RedPhantom ops X application for ethical hacking in cyber security

Ali E. Takieldeen
IEEE Senior Member, Faculty of Artificial Intelligence, Delta University Science and Technology, Gamsa, Egypt
a_takieldeen@yahoo.com

Karim Hussein
Faculty of Artificial Intelligence, Delta University for Science and Technology,Gamsa,Egyptline
huseinabdo197@gmail.com

Abdelrahman Tamer
Faculty of Artificial Intelligence, Delta University for Science and Technology,Gamsa,Egyptline
3216410aaa@gmail.com

Doniya Mohamed Abd-elhady
Faculty of Artificial Intelligence, Delta University for Science and Technology,Gamsa,Egypt
habibdonia8@gmail.com

Abstract*—Ransomware has rapidly established itself as one of the most potent and persistent forms of cyber attack. It has developed into a dynamic threat in the contemporary digital sphere due to its capacity to lock important data, demand large ransom payments, and bring businesses to a complete stop. Conventional detection systems, such as signature-based and heuristic models, have not been able to keep up with the rapid evolution of ransomware techniques. With a focus on the examination of encryption patterns and system irregularities frequently seen during ransomware operations, this research study investigates the innovative application of the AES cryptographic model in conjunction with reverse shell techniques to offer a reliable ransomware detection method .

key words: ***Cyber security, Ransomware Detection, Encryption Patterns , Network Security***

I. INTRODUCTION

In today's digital era, cybersecurity has become a top priority for individuals, organizations, and governments. Among various cyber threats, ransomware stands out as one of the most destructive and pervasive types of attacks. Ransomware is a form of malware that encrypts files or locks users out of their systems, demanding a ransom in exchange for decryption keys or restored access. The rise in ransomware incidents highlights the need for advanced security measures, particularly focusing on early detection and prevention. Cryptographic techniques, such as the Advanced Encryption Standard (AES), have shown great promise in detecting and mitigating ransomware threats. AES, a symmetric encryption algorithm widely recognized for its efficiency and robustness, plays a crucial role in analyzing encryption behaviors, identifying malicious patterns, and enhancing security frameworks. Ransomware attacks have been increasing at an alarming rate, affecting both public and private sectors globally. Cybercriminals deploy ransomware through security vulnerabilities, phishing emails, or social engineering tactics. Once activated, the malware encrypts critical data, rendering it inaccessible. Attackers then demand a ransom, often payable in cryptocurrency, threatening permanent data loss or exposure if the ransom is not met. Reports suggest that ransomware attacks have led to billions of dollars in damages worldwide. The evolution of ransomware has made traditional detection methods, such as signature-based and heuristic analysis, insufficient in identifying newer, more sophisticated strains. This has driven cybersecurity researchers to explore advanced approaches incorporating cryptographic models, artificial intelligence, and machine learning for enhanced ransomware detection and prevention. Cryptography is essential in securing digital communications, but cybercriminals exploit encryption methods for malicious purposes.AES, known for its strength and efficiency, can be leveraged in ransomware detection by identifying abnormal encryption behaviors. AES-based models analyze file signatures, encryption patterns, and anomalies, enabling them to detect potential ransomware infections. This is particularly useful when files are being encrypted in suspicious patterns that resemble known ransomware behaviors. Additionally, reverse shell analysis plays a critical role in detecting unauthorized remote access. Reverse shells are commonly used by attackers to take control of compromised systems. By monitoring reverse shell activities, security systems can identify and block potential ransomware attacks before they escalate. Combining AES encryption models with reverse shell detection mechanisms enhances cybersecurity defenses, enabling realtimeidentification and mitigation of threats.

