for mobile cloud computing.* Future Generation Computer Systems, 2016. **62**: p. 190-195.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

[18] He, D. Zeadally, S. Wu, L. and Wang, H. *Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography*. Computer Networks, 2017. **128**: p. 154-163.

[19] Jin, Y. Tian, C. He, H. and Wang, F. *A secure and lightweight data access control scheme for mobile cloud computing*. in *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*. 2015. IEEE.

[20] Andronio, N., S. Zanero, and F. Maggi. *Heldroid: Dissecting and detecting mobile ransomware*. in *International Symposium on Recent Advances in Intrusion Detection*. 2015. Springer.

[21] Continella, A. Guagnelly, A. Zingaro, G. Pasquale, G. Barenghi, A. Zanero, S. and Maggi, F. *ShieldFS: a self-healing, ransomware-aware filesystem*. in *Proceedings of the 32nd Annual Conference on Computer Security Applications*. 2016.

[22] Sgandurra, D. Gunzalez, M. Mohsen, L. Lupu, L. and E.C. *Automated dynamic analysis of ransomware: Benefits, limitations and use for detection.* arXiv preprint arXiv:1609.03020, 2016.

[23] Kharraz, A. Robertson, W. Balzarotti, D. Bilge, L. and Kirda, e.*Cutting the gordian knot: A look under the hood of ransomware attacks*. in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. 2015. Springer.

[24] Kim, D.-Y., G.-Y. Choi, and J.-H. Lee. *White list-based ransomware real-time detection and prevention for user device protection*. in *2018 IEEE International Conference on Consumer Electronics (ICCE)*. 2018. IEEE.

[25] Gangwar, K., S. Mohanty, and A. Mohapatra. *Analysis and Detection of Ransomware Through Its Delivery Methods*. in *International Conference on Recent Developments in Science, Engineering and Technology*. 2017. Springer.

[26] Shaukat, S.K. and V.J. Ribeiro. *RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning*. in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*. 2018. IEEE.

[27] Nieuwenhuizen, D., *A behavioural-based approach to ransomware detection.* Whitepaper. MWR Labs Whitepaper, 2017.

[28] Chen, Y.-C. Li, Y-J. Tseng, A. and Lin, T. *Deep learning for malicious flow detection*. in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017. IEEE.