Ransomware-based Cyber Attacks: A Comprehensive Survey

Jin Ho Park[1], Sushil Kumar Singh[2], Mikail Mohammed Salim[2], Abir EL Azzaoui[2], Jong Hyuk Park[2*]

[1] Department of Multimedia Engineering, Dongguk University, Korea
[2] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Korea
gomalove@hanmail.net, {sushil.sngh001007, mikail, abir.el, jhpark1}@seoultech.ac.kr

Abstract

Internet of Things (IoT) and sensor devices have been connected due to the development of the IoT and Information Communication Technology (ICT). It offers automatic environments in smart city and IoT scenarios and describes investments in advanced resources in futuristic human lives as sustainable growth of quality-wise life with intelligent infrastructure. Nowadays, IoT devices are continuously increasing and utilized in advanced IoT applications, including Smart Homes, Smart Farming, Smart Enterprises, and others. However, security and privacy are significant challenges with Ransomware-based Cyber-attack detection in IoT due to the lack of security design and heterogeneity of IoT devices. In the last few years, various advanced paradigms and technologies have been utilized to mitigate the security issues with Ransomware attack detection in IoT devices and data. This paper comprehensively surveys Ransomware-based Cyber Attacks and discusses solutions based on advanced technologies such as Artificial Intelligence (AI), Blockchain, and Software Defined Networks (SDN). Then, we design service scenarios for ransomware-based cyber-attack detection. Finally, we summarize the open research challenges and future directions for ransomware in IoT.

Keywords: Ransomware, Cyber attack detection, AI, Blockchain, IoT

1 Introduction

The term “smart city” refers to a system that combines existing infrastructure with modern information and communication technologies to provide a complete set of efficient urban services [1]. The Internet of things (IoT) is the crucial technology for fully scaled smart city realization. IoT integrates networks and human interfaces to develop various smart city applications that store and exchange data in real-time [2-3]. With more IoT and sensor devices, big data is generated according to the smart city’s needs [4]. Automation, communication, and the flow of information in less time and effortlessly are some of the prevalent advantages of IoT. Furthermore, physical devices in IoT infrastructure have the organizing and management capabilities that make their smart devices, and their importance is increasing drastically in all spheres of human existence [5].

Moreover, smart cities have the potential to benefit individuals and communities due to their wide range of applications across health, government, education, and power management. Proper implementation of smart city applications can improve services, lower costs, and provide sustainable solutions. As highlighted earlier, smart cities have a broad spectrum of applications extending to all aspects of consumers’ lives; however, we’ll highlight a few popular ones. Some applications include smart mobility (i.e., smart parking, smart traffic) and smart surveillance [6]. For example, smart parking helps create a real-time map of available parking slots, heavily relying on GPS data. It also enables drivers to see available sports using their gadgets instead of driving around looking for parking spots [7]. Smart traffic help in predicting traffic for safer roads and easier commutes. Moreover, smart streetlights depend on installed sensors to manage streetlight lighting schedules and maintenance for cost-effective cities. These sensors can detect movement and environmental conditions to adjust lights intelligently (i.e., turn off or dim lights) [8].

Nevertheless, ransomware-based cyber-attacks are terrifying IoT application threats [9]. Ransomware is a fusion of the two words “ransom” and “ware,” indicating a type of malware that encrypts important files and then locks down the target machine, rendering it completely unusable in exchange for payment. During a ransomware-based cyber-attack, the attacker encrypts the victim’s data using a robust encryption algorithm and demands a ransom for the decryption key. Therefore, information loss that is either temporary or permanent in some cases, system operations disruption, and money loss are all effects of ransomware-based cyberattacks [10]. The two main categories of ransomware are crypto-ransomware and locker ransomware. To overcome these security risks, several studies have been conducted to solve them. The paper addresses the described problem and contributes in the following manner:

- Discussing a comprehensive survey of Ransomware-based Cyber Attacks in IoT applications.
- A thorough examination of state-of-the-art technology-enabled detection solutions focusing on the methods and strategies in IoT layers.
- We identify AI and Blockchain are the most prominent and promising solutions for ransomware-based cyber-attack detection.
- Design and propose design service scenarios for ransomware-based cyber-attack detection in IoT applications.
- Finally, we identify outstanding issues as potential research directions.

*Corresponding Author: Jong Hyuk Park; E-mail: jhpark1@seoultech.ac.kr

DOI: 10.53106/160792642022122307010

2 Related Work

This section presents the technical aspects and project-based contribution to ransomware-based cyber-attack detection in IoT applications.

