Ransomware Attacks: Tools and Techniques for Detection

Khowla Khaliq
Department of Computer Science,
UniSZA, Gong Badak Campus,
Universiti Sultan Zainal Abidin, Malaysia
& Department of CS & IT
The Superior University
Lahore-54500, Pakistan
khowla.khaliq07@gmail.com

Nor Zairah Ab Rahim
Razak Faculty Technology and Informatics, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra,
54100 Kuala Lumpur, Malaysia
nzairah@utm.my

Khalid Hamid
Department of Computer Science, The Superior University *Lahore-54000, Pakistan*
khalid6140@gmail.com

Muhammad Ibrar
Department of Computer & Mathematical Sciences New Mexico Highlands University, Las Vegas, USA,
mibrar@live.nmhu.edu

Uzair Ahmad
NCBA&E
Lahore-54500, Pakistan
uzairahmad9594@gmail.com

Muhammad Ubaid Ullah
Green
International University
Lahore, Pakistan
muhammad.ubaidullah@giu.edu.pk

2024 2nd International Conference on Cyber Resilience (ICCR) | 979-8-3503-9496-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCR61006.2024.10532926

***Abstract*- Ransomware is a sort of crypto virology virus that attempts to expose or persistently limit access to the accused's private information until a ransom payment is made. Although some ransomware might simply lock the machine without affecting any files, more complex viruses use a tactic known as crypto viral blackmail. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. It encrypts the user's data, rendering them unreadable, and then asks for a ransom from the person to decode them. This paper discusses the characteristics of ransomware, the functionality of ransomware, and the variants of ransomware. Lastly, a framework is proposed to detect the ransomware using the "Kaspersky" anti-malware tools and a virtual machine to prevent ransomware attacks.**

***Index Terms*-- Ransomware, Crypto-Ransomware, Locker-Ransomware, Kaspersky, Anti-Ransomware Solution.**

I. Introduction

Ransomware is a sort of malicious software that encrypts the data of a user or corporation and then demands a ransom in exchange for decrypting the data. This can happen to either an individual user or an entire company. Cybercriminals drive organizations into a corner where the only viable alternative is to pay the ransom by encrypting specific data and demanding a ransom in exchange for the private key. One of the first known ransomware attacks was the 1989 AIDS trojan (PC Cyborg Virus). Floppy disks were used for distribution. Even though the virus was simple and used symmetric cryptography, victims needed to send $189 to a P.O. box in Panama to regain access to their systems. Some ransomware variants have been updated to include additional features, such as security flaws, to convince victims to pay the ransom [1].

The widespread use of ransomware has quickly made it the type of malicious software that is the most visible and widespread. Recent ransomware attacks have affected the ability of organizations to perform essential services, making city government services inoperable and causing considerable damage to a wide range of enterprises [2].

Recovery times for ransomware can vary greatly. Companies are only down for a day or two in sporadic cases. In some rare cases, it can take months. Given their struggle with not knowing what they are doing, most businesses fall between two and four weeks [3].

A. *Ransomware and its Characteristics*

Ransomware is a cyberattack that restricts users' access to their devices, whether by holding the display or the victims' documents until a ransom has been paid. Ransomware is classified depending on multiple factors, including its intensity, method of blackmail, persons aimed, and devices impacted. Malware behaviour analysis reveals that ransomware behaves entirely differently than other types of malware. The diagram demonstrates the five major actions taken throughout a ransomware attack [4,21].

B. *Techniques for detecting, preventing, and mitigating ransomware attacks*

Many solutions have been proposed to analyze and dynamically respond to detected anomalies, protecting users and organizations from ransomware attacks. Although each ransomware employs a distinct encryption technique, examining the executable code and locating those specific crypto components would be hugely advantageous. To analyze and recognize data encryption components, numerous methodologies are being used. The two assessment and identification approaches can be categorized as Static and dynamic analysis. The contextaware term was derived in 1994 by Schilit and Theimer. It is any information that is used to describe an entity's condition is referred to as context. A person, location, or thing is considered vital to the relationship between an application and a user. Users and applications are also referred to as an entity [4].