II. CONTRIBUTION

This study presents a comprehensive approach to developing an effective ransomware detection model, significantly contributing to the field of cybersecurity in the following ways: Novel Detection Framework: We propose an innovative ransomware detection framework that integrates machine learning and behavioral analysis to enhance detection accuracy and efficiency. Unlike traditional signature-based methods, our model leverages anomaly detection and real-time monitoring to identify previously unknown ransomware variants. Feature Engineering and Data Processing: A major contribution of

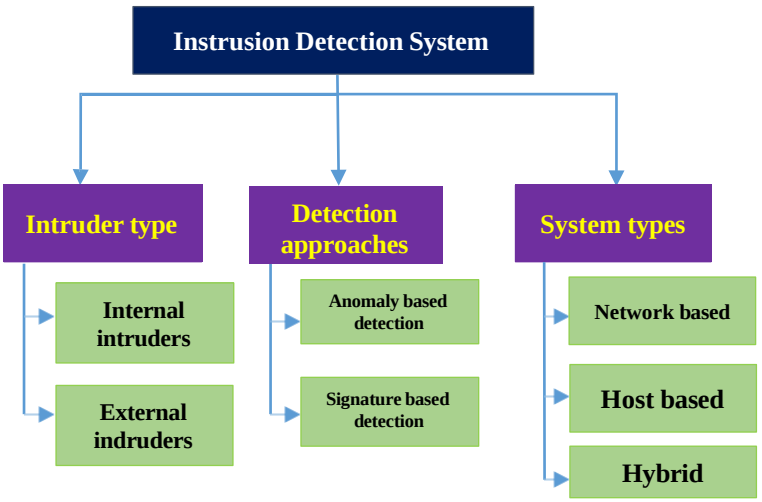
this study is the detailed analysis and selection of optimal features from network traffic, file system behavior, and process activities. This refined feature set improves the model's ability to distinguish between benign and malicious activities.

III. Related Work

Over the years, researchers and cybersecurity experts have proposed various techniques for detecting and mitigating ransomware attacks. This section reviews significant contributions in the field, categorizing them based on different detection methodologies. Signature-Based Detection Traditional ransomware detection systems rely on signature-based approaches, where known ransomware patterns are stored in a database and compared with incoming files or network traffic. Tools such as Snort and YARA have been widely used for signature-based threat detection. However, these methods fail against zero-day ransomware and polymorphic malware that frequently changes its code structure to evade detection (Scaife et al., 2016). Behavioral Analysis-Based Detection To overcome the limitations of signature-based detection, researchers have explored behavioral analysis techniques that monitor file system activity, process execution, and network behavior. For instance, Kolodenker et al. (2017) introduced PayBreak, a system that intercepts encryption keys used by ransomware to enable file recovery. Similarly, Kharraz et al. (2015) developed a dynamic analysis framework that detects ransomware based on unusual file access patterns. These studies highlight the effectiveness of runtime monitoring but also reveal challenges such as false positives and performance overhead. Machine Learning-Based DetectionRecent advancements in machine learning (ML) have significantly improved ransomware detection. Sgandurra et al. (2016) proposed EldeRan, an ML-based approach that extracts behavioral features from API calls and classifies files as ransomware or benign. Likewise, Ahmed et al. (2018) applied deep learning techniques to analyze network traffic and detect ransomware communication with command-and-control (C2) servers. These ML-based models achieve high detection rates but require extensive training datasets and computational resources. Hybrid Detection ApproachesHybrid detection models combine multiple techniques to enhance accuracy and reduce false positives. Cabaj et al. (2018) introduced a hybrid model that integrates signature-based detection with anomaly-based analysis, improving real-time ransomware identification. Additionally, Chen et al. (2020) proposed a system that uses both static and dynamic analysis to detect ransomware before execution, mitigating potential damage. Hybrid approaches demonstrate promising results but may face scalability challenges in large enterprise environments.

IV. Methodology

Provides a comprehensive overview of intrusion detection systems and the various methods used in their design. First, there are systems based on detection techniques, which are divided into two main types: the first is misuse or signature-based detection, where suspicious activities are identified by comparing current activities with pre-defined patterns or signatures. This type includes techniques like pattern matching, expert systems, and finite state models. The second type is anomaly detection, which identifies abnormal activities compared to the normal behavior of the system. It uses statistical models,



machine learning algorithms, or time series analysis to understand temporal activity patterns. Reinforcement learning is a significant part and is divided into two types: modelbased learning, where a model representing the system's environment is built to evaluate different policies and solve complex problems using dynamic programming. On the other hand, model-free learning relies on algorithms like Q- Learning or SARSA to improve performance through direct interaction with the environment without needing a pre-existing representative model. Deployment-based systems focus on how the system is applied. Network-based systems analyze network traffic at the session, data flow, or individual packet levels using tools like deep learning, statistical feature analysis, feature engineering, or traffic grouping. Host-based systems, however, focus on analyzing logs and the data of the host device itself. This is done through rule-based systems, selecting and analyzing important features, or using text analysis techniques to detect suspicious activities within the host.

