Fifteen Deadly Cybersecurity Threats Aimed Covid-19

Abdulellah A. Alaboudi
Assistant Professor of computer science, Shaqra University, Saudi Arabia

Abstract
Cybersecurity has been vital for decades and will remain vital with upcoming ages with new technological developments. Every new day brings advancement in technology, which leads to new horizons, and at the same time, it brings new security challenges. Numerous researchers around the globe are continuously striving hard to provide better solutions for the daily basis of new arising security issues. However, the challenges are always there. These challenges become new norms during the current Covid pandemic, where most industries, small industrial enterprises, education, finance, public sectors, etc. were under several attacks and threats globally. The hacker has more opportunities during the pandemic period by shifting most of the operations live. This research enlightened the several cybersecurity attacks and threats during this pandemic time globally. It provided the best possible recommendations to avoid them using the cyber awareness and with appropriately linked training. This research can provide a guideline to the above stated sector by identifying the related attacks.

Keywords
Cybersecurity, Attacks, Security Threats, Covid-19, Mitigation recommendations.

1. Introduction

The world is changing with time in all domains, and that change is because of technological development. It is evident that the technology is the driving sources for this huge change, such as for the Society 1.0 to Society 5.0, Industrial Revolution IR 1.0 to 5.0, Healthcare 1.0 to 5.0, in cellular world G1 to G5, etc. in all domains. Technological development is the real source for these changes. This development is identical in all daily life applications, and they were growing with a constant speed somehow. However, a rapid change, development and technological development was witnessed during the current pandemic Covid-19 period, where most of the people, industries, offices, public sector were forced to be limited to homes, and there was not any other mean to continue the daily life business and routine operations. This challenge was huge, and at the early stages, it had imaginations that now world can not move with this pandemic situation. However, once again the technology is the one who come forward and bridged this gap, and slowly things started moving. This great move brought to us several new challenges as well, such as resources, trained users, experts, and special challenges for not expert users of technology.

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.18

The recent literature shows a great hype in video conferencing tools globally. In [1] it is evident that a series of countries economies depended on technology, and most of the operations were performed using the video conferencing tools, such as within North America, United States, Canada, Europe, UK,

Germany, Italy, Spain, France, rest of the Europe, Asia-Pacific, China, Japan, India, Rest of Asia-Pacif, and rest of the world. Further, this growth can be witnessed in Figure 1 and Figure 2.

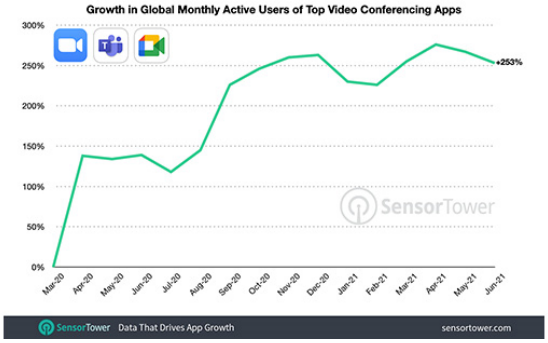

Figure 1: Global Growth for Video Conferencing Apps [2]

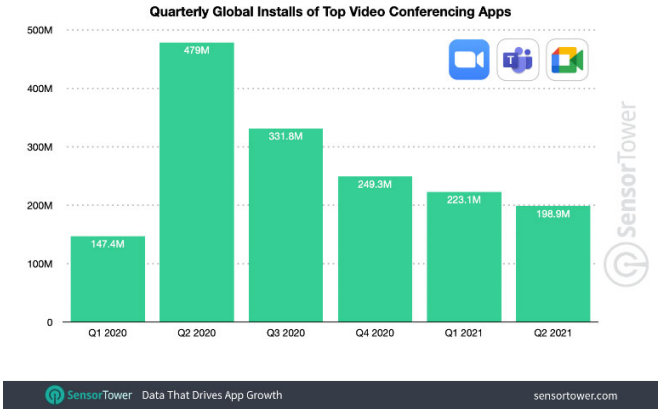

Figure 2: Global Growth for Video Conferencing Apps [3]

In [4] further elaborated more on the work meetings during the Covid-19 and its pros and cons for online meetings. In [5] explain the cutting-edge technologies, which help the

society during this pandemic period. This other side of the coin is the cost security cost of these applications, a series of different attacks [6] happened during this pandemic period.