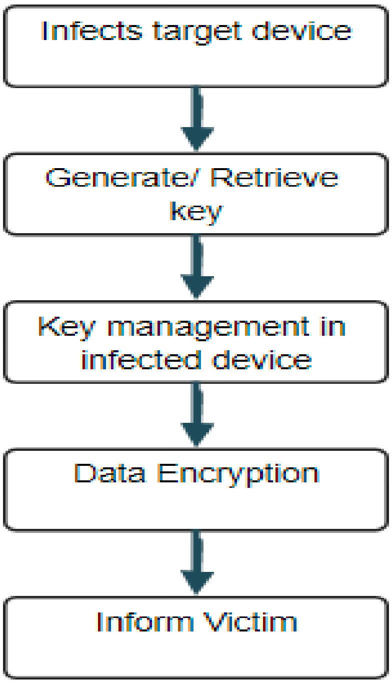

Figure 1: Characteristics of Ransomware.

C. Static Analysis

The use of static analysis allows for the early detection of crypto-binary functions. The heuristic analysis it performs includes looking for loops, entropy, and an unusually high ratio of bitwise operations. These methods facilitate signature detection with the help of data flow graphs and cryptographic constants for analysis.

D. Dynamic Analysis

Learning cryptographic algorithms in real time is the goal of dynamic analysis. One approach to understanding the disturbance produced is to examine the avalanche effect of input on output. The analysis also considers the sum of sequential memory accesses based on input and output parameters.

Numerous free and paid sources are available on the marketplace for ransomware assessment, identification, and intrusion recovery. These solutions employ a strategy that needs to be extracted from ransomware interaction from network communication logs, system states, and I/O exchanges. Many of these tools effectively detect and attempt to prevent many types of ransomware [9].

E. Problem Statement

Ransomware has caught the interest of cyber security departments and authorities in past years due to its fast-growing threats and the development of new variations in trying to bypass virus protection and anti-malware software. It is an advanced malware, but it has captivated the attention of malicious hackers due to its effective attack and immediate effect on economic stakes. The goal of ransomware is to prevent its victim from trying to access one's assets by holding the operating system or hiding aimed records that appear meaningful to the person, which include personal data like; pictures, documents including Excel sheets, and slideshows. As a result, the victim must suffer greatly for his valuable data.

This research will include a thorough ransomware attack workflow and its character traits, which can be a foundation for future ransomware research. Furthermore, current ransomware monitoring systems and established ransomware prevention strategies will be reviewed. We will suggest the best model for detecting and preventing ransomware based on the study results.

II. Literature Review

In their study, Rhythima Shinde et al. conducted a systematic review, interview sessions with victims of ransomware, and a survey with a random selection of victims and non-victims of ransomware. They went on to say that low-ranking knowledge among many business experts was affirmed, and unwillingness to spend as a victim is a universal pattern. The researchers have found that ransomware knowledge and understanding are extremely low, particularly among the elderly. With the emergence of Web services, the spread of ransomware has already become relatively simple. Workers' rising carelessness and reliance on the IT department for malware and viruses is affirmed in office settings. Moreover, established remediation strategies are likely adequate, but very few individuals use them. Finally, they affirmed a long-held belief concerning ransomware nearly all victims are extremely reluctant and thus unable to pay that money [11].

Two researchers, Jinal P. Tailor and Ashish D. Patel, demonstrated that ransomware has vastly improved its encryption methods. Furthermore, a successful detection system that drastically minimizes victim data loss might be developed via meticulous investigation of ransomware behavior. Several families of ransomware were found to share several commonalities in the study's findings. Ransomware is becoming more common, so the encryption algorithms used to lock users out of their data are getting more complex. Defending against ransomware will remain a top priority for researchers and IT security experts. When suspicious file activity is detected, the user is notified immediately by CryptoDrop, an early warning detection system. Implementing practical protection methods is achievable in Windows by continuously monitoring file system activity and registry activity; if these registry values are monitored in real-time, ransomware can be detected [1].

Amos Loh Yee Ren et al. proposed a method to deal with ransomware or malware by using virtual machines. Instead of allowing malware to infect the host system, the goal is to detach potential suspicious programs into the virtual environment and prevent their spread. While our solution successfully isolates any suspicious program until it could cause significant damage, it has some constraints. With new technological advances, it's challenging for a system to run over very few virtual machine instances at once. As a result, the user is limited to four downloads per instance because each file is placed in a separate, dedicated virtual machine to prevent one document from contaminating the others [12].

In their survey study, Bander Ali Saleh and Al-rimy et al. filled the void and presented a comprehensive evaluation of the research on ransomware and its detection and protection strategies. The survey presented a fresh taxonomy of ransomware from multiple angles. In addition, they elaborated on the variables that contribute to the success of ransomware assaults before covering the study into ransomware countermeasures, including analysis,

979-8-3503-9496-2/24/$31.00 ©2024 IEEE

prevention, detection, and prediction solutions. The survey concluded with a brief discussion of outstanding issues and potential future study topics [7].