2.1 Technical Aspects

Ransomware refers to malicious software that can invade the system and disturb the normal operation of the system. It used various ways and channels, such as network, program vulnerability, and malicious inducement, trying to obtain the computer system's and network's resources and obtain the users' private sensitive information without their permission [11]. They break the systems and demand ransom payments from legitimate owners by destroying important data or Posting users' data on the Internet. However, even if the user pays the ransom, there is no guarantee against the risk, and the malware owner can deny it, demand more money, or destroy the data. Therefore, ransomware is a malicious and illegal profit-making software, and there is no guaranteed mechanism to ensure that users can avoid risks after payment. File encryption ransomware means that users' pictures, videos, documents, applications, and all files, including databases, are encrypted, and the infected files are deleted after encryption. Users caught in the ransomware are presented with a text document containing payment instructions in the corresponding folder. The problem is only discovered when a user tries to open an encrypted file.

The most typical case is WannaCry [12]. This type of ransomware is the most common by far. After infecting a system, it will change the system desktop and display a ransom payment prompt. A typical type of ransomware is WinLocker, which locks a computer's screen and demands payment. It shows a full-screen image and keeps all other Windows open. Fortunately, ransomware does not encrypt users' files, so there is a chance that their data can be recovered [13]. Master Boot Record (MBR) ransomware is a virus that affects the MBR and interrupts normal computer startup as cyber-attacks. The MBR is the part of a computer's hard drive that affects the startup function of the operating system. The MBR ransomware will pay the ransom content on the screen. Petya is one of these viruses. Unlike file ransomware, this type of ransomware may take disk-level encryption technology to overwrite the entire disk after infection, and the data is almost impossible to recover [14]. Web server encryption ransomware is a virus that encrypts files on web servers. It often uses known vulnerabilities in content management systems to release and install ransomware on web services, such as the Master ransomware virus. There is also ransomware on mobile devices [15]. There is far more ransomware on Android than on IOS, and users typically get infected by downloading, browsing untrusted websites, or opening masquerades. Ransomware can be spread in the following ways: Users browse websites with security threats, and the system is infected by a Trojan horse. There are also active infections that spread through emails and other means. As long as users download corresponding attachments, ransomware will be installed silently in the background in an invisible form. The malicious infection attacks users through a network, system, and application vulnerabilities and infects computers in the network. A bundle spread is a bundle infection that is downloaded along with other malware and bundled to infect a user's host. Media infections include removable storage media, local and remote drives, network shared broad-cast, social media transmission, and other media transmission modes. Ransomware types and Comparison with existing research study and development about Ransomware is shown in Table 1.

Table 1. Comparison with existing research study and development

Ransomware name	Year	Ransomware types	Characteristics
Maze [16]	2019	Encryption	Decrypting the ransom depends on how important the infected computer is.
Ryuk [17]	2018	Encryption	Disable the Windows System Restore option on the infected computer.
EKANS [18]	2020	Encryption	Many process applications associated with industrial control operations have stalled.
Ragnar locker [19]	2019	Encryption	The malware is deployed as a virtual machine (VM) to evade traditional defenses.
Bazar loader [20]	2021	Windows	Backdoor Access, when a host is part of an Active Directory (AD) environment.
Lock bit [21]	2022	Malicious software	Highly targeted attacks against enterprises and other organizations.

The Maze ransomware first appeared in May 2019 and claimed that the amount of money paid for decryption depends on infected computers' importance, including office computers and servers, meaning that the cost of decryption will be correspondingly higher for high-value targets. The Ryuk ransomware virus was discovered in August 2018. It mainly targets large enterprises for targeted extortion attacks. One particularly sneaky feature of Ryuk is the ability to disable the Windows Re-store Windows System option on an infected computer, making it harder for victims to recover encrypted data without paying a ransom. EKANS ransomware (also known as Snake), first discovered in January 2020, is a new type of ransomware that specifically targets industrial control systems. EKANS code contains a series of commands and procedures specific to the functions of industrial control systems, which can cause many process applications related to industrial control operations to stall. The EKANS ransomware does not target a specific device or system but rather hopes to take down an entire network. However, it lacks a selfpropagating mechanism, so it must be introduced manually into the ICS environment. Finally, RangerLocker ransomware was discovered in December 2019, and it laments malware as virtual machines (VMS) to evade traditional defenses. The ransomware code is small, just 48KB after removing its custom shell program, and is encoded in a high-level programming language (C/C++). The target is often the company. The malware aims to encrypt any file that can be encrypted and demands a ransom to decrypt it. A new type of artificial ransomware, "PonyFinal," deploys attacks by manually starting payloads. It uses "brute force" against the target company's system administration servers without relying on tricking users into launching payloads via phishing links or emails. Primarily for healthcare facilities in the COVID-19 crisis.