This research elaborates the higher use of technology and its dependency during this pandemic period and cybersecurity threats aimed in general and particularly to this Covid-19 period. Further research elaborates on the possible precautions and mitigation methods for individuals, organizations, and different sectors.

The rest of the paper is organized in following way, section 2 elaborates in detail the literature review for the top 15 attacks and cybersecurity threats aimed to the current pandemic period. Section 3 provides a comprehensive discussion, to conclude the issues, and recommend the possible precautions, and mitigation methodologies, Section 4 elaborates on conclusion of this research.

2. Literature Review

This section will briefly identify the top 15 attacks during this Covid-19 period and their severity and domain one by one.

2.1 Malware

Among the most popular attacks during this pandemic period Malaware was the one of them. Malware is the combination of Mal + ware, the Mal is taken from malicious and ware is taken from the software, after combination it becomes malware, which represents to a software with malicious functioning, or undesired functioning. Several research are available to explain different mitigation and detection methods for malware, such as in [7,8]. In [9-11] authors discussed about malware identification in Android platforms using different techniques. The current intensity of malware attacks can be identified through following figure 3, which depicts the different types of malwares.

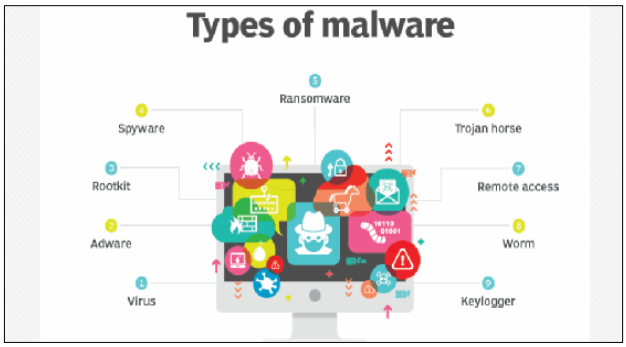

Figure 3: Types of Malware [12]

2.2 Phishing

1. Phishing is another most common type of attack, where hackers easily can steal user data, by applying the phishing approach, that data could be login credentials, or any other users related data, which can be exploited later. Mostly this type of attack is to steal the credit card data. In [13-15], authors briefed in a detail about the phishing attacks identifications using the AI advance approaches, in [16] authors presented a phishing funnel model for finding the phishing attacks for the websites, these attacks [17] are common and most frequent for different applications. Phishing has several different ways to have attacks over the user end. Users need to be careful while using any unknown emails. They may avoid clicking any unknown links or even emails.

2.3 Man-in-the-middle attack (MITM)

Man in the middle attack is most common between user and web server when data packets are shared among both. In this type of attack attacker either destroy the integrity of the message partially or completely depending on the case. In [18] authors explained the mitigation methods for the Man in the middle attacks for Internet of Medical Things. This attack is common for most of the application domain. Figure 4 shows a typical type of man in the middle attack.

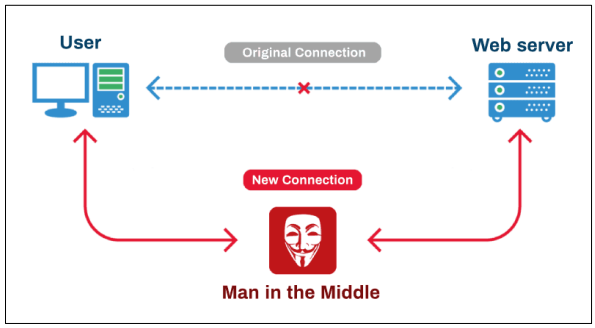

Figure 4: Man in the Middle Attack [19]

This attack type can be common in any type of network, including [20-22] Internet of things, smartphone applications and IoT based other applications as well. This attack was common for the video conferencing mainly during this covid-19 period.