In their study, Saurabh Kumar Sen et al. provided the groundwork for further investigation into the ransomware problem in enterprises. To demonstrate the operation of ransomware, they depicted the difficulties businesses face using a similar format. By blending research, a personal illustration of a ransomware assault, Cyber Security tool experience, and a graphical representation of ransomware's work, the general public will better understand the risk of a ransomware attack. This study aimed to enhance malware detection, prevention, and mitigation. Using the way to lessen the harm caused by ransomware attacks and techniques to minimize network vulnerabilities to ransomware attacks. In addition, in the future, this research will aid in developing a more effective and simple malware to minimize ransomware-related organization losses. Additionally, this discovery will inspire fresh researchers and analytics for decrypting tainted files [2].

Francesco Mercaldo presented a hybrid conceptual model for preventing ransomware threats by seeking to exploit API calls using static analysis and commands using dynamic analysis. They tested the impact of API calls and commands to distinguish between ransomware and legitimate implementations using the Cuckoo structure, and the outcomes were promising. The researcher intends to assess the proposed conceptual model and its performance on a significantly bigger class of applications, both inconsequential and harmful, in the long term. Furthermore, the authors intended to consider the use of official solutions to increase the accuracy of ransomware mitigation tasks, owing to the effectiveness of analysis techniques in those other disciplines [9].

Ibrahim Nadir and Taimur Bakhshi researched the history and latest transformation of ransomware attacks, giving a comprehensive classification scheme of the underlying security holes and presently offered mitigation strategies. Further, precautionary suggestions to assist users and service providers in securing equipment against ransomware risks were addressed. Ultimately, the economic and broad consequences of trying to make monetary compensation and web resources provided by protection and law-enforcement concerns were summarized to boost consumer awareness and empower people against such an increasingly proficient form of recent cyberattacks [3].

In their paper, Zhen Lia and Qi Lia offered two preemptive ways to counteract data-selling ransomware: preventive data encryption and preventive data deception. They argued that users may create a preventative portfolio by combining the two preventive actions. They created a one-of-a-kind game theoretical model of data-selling ransomware to investigate the attacker and victim equilibrium strategies. The portfolio equilibrium solution, data encryption, and deception tradeoff analysis were constructive for customers setting up systems to protect against ransomware assaults. The effectiveness of the preventative portfolio was proved through simulated testing, which increased user utility while significantly reducing the attacker's profit [6].

Ransomware attack detection is a critical cybersecurity challenge that may be leveraged with advanced machine learning techniques [22-35] to enhance detection capabilities, allowing for more proactive and adaptive responses to evolving ransomware threats.

III. Proposed Methodology

Ransomware is a growing illegal behavior with multiple variations [36]. The elements of sharable or interconnected drive systems, external sources storage server devices, and cloud computing services modelled to compromised machines are all encrypted by different aspects.

Although it is impossible to completely eradicate the ransomware threat, it might be managed by taking some precautions. Based on earlier research, notably [12], a method utilizing virtual machines (VMs) is created to detect and prevent ransomware [16]. We've suggested an approach for this purpose to detect and prevent ransomware.

Our ransomware detection process typically consists of several multiple blocks (e.g. source device, threat detection with the help of various pre-defined security rules and attack patterns). First, information from the attack log file is gathered and parsed. Next, normalization is done to standardize and save it in a format that allows for easy analysis and reviews, correlation via rule engine or based on various patterns and analytical techniques, and trigger events), all of which can operate independently but all work together.

Phase 1

In the proposed methodology, phase 1 will be based on a controlled environment to detect a ransomware attack. To detect the real-time ransomware attack, the “Kaspersky” ransomware detection tool will be used which is a ransomware protection tool and provides cloud services for behavior detection and blocking ransomware on the spot. The controlled environment includes signature-based detection of ransomware, behavior-based detection of ransomware, correlation techniques for detecting ransomware, and rules and policies defined to detect ransomware.

Phase 2

In phase 2 of the proposed methodology, we use a VM to deploy a security tool or proxy-based software firewall for ransomware avoidance. It is sometimes referred to as a proxy server or a gateway firewall.

Protecting network resources using message filtering at the application layer, this proxy server doubles as a firewall and web filter. One function of a proxy server is to act as an intermediary between clients and other servers. It can compress data, filter traffic, and find diseases. Using a proxy server also allows users to remain anonymous online or gain access to restricted resources. On the other hand, a proxy firewall monitors every data passing through it in search of malicious activity.