2.2 Project-based Contribution

In this subsection, we discussed project-based contributions to ransomware-based cyber-attacks attack detection and prevention. Various projects are available which are the following:

- *Cynet XDR*: It is a powerful ransomware protection platform that provides extended visibility and protection across endpoints, networks, and users. Cynet can detect ransomware at the beginning of its cycle and respond to it automatically, thus stopping the process before files or drives are encrypted. The platform can also adapt to new ransomware techniques effectively due to its in-depth knowledge-based AI capabilities. Cynet AI can detect suspicious files and classify them based on their nature. It uses several real-time protection mechanisms to detect and prevent ransomware.
- *Enterprise Vulnerability Management Software*: Manager Plus is multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions.
- *CrowdStrike Falcon Ransomware Protection:* An endpoint protection platform that combines defense strategies to prevent infection with ransomware. The platform of Falcon combined the traditional functions of anti-virus software and firewalls to block a wide range of malware, including ransomware.
- Acronis: Acronis' AI-based technology monitors systems in real-time, distinguishing normal activities from threats like unauthorized encryption. Because our technology searches for suspicious behavior instead of malicious code, it can spot ransomware whether or not the strain has been previously seen.

3 Advanced Technology-enabled Solutions for Ransomware

In this section, we discussed advanced technology-based solutions for ransomware-based cyber-attack detection in IoT applications. These advanced technologies are divided into two parts: AI-based and Blockchain-based Solutions for Ransomware Attack Detection in IoT and smart city applications. These advanced technologies are Machine Learning, Deep Learning, Blockchain, and Software-defined networking (SDN).

3.1 AI-based Solutions

Artificial Intelligence is an essential technology for ransomware-based cyber-attack detection for IoT because it offers an automatic environment with various solutions. These solutions depend on Neural Networks, Support Vector Machines (SVM), Decision Trees, Hidden Markov Model (HMM), Hierarchical Clustering, Game Theory (GT), and Natural Language Processing (NLP). Therefore, according to existing research, we categorized AI-based solutions for ransomware attack detection into two parts: Machine Learning-based Solutions and Deep and Federated Learning-based Solutions.

3.1.1 Machine Learning-based Solutions

An evaluation metric for crypto-ransomware detection is proposed by Kok et al. [22] with machine learning technology and a pre-encryption detection algorithm. The signature repository (SR) and learning algorithm mechanism (LAM) is used in above mention algorithm. Any signature matches (SR) identify ransomware and Learning Algorithm (LA) detects known and unknown crypto-ransomware. LA uses a machine learning approach to train the predictive model using data from the application program interface. Scalas et al. [23] proposed API-related information-based effective system for Android Ransomware Detection. It is dependent on learning-based strategies (package, classes, methods) and discriminates the generic malware, ransomware, and actual ware. Finally, an introspection-based approach is proposed by Tang et al. [24] to detect Crypto-Ransomware as RansomSpector. It is based on a virtual machine introspection mechanism and works in the hypervisor layer of the operating system. So, the proposed approach can examine OS-level ransomware. Moreover, it observes both filesystem and network actions for ransomware detection. Berrueta et al. [25] proposed a ransomware detection tool dependent on file-sharing traffic analysis. With the proposed mechanism tool, the research study observes the file-sharing traffic between the client and server. Then, it analyzes the traffic patterns by machine learning technology with ransomware actions while reading and overwriting files. Finally, researchers compared three machine learning models, and proposed tool's validation result is best compared to others.

3.1.2 Deep and Federated Learning-based Solutions

Baek et al. [26] proposed a two-stage hybrid Ransomware detection scheme to protect IoT devices from a Ransomware attack in the Smart City, based on Deep Learning technology. It consists of two stages; the opcode is extracted from learned information via a bidirectional LSTM model in the first stage after static analysis. Then, in the second stage, a dynamic analysis is performed on files categorized as benign in a nested virtual domain. Dynamic Analysis for IoT Malware Detection (DAIMD) scheme is developed by Jeon et al. [27] based on the CNN Model to detect well-known and new malware and decrease the quantity of damaged IoT devices in the networks. The proposed scheme analyzed IoT malware and extracted manners related to memory, network, virtual file system, process, and system call. Rey et al. [28] proposed a Federated Learning-based framework for Malware Detection in IoT Devices. The N-BalIoT dataset modeling network traffic of various IoT devices affected by malware evaluated the proposed framework. The supervised and unsupervised federated model is utilized to detect Ransomware attacks in unseen IoT devices. The main objective of the proposed framework is to offer privacy preservation in the IoT environment and detect Ransomware attacks on the IoT devices of the networks. Pei et al. [29] developed a semi-supervised federated IoT malware detection framework based on knowledge transfer technologies (FedMalDE) for IoT Malware Detection and underlying correlation between labeled and unlabeled records to infer labels towards unlabeled samples by the knowledge transfer mechanism.