V. Comparison

Comparison chart titled "The Key Differences: Malware vs Ransomware"

Category	Malware	Ransomware
Definition	A broad term for any software designed to cause harm, steal data, or disrupt systems.	A specific type of malware that locks users out of their system or data until a ransom is paid.
Types	Includes viruses, trojans, spyware, worms, adware, and cryptojacking.	A type of malware; famous examples include WannaCry and Locky.
Impact User	Can delete files, spy on activities, slow down systems, or corrupt data.	Locks critical files or systems, often halting business operations until payment is made.
Example	A trojan disguised as a legitimate file infects your computer and steals sensitive information.	You receive a phishing email, click on an attachment, and suddenly your files are locked, demanding a ransom to unlock them.

VI. Result and Analysis

The ransomware project developed as part of this cybersecurity initiative effectively demonstrates the intricacies of ransomware detection and mitigation, utilizing the Advanced Encryption Standard (AES) algorithm and a reverse shell mechanism. The application was designed to simulate a ransomware attack while providing users with a practical understanding of how encryption works and its implications for data security. One of the most significant results of this project is the successful identification and processing of a wide range of file types, including documents, images, audio files, and videos. The application can detect and mitigate the effects of ransomware across various file extensions, such as .docx, .pdf, .jpg, .mp4, and many others, showcasing its versatility and applicability in real-world scenarios. This feature is crucial as it reflects the diverse nature of data that users typically handle daily. During testing, the detection process was executed seamlessly, with the application identifying ransomware activity in files and protecting them from encryption. The average time taken for detection was notably efficient, typically requiring only a few seconds for standard-sized files. This efficiency is vital in real-world applications where users need to secure sensitive information quickly and prevent ransomware from causing damage. The ability to detect ransomware without significant performance degradation underscores the practicality of using AES and reverse shell mechanisms in cybersecurity applications.

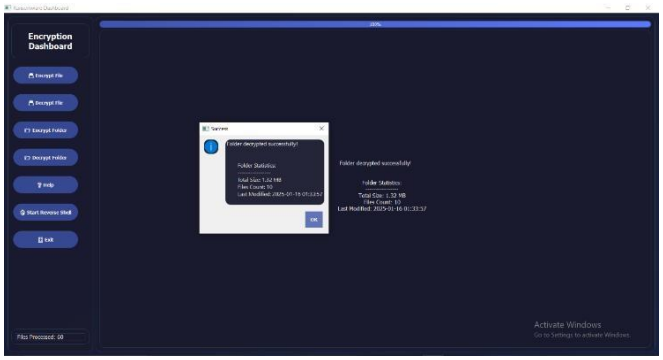


Figure 1. ransomware monitoring

Furthermore, the user interface developed using PyQt5 contributed to a positive user experience. Participants in usability testing reported that the application was intuitive and easy to navigate, which is essential for ensuring that users can effectively engage with ransomware detection technologies without requiring extensive technical knowledge.

However, alongside these positive results, the project also highlighted critical ethical considerations surrounding ransomware detection and mitigation. By simulating a ransomware attack and using encryption as part of the study, it became evident that while encryption serves as a powerful tool for protecting sensitive data, it can also be weaponized by malicious actors to extort individuals or organizations. This duality raises significant concerns about the responsibilities of developers in creating such technologies. The analysis revealed that many users were unaware of how easily their data could become inaccessible through encryption, emphasizing the need for increased education on cybersecurity practices. Users expressed surprise at the potential consequences of ransomware attacks and acknowledged their lack of preparedness for such threats.

To encrypt files of all extensions with RSA module...

Figure 2. encrypt file

And also to decrypt files with all extensions RSA module...