It may also enforce security policies and identify network intrusions. A good proxy server will filter out harmful websites before reaching the internal network. Serving as a conduit between end users and the internet. That's why it's helpful in keeping hackers out of a closed network. The primary function of proxy servers placed in VMs is to protect direct connections between Internet clients and resources. The proxy server also protects the client's IP address from being identified when the client requests any other servers.

Figure 2 elaborates on the proposed architecture for ransomware detection and prevention.

In the proposed methodology, a controlled environment has been first used to detect a ransomware attack. To detect the real-time ransomware attack, the “Kaspersky” ransomware detection tool will be used, which is a ransomware protection tool and provides cloud services for

979-8-3503-9496-2/24/$31.00 ©2024 IEEE

behaviour detection and blocking ransomware on the spot. The controlled environment includes signature-based detection of ransomware, behaviour-based detection of ransomware, correlation techniques for detecting ransomware, and rules and policies defined to detect ransomware. When a user clicks on a link, “Kaspersky” analyses it and matches the executable file with the stored signatures and rules in the database. If the executable file doesn’t match with earlier identified signatures, the file will be passed to the user for further action. If the executable file matches with earlier identified signatures the file will be passed to the second phase i.e., the virtual machine [18].

In the second phase of the proposed methodology, we use a VM to deploy a security tool or proxy-based software firewall for ransomware avoidance. It is sometimes referred to as a proxy server or a gateway firewall. Protecting network resources using message filtering at the application layer [19], this proxy server doubles as a firewall and web filter. One function of a proxy server is to act as an intermediary between clients and other servers [20]. It can compress data, filter traffic, and find diseases. Using a proxy server also allows users to remain anonymous online or gain access to restricted resources. On the other hand, a proxy firewall monitors every data passing through it in search of malicious activity [13].

It may also enforce security policies and identify network intrusions [14]. A good proxy server will filter out any harmful websites before they reach the internal network. Serving as a conduit between end users and the internet [15]. That's why it's useful for keeping hackers out of a closed network. The primary function of proxy servers placed in VMs is to protect direct connections between Internet clients and Internet resources. The proxy server also protects the client's IP address from being identified when the client makes any request to any other servers [17].

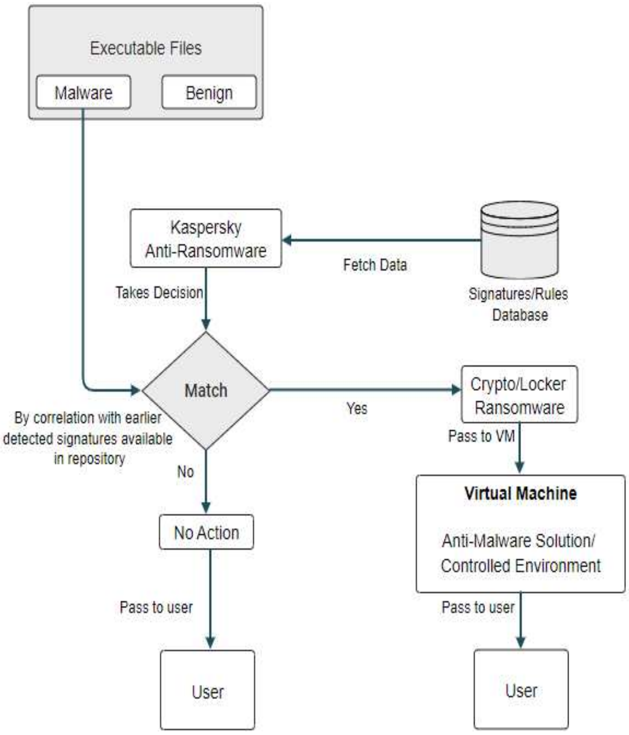
Executable Files
Malware
Benign
Kaspersky Anti-Ransomware
Fetch Data
Signatures/Rules Database
Takes Decision
Match
By correlation with earlier detected signatures available in repository
Yes
Crypto/Locker Ransomware
Pass to VM
No
No Action
Virtual Machine
Anti-Malware Solution/ Controlled Environment
Pass to user
Pass to user
User
User

Figure 2: Proposed Architecture for Ransomware Detection and Prevention.