2.4 Distributed Denial-of-Service (DDoS) attack

The hacker uses DDOS attacks to stop or deny service on the server, where the user can experience delay to receive the services. In this hacker try to attempt several attacks at the same time to keep the server ports busy, the distributed DDoS can create worsen situation for any targeted server. A typical scenario for the DDoS attack can be seen in Figure 5,

while Figure 6 shows the targeted industries for the quarter 2 of 2021 recent data.

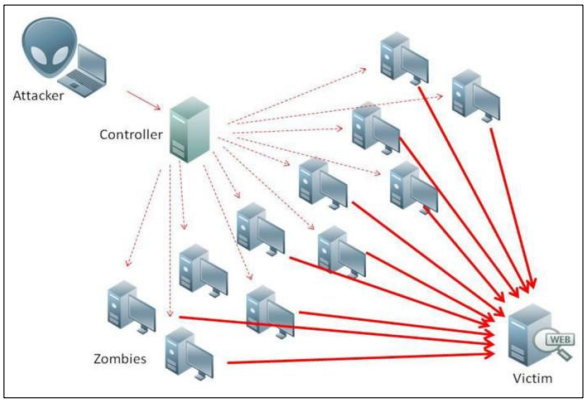

Figure 5: Man in the Middle Attack [20]

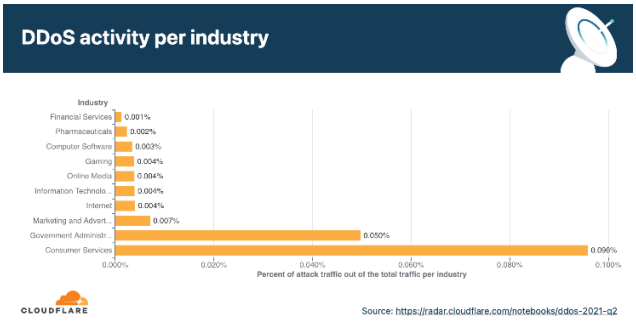

Figure 6: DDoS Attack for quarter 2 2021[21]

The authors in [22] defines defense mechanism against the DDoS attack to prevent from this situation. Authors in [23-25] authors described about the DDoS attacks on multimedia internet of things, using the machine learning approaches in Internet of things as well.

2.5 Zero-day exploit

A zero-day exploit is the type of vulnerability where hackers can find out any vulnerability in a limited time before the developers know about that, and that vulnerability can be exploited easily for different attacks depending on the vulnerability found. Authors in [26-28] explained about different vulnerabilities, in criminal network and smart cities. This attack is not common in most of the software, it depends totally on the software production quality, in case if secure SDLC is not adopted properly then possibly a number of vulnerabilities will be there to utilized otherwise, less chances for this type of attack.

2.6 SQL Injection

SQL injection is the type of attack where hackers mainly target to the backend of the application. Hacker plan to modify the data entries in different way directly. This type of attack is critical and can happen on any application [29-31], such as web-based application, mobile application, etc., which ever will have a database as a backend. A successful Injection attack can be capable of several things such as modifying the data, altering, deleting the data, reading and retrieving the data as well. Figure 7 can typically explain about the SQL injection attack.