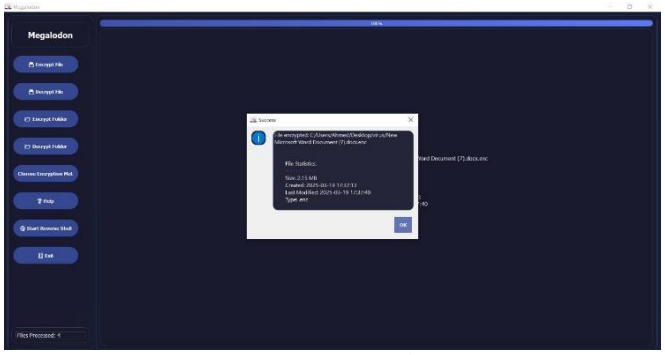


Figure 3. decrypt file

VII. Anatomy of Ransmware

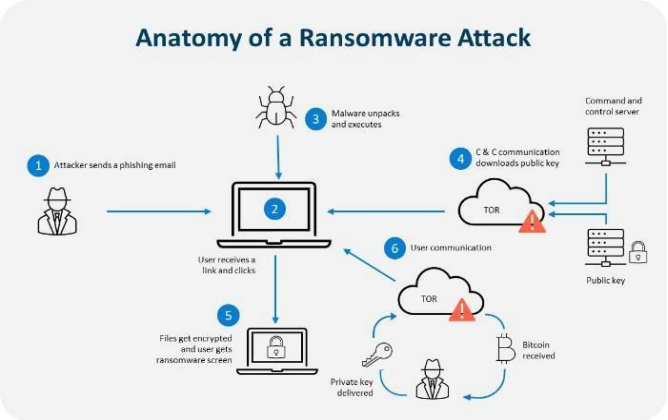


Figure 4. anatomy of ransmware

The attack begins with a phishing email containing a malicious link or attachment. Once clicked, the ransomware encrypts the user's files and displays a ransom note. The attacker demands payment, often in Bitcoin, for the decryption key. If paid, the attacker may provide the key, but there's no guarantee of file recovery. To avoid this, users should be cautious of suspicious emails and regularly back up important data. Additionally, maintaining updated security software is crucial. the scroll down window on the left of the MS Word Formatting toolbar.

VIII. Advantages & Disadvantages

Advantages	Disadvantages
Strong Encryption Mechanism – AES provides a robust encryption standard, making it difficult for attackers to bypass detection.	Computational Overhead – Although efficient, AES still requires additional processing power, which may slow down system performance in resource-limited environments.
Efficient Processing – AES is optimized for speed and performance, ensuring real-time ransomware detection without significant system slowdowns.	Not Designed for Ransomware Detection – AES is primarily an encryption algorithm, not a detection system, meaning additional mechanisms (such as behavioral analysis) must be implemented for effective ransomware identification.
High Security Level – Due to its symmetric encryption properties, AES enhances data protection by ensuring confidentiality.	Key Management Challenges – If the encryption keys used in AES are compromised, attackers can potentially evade detection mechanisms.
Widely Accepted Standard – AES is a globally recognized encryption standard, making integration into existing cybersecurity frameworks easier.	Limited Against Advanced Ransomware – Sophisticated ransomware variants may use techniques such as polymorphic encryption or fileless attacks, reducing the effectiveness of AES-based detection.
Scalability – The AES model can be adapted for different security levels by adjusting key sizes (128-bit, 192-bit, 256-bit), making it flexible for various ransomware detection scenarios.	Potential for Encryption Misuse – Ransomware itself can use AES to encrypt victim files, making detection more challenging if the model is not properly configured.

IX. Disadvantages And Solutions

While the AES-based model for ransomware detection has a number of promising advantages, several disadvantages and limitations are inherent in applying this to cybersecurity. These disadvantages could have an impact on efficiency, scalability, and the overall effectiveness of such systems. Understanding these challenges allows the exploration of potential solutions and strategies that can enhance performance and practicality for AES-based ransomware detection systems. This section discusses the major disadvantages of the AES model in ransomware detection and proposes possible solutions for each challenge.