IV. Conclusion

Ransomware is a crypto-virology virus that seeks to expose or permanently restrict access to the accused's sensitive information in exchange for a ransom payment. In this research article, an analysis is conducted to reveal the varieties of ransomware assaults, how ransomware attacks work, and approaches utilized for ransomware detection and prevention. A ransomware detection framework is also offered to detect the ransomware attack. The proposed method will first check the executable files by comparing them to the "Kaspersky" ransomware detection tool's database. The "Kaspersky" database contains ransomware signatures and established rules for ransomware detection. If the executable file fits the signature, the detector will identify it as ransomware and thus will restrict it. Alternatively, the detector will provide the file to the users for additional processing.

Acknowledgment

We are very thankful to Dr. Nor Zairah Ab Rahim and the institute of Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia.

References

[1] J. P. Tailor and A. D. Patel, “A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control,” p. 7, 2017.

[2] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,” Comput. Secur., vol. 74, pp. 144–166, May 2018, doi: 10.1016/j.cose.2018.01.001.

[3] N. Aldaraani and Z. Begum, “Understanding the impact of Ransomware: A Survey on its Evolution, Mitigation and Prevention Techniques,” in 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Apr. 2018, pp. 1–5. doi: 10.1109/NCG.2018.8593029.

[4] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, “Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions,” Sustainability, vol. 14, no. 1, p. 8, Dec. 2021, doi: 10.3390/su14010008.

[5] M. A. S. Monge, J. M. Vidal, and L. J. G. Villalba, “A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation,” in Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg Germany, Aug. 2018, pp. 1–10. doi: 10.1145/3230833.3233249.

[6] E. Berrueta, D. Morato, E. Magaña, and M. Izal, “Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic,” Expert Syst. Appl., vol. 209, p. 118299, Dec. 2022, doi: 10.1016/j.eswa.2022.118299.

[7] I. A. Chesti, M. Humayun, N. U. Sama, and N. Jhanjhi, “Evolution, Mitigation, and Prevention of Ransomware,” in 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, Oct. 2020, pp. 1–6. doi: 10.1109/ICCIS49240.2020.9257708.

[8] “Gonzalez and Hayajneh - 2017 - Detection and prevention of crypto-ransomware.pdf.”

[9] F. Mercaldo, “A framework for supporting ransomware detection and prevention based on hybrid analysis,” J. Comput. Virol. Hacking Tech., vol. 17, no. 3, pp. 221–227, Sep. 2021, doi: 10.1007/s11416-021-00388-w.

[10] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, “Ransomware detection and mitigation using software-defined networking: The case of WannaCry,” Comput. Electr. Eng., vol. 76, pp. 111–121, Jun. 2019, doi: 10.1016/j.compeleceng.2019.03.012.

[11] R. Shinde, P. Van der Veeken, S. Van Schooten, and J. van den Berg, “Ransomware: Studying transfer and mitigation,” in 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, Dec. 2016, pp. 90–95. doi: 10.1109/CAST.2016.7914946.

[12] R. Brewer, “Ransomware attacks: detection, prevention and cure,” Network Security, vol. 2016, no. 9, pp. 5–9, Sep. 2016, doi: 10.1016/S1353-4858(16)30086-1.

[13] K. Hamid, M. waseem Iqbal, M. Aqeel, T. Rana, and M. Arif, “Cyber Security: Analysis for Detection and Removal of Zero-Day Attacks (ZDA),” 2023, pp. 172–196. doi: 10.1201/9781003190301-10.

[14] S. Bhatti, K. Hamid, A. Bashir, zishan zafar, ahmad raza, and M. waseem Iqbal, “Solutions, Countermeasures, And Mitigation Methods For The Rise Of Automotive Hacking,” vol. 56, pp. 77–99, Jun. 2023, doi: 10.17605/OSF.IO/UG6VD.

[15] Z. Zafar, K. Hamid, M. Kafayat, M. waseem Iqbal, Z. Nazir, and A. Ghani, “AI-Based Cryptographical Framework Empowered Network Security,” *Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng.*

Technol. Ed., vol. 42, pp. 497–510, Apr. 2023, doi: 10.17605/OSF.IO/W69VT.

[16] K. Hamid, M. waseem Iqbal, M. Aqeel, X. Liu, and M. Arif, "Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA)," 2023, pp. 248–262. doi: 10.1007/978-981-99-0272-9_17.

[17] K. Hamid, S. Bhatti, N. Hussain, M. Fatima, S. Ramzan, and M. waseem Iqbal, "Irregularity Investigation of Certain Computer Networks Empowered Security," vol. 41, pp. 75–93, Dec. 2022, doi: 10.17605/OSF.IO/TJ6XN.