3.2 Blockchain-based Solutions

Blockchain and SDN are essential technological networks for ransomware-based cyber-attack detection for IoT applications. Blockchain has many significant features, such as decentralization, integrity, tamper-proof ledger, and peer-to-peer manner, used in the IoT-enabled smart city [30]. Almashadani et al. [31] proposed a crypto-ransomware detection system based on a multi-classifier network. They used a case study of Lock Ransomware, followed by two different levels, including packet-level and flow-level. With the help of TCP, HTTP, DNS, and NBNS traffic, 18 features are extracted with packet and flow levels. Akcora et al. [32] proposed a novel, efficient and secure framework for Bitcoin Blockchain. It automatically predicts new ransomware transactions in the blockchain network based on the no-stored past transactions. The advanced data analytic machinery of Topological Data Analysis is used by the proposed framework that predicts the ransomware payments on Bitcoin in the networks. With the help of Software-Defined Networking, Finally, Faghihi et al. [33] proposed a data-centric detection and prevention method for smartphone crypto-ransomware (RansomCare). It detects smartphone crypto-ransomware in real time by employing dynamic and lightweight static analysis. This solution is capable and provides data privacy when a user's files are lost and offers high accuracy of crypto-ransomware on smartphones.

Existing research addressed security and privacy issues such as Ransomware-based Cyber Attack Detection, but it did not resolve privacy issues entirely. Thus, we survey as a comparison with existing research study and development is shown in Table 2, it consists of six fields, including research work, year, key technology, environment/ application, and approach/ Algorithm/ Methods/ Scheme/ Analysis.

Table 2. Advanced technology-enabled existing solutions

Key technology	Research work	Environment/ Application	Approach/ Algorithm/ Methods/ Scheme/ Analysis
Machine Learning	Kok et al. [22] [2020]	Application Program Interface	Pre-encryption Algorithm with SR and LA.
	Scalas et al. [23] [2019]	System API	Learning-based detection strategies.
	Tang et al. [24] [2021]	VMI, network activities	Introspection-based approach to detect crypto-ransomware.
	Berrueta et al. [25] [2022]	File-sharing network scenarios	File sharing traffic analysis for Ransomware detection.
Deep and Federated Learning, CNNs	Baek et al. [26] [2021]	Smart City	Two-layer-based scheme for the security of IoT devices.
	Jeon et al. [27] [2020]	IoT	DAIMD scheme for IoT Malware detection.
	Rey et al. [28] [2021]	IoT Devices	Federated Learning-based framework for Malware Detection.
	Pei et al. [29] [2022]	IoT Malware Detection	Knowledge Transfer and Federated Learning.
Blockchain and SDN	Almashadani et al. [26] [2019]	Testbed for real and virtual machines	Crypto ransomware network activities based on Locky Ransomware, Domain Generation Algorithm.
	Akcora et al. [27] [2020]	Bitcoin Blockchain	Topological Data Analysis for Ransomware Prediction.
	Faghihi et al. [28] [2021]	Smartphone	Data-centric detection and prevention method for smartphone crypto-ransomware.

4 Ransomware-based Detection Service Scenario and Open Research Challenges

In this section, we discuss service scenarios and open research challenges for ransomware-based cyber-attack detection in IoT with the technical flow of service scenarios.

4.1 Ransomware-based Cyber Attack Detection Service Scenario

A design overview of the Ransomware-based Cyber Attack Detection service scenario for secure communication in smart cities and IoT is shown in Figure 1. It consists of three layers: IoT Device Layer, Ransomware Detection Layer, and Distributed Cloud Layer. Each layer has specific functionality and connects to the other layer. In the bottom layer, we provided IoT Device IDs following the Smart Contract Rules and Regulations. Government Authority offers these rules. A Deep Learning-based Ransomware detection methodology is used in the middle layer of the basic service scenario. After finding actual IoT and smart city applications' data without Ransomware attacks, we transferred to the upper layer, where we utilized Blockchain-enabled Decentralized Cloud Networks. With the help of the decentralized and distributed cloud, we offer security and privacy for IoT data in the IoT Environment. In this service scenario, Blockchain offers decentralized storage at the cloud layer, and deep learning provides ransomware detection networks for actual data communication to the cloud layer.

The technical flow of Ransomware Identification Service-Scenarios for Secure Communication in an IoT Environment is shown in Figure 2. This model consists of three functions: IoT Device Registration ID with Smart Contract, Deep Learning-based Ransomware Detection, and Blockchain-based Decentralized Data Storage. The first function is completed at the first layer. The second function is done at the middle layer, and the last function is completed at the upper layer. Hybrid feature engineering techniques used in Deep Learning-based Ransomware Detection identify the main characteristics of malicious data in the system activities, and Blockchain is used for decentralized storage.