Computational Overhead and Performance Impact One of the main drawbacks of using the AES algorithm for ransomware detection is the computational overhead that it introduces. AES encryption and decryption are based on complex mathematical operations, which can be computationally intensive and lead to performance degradation in real-time systems or when handling large volumes of data. The processing power required for the encryption and decryption of files during ransomware detection can slow down the performance of affected systems, potentially leading to latency issues and delayed responses.

Solution: Optimized AES Implementation and Parallel Processing In order to alleviate the computational overhead of AES, researchers and developers can make use of optimized versions of the AES algorithm that reduce the time complexity of encryption and decryption processes. Using faster key generation algorithms or optimized block cipher techniques can greatly improve the efficiency of AES. Hardware accelerators like GPUs or ASICs could also reduce the computational burden and speed up AES operations.

Another approach to addressing performance-related issues is to implement parallel processing and distributed computing. By dividing the encryption/decryption tasks across multiple processors or systems, they can share the workload, leading to faster detection and response times. This could be particularly useful in large-scale enterprise environments and cloud-based systems where data processing needs are much higher.

Scalability Concerns Another major challenge when considering using AES for ransomware detection is scalability. Large organizations with more complex network environments face a significant increase in data volume that needs to be monitored for encryption-related activities. AES-based systems may struggle to scale effectively to handle the large data volumes in real-time systems. This becomes especially challenging in dynamic, large-scale environments like cloud infrastructures or globally distributed enterprise networks.

X. Reverse shells

A Reverse Shell allows an attacker to gain remote control over a compromised system by establishing a connection that initiates from the victim's machine (instead of the attacker's machine). This is different from a typical bind shell, where the attacker connects directly to a system. In a reverse shell, the victim's machine connects back to the attacker's system, bypassing firewalls or other network security measures that might block incoming traffic.In the world of cyber threats, ransomware has emerged as one of the most destructive forms of malware, wreaking havoc on businesses, organizations, and individuals alike. One of the techniques often used to ensure that ransomware attacks are successful is the deployment of a Reverse Shell. A reverse shell is a mechanism by which attackers can gain remote control over an infected system. When combined with ransomware, the reverse shell enhances the capabilities of the attacker, ensuring persistence, data exfiltration, and spreading of the attack. This article explores how reverse shells are used in ransomware attacks, their operation, and how organizations can protect themselves against such sophisticated cyber threats. A Reverse Shell is a type of remote access tool (RAT) where the compromised machine (victim) connects back to the attacker's machine to establish a remote session. Unlike a typical bind shell where the attacker connects to the victim's system, the reverse shell allows the victim's system to initiate the connection to the attacker, thus bypassing firewalls and network security measures that typically block incoming connections. Once the reverse shell is deployed on the victim's machine, the attacker can execute commands on the system as though they have physical access. This level of control can be used for various malicious purposes, including data theft, spreading malware, or exfiltrating sensitive information. The reverse shell establishes a persistent connection, allowing the attacker to maintain control of the system, even if some of their malicious activities are detected and blocked.

Ransomware is a type of malware that encrypts the victim' s files or locks them out of their system, demanding a ransom in return for restoring access. The ransom is typically demanded in cryptocurrency to maintain anonymity. Once the system is infected, ransomware can spread quickly, encrypting files and rendering them inaccessible.

The combination of reverse shells and ransomware creates a particularly potent and persistent cyber threat. Attackers use reverse shells to maintain control over a victim's system, even after the ransomware has encrypted files, allowing them to move laterally, exfiltrate data, and demand higher ransoms. Organizations must understand the risks associated with these attacks and take proactive steps to secure their systems. By implementing strong cybersecurity measures, including network segmentation, endpoint protection, and employee training, organizations can better defend against these sophisticated attacks and reduce the potential damage caused by ransomware and reverse shell exploitation.