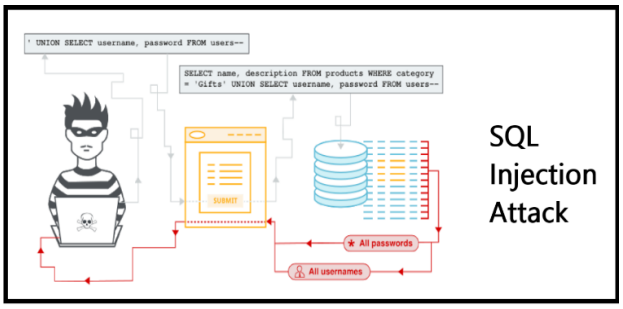

Figure 7: SQL Injection attack example [32]

SQL injection attack could be of several types, including inband SQL injection attack, Inferential (Blind) SQL Injection, Out-of-band SQL Injection, etc. this type of attack can be prevented by following the secure SDL phase secure coding critically to address all the issues, and manage the inputs values.

Reading sensitive and confidential data from the database

Retrieving the content of a specific file present on the database management system (DBMS)

Enforcing administrative operations like shutting down the DBMS

Without proper mitigation controls and security measures, the SQL injection attack can leave an application at a huge risk of data compromise. It can impact the data's confidentiality and integrity as well as the authentication and authorization with respect to the application. It can also empower an adversary to steal confidential information like user credentials, financial information, or trade secrets by misusing the vulnerability existing in an application or program.

2.7 DNS Tunnelling

DNS Tunneling is a unique type of process where attacker can encode the data for the protocols in DNS queries and

responses. This type of attack can make a ground for other attacks by injecting the malware, by bypassing the firewalls. This type of attack can also be done mainly for the web-based application but at the wider scale where it can involve the higher variety of different applications [33-34], including the smart gadgets and IoT-based applications. In addition, this is equally harmful for industrial internet of things [35-36] as well. Authors in [37] elaborate in detail about the DNS Tunnelling related issues.

2.8 Business Email Compromise (BEC)

Business Email compromise is very close to spam emails and Phishing attacks, where the hackers first start with target and wait for her response, and once having response, now can damage the victim machine easily. This approach is common for the business email accounts, where hacker can use fake or bogus invoices, receipts etc. to attract the victims, as later can utilize the business emails by controlling them for alteration and sharing the emails. In [38-41], authors described the business email issues and data breaches for the office emails.

2.9 Cryptojacking

Crypto currencies, become more favorite for the hackers where the hacker easily use Cryptojacking. In the Cryptojacking hackers use your machines computing power and generated the crypto currencies. Later they misuse the currencies and user machine computations. In [42-45] the authors elaborated about the cryptojacking. This type of attack is not as common as of the other attacks discussed, since this is only used for the crypto currency's generation.

2.10 Drive-by Attack

Any sort of attack has the man source as download, most of the software uses different approaches to scan the attachments, files, or any other related stuff before download. Since those downloaded files could be main source of attackers as a gateway to approach your machine. The drive-by-attack approach refers to the attacks through the download with unintentional downloads without scanning, which might have malicious software, code, etc. which behave like a gateway for the hackers. This approach can be applied for several application types, including web-based, mobile apps, etc. any sort of where download of files process is involved. In [46-49], authors explained this with different application areas such as cloud applications, Android application, etc. In [50] authors elaborated about the mitigation approaches for download attacks.

2.11 Cross-site scripting (XSS) attacks

Cross-site scripting XSS, having the same approach as of SQL injection attack. Mainly this belongs to the injection type of attack. The main difference between XSS and the hackers targets the front end of the application while the SQL injection targets the back end of the application, mainly the database. The authors [51] explained the integrated approach to prevent SQL and XSS scripting at the same time. These both type of attacks effective mitigation is through secure coding phase, where to follow the secure code standards to avoid injection attack. In [52-54] authors discussed about the injection attacks.

2.12 Password Attack

The hacker's password attack is the most common and heavily applied approach for personal and corporate users' data. The hacker has multiple ways to adopt the password attacks including, Dictionary attacks, Brute force attacks [55], Phishing attacks, credential stuffing, Keylogging, etc. the hackers adopted this as a most powerful tool. The authors in [56-59] discuss the security issues and concerns related to this.