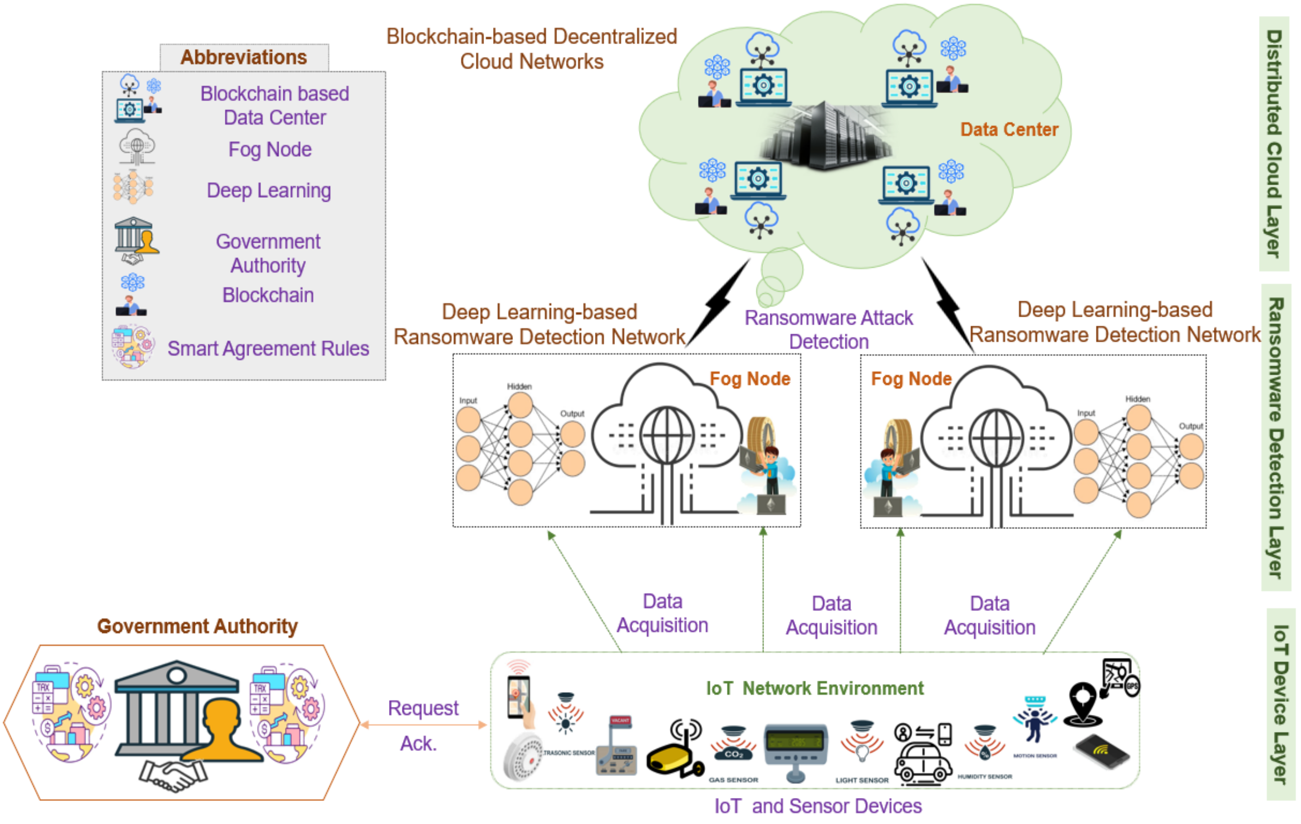


Figure 1. Design overview of ransomware-based cyber attacks identification service- scenarios