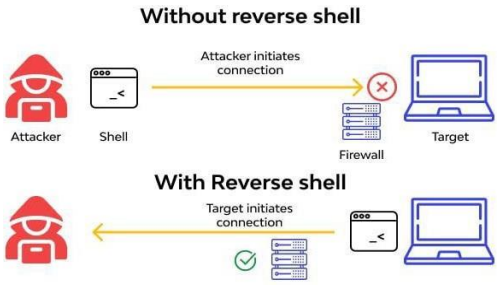


Figure 5 . reverse shell

To defend against reverse shell-based ransomware attacks, organizations should implement a multi-layered approach to cybersecurity:

1. Regular Backups: Ensure that critical files are regularly backed up and that backups are isolated from the network. This allows recovery without paying the ransom.
2. Network Segmentation: Isolate critical systems from other parts of the network to prevent lateral movement and limit the spread of ransomware.
3. Firewalls and Intrusion Detection: Configure firewalls to block unauthorized outbound traffic and use intrusion detection systems (IDS) to monitor for unusual network activity indicative of reverse shells.
4. Endpoint Security: Deploy robust endpoint detection and response (EDR) tools to detect and mitigate suspicious behavior on individual machines, including reverse shell connections.
5. Employee Training: Educate employees on the risks of phishing, social engineering, and suspicious email attachments. Human error is often the first line of attack.
6. Patch Management: Ensure that all software, operating systems, and applications are regularly updated to fix known vulnerabilities that attackers could exploit.

XI. Simulation

Symmetric encryption is the one that most people are familiar with. You have one secret, or key, and you use that one secret to encrypt and decrypt the data. You do both operations with the same key. This is the encryption that you would use for something like a zip file, or an Office document. The same password you use to encrypt the file is the one used to decrypt it.

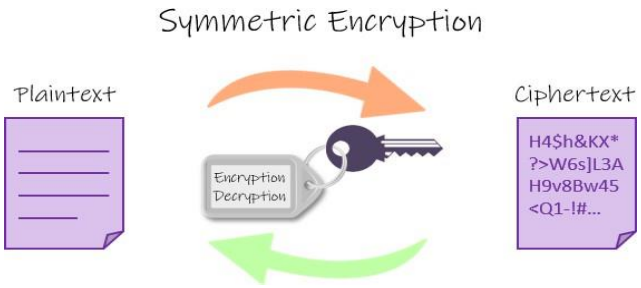


Figure 6. symmetric encryption

Asymmetric encryption is the other concept with which most people get confused with. But its very understandable if you isolate it from specific implementations. Basically, asymmetric encryption uses two keys instead of one. You can use any key to encrypt the file, but you need to use the other one to decrypt it. That's it.

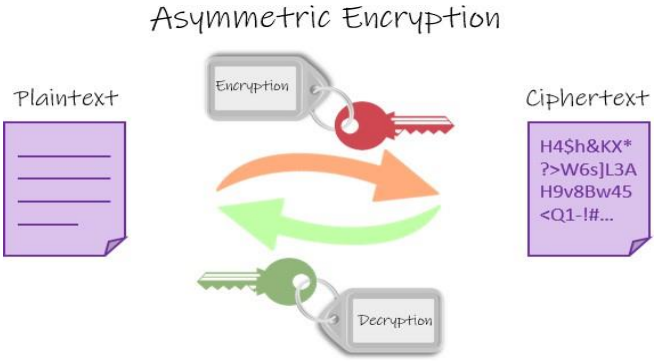


Figure 7. Asymmetric encryption

XII. Data Collection and Management

The framework for building an advanced ransomware detection system using the AES model and reverse shell techniques is a meticulously designed structure that integrates cryptographic principles, real-time analysis, and intelligent decision-making to combat ransomware threats effectively. This framework is designed to ensure the highest levels of data integrity, confidentiality, and security while adapting to evolving cyber threats. The key components of the framework include systematic layers of detection, analysis, and response to ransomware activities.

The ransomware detection system's foundation lies in its layered approach, where each layer contributes uniquely to the overall protection mechanism. The Data Monitoring Layer is responsible for tracking all file operations continuously, identifying unusual behaviors such as unauthorized encryption activities, and triggering alerts when suspicious patterns are detected. This layer operates seamlessly with minimal resource consumption to ensure smooth system performance.