[18] Nasir, M.U., et al., Breast cancer prediction empowered with fine-tuning. Computational Intelligence and Neuroscience, 2022.

[19] Hujran, O., et al., "Big Data and Its Effect on the Music Industry", The 3rd International Conference on Software Engineering and Information Management, 2020, pp. 5–9.T. Mohamed, et al., "Intelligent Hand Gesture Recognition System Empowered With CNN," in Proc. 2022 International Conference on Cyber Resilience, ICCR 2022, Dubai, UAE, Oct. 6-7, 2022, doi: 10.1109/ICCR56254.2022.9995760.

[20] Alkeem, E.A., Shehada, D., Yeun, C.Y., Zemerly, M.J. and Hu, J., 2017. New secure healthcare system using cloud of things. Cluster Computing, 20(3), pp.2211-2229.

[21] Zitar, R.A., Abualigah, L., Al-Dmour, N.A., "Review and analysis for the Red Deer Algorithm", Journal of Ambient Intelligence and Humanized Computing, , 2021.

[22] Malik, J.A. and Saleem, M., 2022. Blockchain and Cyber-Physical System for Security Engineering in the Smart Industry. In Security Engineering for Embedded and Cyber-Physical Systems (pp. 51-70). CRC press.

[23] Cuauhtemoc, J., et al., 2022. Ai-based prediction of capital structure: Performance comparison of ann svm and lr models. Computational Intelligence & Neuroscience.

[24] Shah, R.K., et al., 2022, May. Detect phishing website by fuzzy multi-criteria decision making. In 2022 1st International Conference on AI in Cybersecurity (ICAIC) (pp. 1-8). IEEE.

[25] Ahmed, F., Asif, M. and Saleem, M., 2023. Identification and Prediction of Brain Tumor Using VGG-16 Empowered with Explainable Artificial Intelligence. International Journal of Computational and Innovative Sciences, 2(2), pp.24-33.

[26] Nidal Al-Dmour , "TraffSim: Multiagent Traffic Simulation", European Journal of Scientific Research, ISSN 1450-216X Vol.53 No.4 (2011), pp.570-575, EuroJournals Publishing, Inc. 2011.

[27] Heba Abunahla, Dina Shehada, Chan Yeob Yeun, Baker Mohammad, Maguy Abi Jaoude, "Novel secret key generation techniques using memristor devices", AIP Advances, February 2016

[28] Saleem, M., Khan, M.S., Issa, G.F., Khadim, A., Asif, M., Akram, A.S. and Nair, H.K., 2023, March. Smart Spaces: Occupancy Detection using Adaptive Back-Propagation Neural Network. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-6). IEEE.

[29] Athar, A., Asif, R.N., Saleem, M., Munir, S., Al Nasar, M.R. and Momani, A.M., 2023, March. Improving Pneumonia Detection in chest X-rays using Transfer Learning Approach (AlexNet) and Adversarial Training. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-7). IEEE.

[30] Abualkishik, A., Saleem, M., Farooq, U., Asif, M., Hassan, M. and Malik, J.A., 2023, March. Genetic Algorithm Based Adaptive FSO Communication Link. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-4). IEEE.

[31] Turki Al Masaeid, et al., "Futuristic Design & Development of Learning Management System including Psychological Factors Resolution", Journal for ReAttach Therapy and Developmental Diversities, 5(2s), 176–188, 2022.

[32] Z. E. Ahmed et al., "Optimization Procedure for Intelligent Internet of Things Applications," 2022 International Conference on Business Analytics for Technology and Security (ICBATS), 2022

[33] T. M. Ghazal et al., "E-Supply Chain Issues in Internet Of Medical Things," 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2022

[34] Malik, R., Raza, H. and Saleem, M., 2022. Towards A Blockchain Enabled Integrated Library Managment System Using Hyperledger Fabric: Using Hyperledger Fabric. International Journal of Computational and Innovative Sciences, 1(3), pp.17-24.

[35] Malik, J.A. and Saleem, M., 2022. Blockchain and Cyber-Physical System for Security Engineering in the Smart Industry. In Security Engineering for Embedded and Cyber-Physical Systems (pp. 51-70). CRC press.

[36] Joonsang Baek, Quang Hieu Vu, A. Jones, S. Al Mulla and Chan Yeob Yeun, "Smart-frame: A flexible, scalable, and secure information management framework for smart grids," 2012 International Conference for Internet Technology and Secured Transactions, London, UK, 2012

979-8-3503-9496-2/24/$31.00 ©2024 IEEE