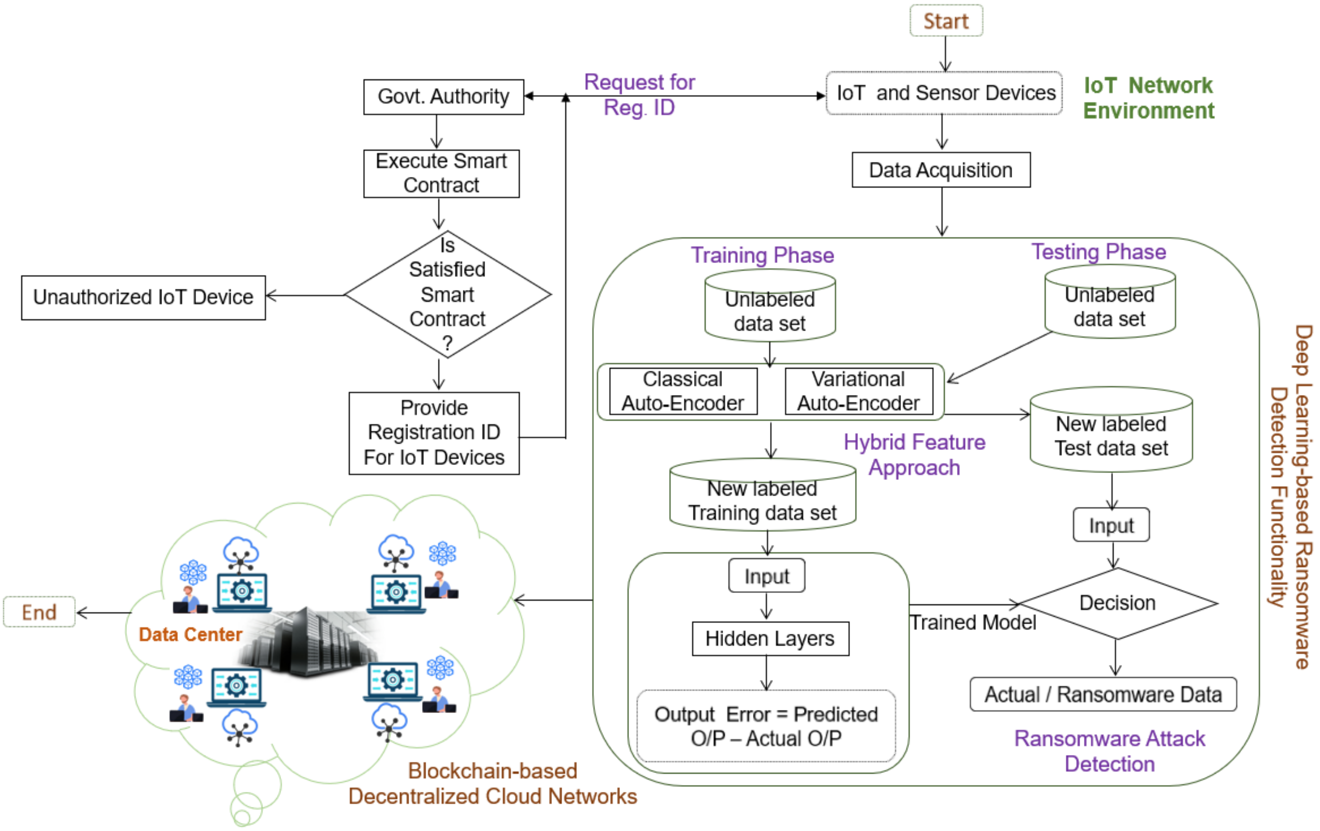


Figure 2. Technical flow of ransomware identification service-scenarios

4.2 Future Directions, Open Challenges for Ransomware Detection

Ransomware attacks continually evolve the security of IoT devices implemented across a smart city, including medical devices, autonomous vehicle sensors, and others. Additionally, challenges in Smart Cities increase due to the low computational power of devices and the lack of uniform security architecture. So, there are some open challenges and future directions of ransomware attacks on IoT.

- *Heterogeneity of IoT devices:* IoT devices installed across the smart city are manufactured with different hardware and software support and capabilities. A lack of interconnectivity between varying device operating systems and constrained hardware systems prevents network security administrators from implementing inbuilt intrusion detection systems and cryptographic encryption schemes [34]. Furthermore, the presence of legacy systems in smart cities disrupts the prevention of the spread of ransomware to other devices due to a lack of firmware support enabling attackers to security protocols due to pre-existing vulnerabilities in the software code. Network security for heterogenous IoT devices should be maintained using Digital Twin on the edge layer for active and real-time anomaly detection of device behavior. Packet inspection between the Digital-Physical twin synchronization can be maintained using the packet inspection methods to detect MITM attacks.
- *Physical security:* Wireless IoT devices transmit data to Edge gateways where the security of device data management and authentication is essential. Physical access to edge devices should be restricted and maintained using multi-factor and biometric ID authentication systems [35]. Attackers near IoT devices attempt to cause physical harm, drain batteries using direct-IoT script injection, and circumvent access control policies for data tampering. Measures such as IoT devices should be monitored using CCTV to prevent attackers from attempting to circumvent device security. Attacks such as Delay attacks and Relay attacks via illegal data collection are expected. Thus, secure routing protocols, data hashing, and encryption-based authentication measures are necessary to safeguard data on the device directly.
- *Energy efficiency:* High energy consumption of Intrusion Detection Systems using Machine Learning and Deep Learning measures prevents their direct application on IoT devices. IoT devices have lower computational power than legacy sensor devices and thus require energy-efficient focused solutions such as lightweight consensus protocols for blockchain-based solutions. Lightweight key distribution methods are essential for transmitting data between Cloud-Edge-IoT nodes without the risk of man-in-the-middle attacks [36-37].

5 Conclusion

With the recent advancement in ransomware detection, we state-of-art surveyed Ransomware-based Cyber Attacks and presented existing solutions based on advanced technologies such as Machine Learning, Deep Learning, Federated Learning, Blockchain, and Software Defined Networks (SDN). Furthermore, we design service scenarios for ransomware-based cyber-attack detection in IoT applications. Finally, we discussed future directions and open challenges for ransomware-based cyber-attack detection IoT environmental applications, including Smart Home, Smart Industry, Smart Manufacturing, Smart Vehicular Networks, and others.