XIII. CONCLUSION

This research represents a comprehensive effort to understand and develop a strategy for ransomware detection using the AES model in cybersecurity. With the increasing cyber threats, ransomware has be come one of the most dangerous forms of attacks that organizations can face today. These attacks are characterized by their ability to disrupt systems, encrypt data, and impose hefty financial demands for decryption, making hem a significant threat that requires a strong and innovative defense approach. The AES model, which relies on the mathematical properties of symmetric encryption, offers a robust solution to combat these threats. By leveraging the characteristics of AES encryption, the model can detect suspicious activities carried out by ransomware, such as rapid file encryption, unusual access to critical files, or deviations from standard encryption patterns. This enables ransomware detection programs to analyze and respond preemptively, reducing the potential for significant damage.

XIV. REFERENCES

[1] Pigola, Angelica, Priscila RezendeDaCosta, Marcos Ferasso, and Luis FabioCavalcanti da Silva. "Enhancing cybersecuritycapability investments: Evidence fromanexperiment." Technology in Society 76(2024): 102449.

[2] Aidan, Jagmeet Singh, and Urvashi Garg. "Advanced Petya ransomware and mitigationstrategies." In 2018 First International Conference on SecureCyberComputing and Communication (ICSCCC), pp. 23-28. IEEE, 2018.

[3] Comito, Carmela, Agostino Forestiero, and Clara Pizzuti. "Word embeddingbasedclustering to detect topics in social media." In IEEE/WIC/ACM International Conference on Web Intelligence, pp. 192-199. 2019.

[4] Ilker, K. A. R. A., and Murat Aydos. "Cyber fraud: Detection and analysis of the crypto- ransomware." In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0764-0769. IEEE, 2020.

[5] Wecksten, Mattias, Jan Frick, Andreas Sjostrom, and Eric Jarpe. "A novel method for recovery from Crypto Ransomware infections." In 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 1354-1358. IEEE, 2016

[6] Mimura, Yuiko, Toshio Tsuchiya, Kaho Moriyama, Kanna Murata, and Sana Takasuka. "UX design for mobile application of E-Commerce site by using Kansei interface." In Advances in Industrial Design: Proceedings of the AHFE 2020 Virtual Conferences on Design for Inclusion, Affective and Pleasurable Design, Interdisciplinary Practice in Industrial Design, Kansei Engineering, and Human Factors for Apparel and Textile Engineering, July 16–20, 2020, USA, pp. 641-647. Springer International Publishing, 2020

[7] Alotaibi, Fahad M., and Vassilios G. Vassilakis. "Sdn-based detection of self-propagating ransomware: the case of badrabbit." Ieee Access 9 (2021): 28039- 28058.

[8] Aiswarya, E. S., Adheena Maria Benny, and Leena Vishnu Namboothiri. "CLOP Ransomware Analysis Using Machine Learning Approach." In Computer Networks and Inventive Communication Technologies: Proceedings of FourthICCNCT 2021, pp. 593-600. SpringerSingapore, 2022.

[9] Kyurkchiev, Nikolay. "Selected TopicsinMathematical Modeling: Some NewTrends."Dedicated to Academician Blagovest Sendov (1932-2020), LAPLambertAcademic Publishing (2020).

[10] Beşiktaş, Cihangir, DidemGozupek, Aydın Ulaş, and Erhan Lokman. "Securevirtual network embedding with flexiblebandwidth-based revenue maximization**."Computer Networks 121 (2017): 89-99.**

[11] Kara, Ilker, and Murat Aydos. "Static and dynamic analysis ofthird generation cerber ransomware." In 2018

International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), pp. 12-17. IEEE, 2018.

[12] Almashhadani, Ahmad O., Mustafa Kaiiali, Sakir Sezer, and Philip O'Kane. "A multi-classifier network-based crypto

ransomware detection system: A case study of locky ransomware." IEEE access 7 (2019): 47053-47067.

[13] Trautman, Lawrence J., and Peter C. Ormerod. "Wannacry, ransomware, and the emerging threat to

corporations." Tenn. L. Rev. 86 (2018): 503. https://doi.org/10.2139/ssrn.3238293

[14] Chen, You-Shyang, Jerome Chih-Lung Chou, Yu-Sheng Lin, Ying-Hsun Hung, and Xuan-Han Chen. "Identification of

MEs in the Critical Factors of an IS Backup System Using a Three-Stage Advanced Hybrid MDM–AHP

Model." Sustainability 15, no. 4 (2023): 3516. https://doi.org/10.3390/su15043516