In future work, we will propose a novel architecture or scheme based on the service scenario of Ransomware-based Cyber-attack detection in advanced IoT applications using emerging technologies and cryptographical methods (Gated Recurrent Unit-GRU, Homomorphic Encryption-HE).

Acknowledgments

This research was supported by the Future Challenge Defense Technology Research and Development Project (9129156) hosted by the Agency for Defense Development Institute in 2020.

References

[1] S. K. Singh, C. Lee, J. H. Park, CoVAC: A P2P smart contract-based intelligent smart city architecture for vaccine manufacturing, *Computers & Industrial Engineering*, Vol. 166, Article No. 107967, April, 2022.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, *IEEE Communions Surveys and Tutorials*, Vol. 17, No. 4, pp. 2347-2376, Fourth quarter, 2015.

[3] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. E. Azzaoui, T. W. Kim, Y. Pan, J. H. Park, A comprehensive survey on core technologies and services for 5G security: taxonomies, issues, and solutions, *Human-Centric Computing Information Sciences*, Vol. 11, Article No. 3, January, 2021.

[4] J. Wang, Y. Yang, T. Wang, R. S. Sherratt, J. Zhang, Big Data Service Architecture: A Survey, *Journal of Internet Technology*, Vol. 21, No. 2, pp. 393-405, March, 2020.

[5] A. Zahra, M. A. Shah, IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting, *2017 23rd international conference on automation and computing (icac)*, Huddersfield, UK, 2017, pp. 1-6.

[6] S. K. Singh, Y. Pan, J. H. Park, Blockchain-enabled Secure Framework for Energy-Efficient Smart Parking in Sustainable City Environment, *Sustainable Cities and Society*, Vol. 76, Article No. 103364, January, 2022.

[7] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, P. Siano, Iot-Based Smart Cities: A Survey, *2016 IEEE 16th international conference on environment and electrical engineering (EEEIC)*, Florence, Italy, 2016, pp. 1-6.

[8] ACiiST, *Smart City Applications Needs*, ACiiST, https://www.aciist.com/smart-city-applications-needs/ (Accessed 2022-07-21).

[9] J. C. S. Sicato, S. K. Singh, S. Rathore, J. H. Park, A comprehensive analyses of intrusion detection system for IoT environment, *Journal of Information Processing Systems*, Vol. 16, No. 4, pp. 975-990, August, 2020.

[10] B. Xiong, K. Yang, J. Zhao, K. Li, Robust dynamic network traffic partitioning against malicious attacks, *Journal of Network and Computer Applications*, Vol. 87, pp. 20-31, June, 2017.

[11] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. K. Khan, Ransomware: Recent advances, analysis, challenges and future research directions, *Computers & Security*, Vol. 111, Article No. 102490, December, 2021.

[12] H. Oz, A. Aris, A. Levi, A. S. Uluagac, A survey on ransomware: Evolution, taxonomy, and defense solutions, *ACM Computing Surveys (CSUR)*, Vol. 54, No. 11s, pp. 1-37, January, 2022.

[13] Y. L. Connolly, S. W. David, The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, *Computers & Security*, Vol. 87, Article No. 101568, November, 2019.

[14] S. Kok, A. Abdullah, N. Z. Jhanjhi, M. Supramaniam, Ransomware, threat and detection techniques: A review, *International Journal of Computer Science and Network Security*, Vol. 19, No. 2, pp. 136-146, February, 2019.

[15] I. Almomani, R. Qaddoura, M. Habib, S. Alsoghyer, A. Al Khayer, I. Aljarah, H. Faris, Android ransomware detection based on a hybrid evolutionary approach in the context of highly imbalanced data, *IEEE Access*, Vol. 9, pp. 57674-57691, April, 2021.

[16] Q. Kerns, B. Payne, T. Abegaz, Double-Extortion Ransomware: A Technical Analysis of Maze Ransomware, *Proceedings of the Future Technologies Conference*, Vancouver, Canada, 2021, pp. 82-94.

[17] S. Kuraku, D. Kalla, Emotet Malware—A Banking Credentials Stealer, *IOSR Journal of Computer Engineering*, Vol. 22, No. 4, pp. 31-41, July-August, 2020.

[18] G. V. Santangelo, V. G. Colacino, M. Marchetti, Analysis, prevention and detection of ransomware attacks on Industrial Control Systems, *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, Boston, MA, USA, 2021, pp. 1-5.

[19] J. E. de S. Pimentel, D. A. Cabrera, C. E. Forte, Ransomware: do surgimento aos ataques “as a service”, *FatecSeg-Congresso de Segurança da Informação*, Vol. 1, pp. 1-15, October, 2021.

[20] B. Duncan, *Case Study: BazarLoader to Network Reconnaissance*, Online: October 18, 2021, https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/

[21] Kaspersky, LockBit ransomware — *What You Need to Know*, https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

[22] S. H. Kok, A. Azween, N. Z. Jhanjhi, Evaluation metric for crypto-ransomware detection using machine learning, *Journal of Information Security and Applications*, Vol. 55, Article No. 102646, December, 2020.

[23] M. Scalas, D. Maiorca, F. Mercaldo, C. A. Visaggio, F. Martinelli, G. Giacinto, On the effectiveness of system API-related information for Android ransomware detection, *Computers & Security*, Vol. 86, pp. 168-182, September, 2019.

[24] F. Tang, B. Ma, J. Li, F. Zhang, J. Su, J. Ma, RansomSpector: An introspection-based approach to detect crypto ransomware, *Computers & Security*, Vol. 97, Article No. 101997, October, 2020.

[25] S. I. Bae, G. B. Lee, E. G. Im, Ransomware detection using machine learning algorithms, *Concurrency and Computation: Practice and Experience*, Vol. 32, No. 18, Article No. e5422, September, 2020.

[26] S. Baek, J. Jeon, B. Jeong, Y. S. Jeong, Two-Stage Hybrid Malware Detection Using Deep Learning,

Human-Centric Computing and Information Sciences, Vol. 11, Article No. 27, June, 2021.

[27] J. Jeon, J. H. Park, Y. S. Jeong, Dynamic analysis for IoT malware detection with convolution neural network model. *IEEE Access*, Vol. 8, pp. 96899-96911, May, 2020.

[28] V. Rey, P. M. S. Sánchez, A. H. Celdrán, G. Bovet, M. Jaggi, Federated learning for malware detection in iot devices, November, 2021, *https://arxiv.org/abs/2104.09994*.

[29] X. Pei, X. Deng, S. Tian, L. Zhang, K. Xue, A Knowledge Transfer-based Semi-Supervised Federated Learning for IoT Malware Detection, *IEEE Transactions on Dependable and Secure Computing*, pp. 1-1, May, 2022, DOI: 10.1109/TDSC.2022.3173664.

[30] J. Zhang, S. Zhong, T. Wang, H. C. Chao, J. Wang. Blockchain-Based Systems and Applications: A Survey, *Journal of Internet Technology*, Vol. 21, No. 1, pp. 1-14, January, 2020.

[31] A. O. Almashhadani, M. Kaiiali, S. Sezer, 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, March, 2019.

[32] C. G. Akcora, Y. Li, Y. R. Gel, M. Kantarcioglu, BitcoinHeist: Topological data analysis for ransomware detection on the bitcoin blockchain, June, 2019, https://arxiv.org/abs/1906.07852.

[33] F. Faghihi, M. Zulkernine, RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware, *Computer Networks*, Vol. 191, Article No. 108011, May, 2021.

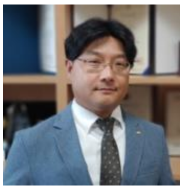
[34] J. Wang, H. Han, H. Li, S. He, P. K. Sharma, L. Chen, Multiple Strategies Differential Privacy on Sparse Tensor Factorization for Network Traffic Analysis in 5G, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 3, pp. 1939-1948, March, 2022.

[35] M. M. Salim, J. Kang, Y. Pan, J. H. Park, A Lightweight authentication scheme for IoT against Rogue Base Station Attacks, *Mathematical Biosciences and Engineering*, Vol. 19, No. 11, pp. 11735-11755, August, 2022.

[36] J. P. Gutierrez, K. Lee, High-Rate Denial-of-Service Attack Detection System for Cloud Environment Using Flume and Spark, *Journal of Information Processing Systems*, Vol. 17, No. 4, pp. 675-689, August, 2021.

[37] S. K. Singh, L. T. Yang, J. H. Park, FusionFedBlock: Fusion of Blockchain and Federated Learning to Preserve Privacy in Industry 5.0, *Information Fusion*, Vol. 90, pp. 233-240, February, 2022.

Biographies



Jin Ho Park is a Professor at the Dongguk University, Seoul, South Korea. Contact him at gomalove@hanmail.net.

Sushil Kumar Singh is a Ph.D. scholar with the Seoul National University of Science and Technology, Seoul, South Korea.

Mikail Mohammed Salim is a Ph.D. scholar with the Seoul National University of Science and Technology, Seoul, South Korea.

Abir EL Azzaoui is a Ph.D. scholar with the Seoul National University of Science and Technology, Seoul, South Korea.

Jong Hyuk Park is a Professor at the Seoul National University of Science and Technology, Seoul, South Korea. Contact him at jhpark1@seoulth.ac.kr.