2.13 Eavesdropping attack

The hackers mainly attempt eavesdropping by intercepting the communication or data packets, which the hacker can mishandle. The real challenge in this type of attack is that it is really hard to identify this attack and at the same time its mitigation as well. In [61-63] authors discussed the eavesdropping attacks with different perspectives. In [64] authors discussed the fast-eavesdropping attack against touchscreens.

2.14 AI-Powered Attacks

Handling advance cyber-attacks is not an easy job. With the technological development, the attackers also adopt advanced methods for attacks, making it even more critical. Cyber criminals are using AI drive attacks to compromise the targeted machines with more effective and efficient way, the AI drive main attacks are such as, AI Phishing Attacks, Malware and Ransomware, Data Poisoning, Insider Behavior Analysis Abuse, and Deep Fake [65], these AI base attacks are more powerful, and it is hard to handle them apparently in time. Further, authors in [66-68] elaborate on AI attacks.

2.15 IoT-Based Attacks

IoT based attacks are more common now a days, since most of the smart applications are using IoT devices which makes them more vulnerable at the same time with smarter. The authors discussed IoT-based application's role in different [69-72] areas, including smart homes, smart cities, smart devices, etc. In [73] authors describe the network-based Internet of Things baIoT attacks, their severity, and mitigation methods. In [74] the authors describe about the IoT based applications DDoS attacks and their mitigation. Further, authors in [75] authors discussed about cyber-physical attacks and their mitigation. Authors in [76] described about the cyber security challenges for IoT-based smart grid networks. Furthermore, there is a range of different IoT based attacks as mentioned in Figure 8.

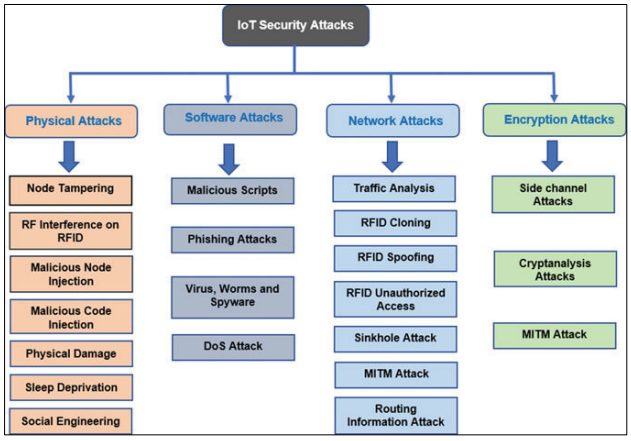

Figure 8: Internet of Things Attack [77]

3. Discussion

This research discussed the cyber security attacks aimed to the current pandemic Covid-19. The study highlighted that the technology is the only survival during this pandemic time, and will remain our survival for the future as well. However, with the rapid growth of technology in hurry brought us different number of challenges in terms of the security and privacy. The cybersecurity attacks are launched exponationally during this period on individual and corporate basis globally, The statiscis shows that the cyberattacks are ten time higher with the routine growth during this pandemic period. That is a high risk for the users.

This research further elaborates on the major fifteen different cybersecurity threats and attacks, their severity, and their attempts to different domains. Lastly, this research elaborate the different possible mitigation methods as well.

This research recommended avoiding the unnecessary use of the Internet, careful use of emails, and other related links, which may lead to compromise the data. Precautions and adopting security policies are the best approach to avoid any incidents before happenings.

Reference

[1] Dublin (Business Wire), Impact of COVID-19 on the Video Conferencing Market, 2020, https://www.businesswire.com/news/home/20200416005739/en/Impact-of-COVID-19-on-the-Video-Conferencing-Market-2020---ResearchAndMarkets.com, Accessed on November 2021.

[2] Guy Campos, Videoconferencing app usage 'hits 21 times pre-Covid levels', https://www.avinteractive.com/news/collaboration/usage-mobile-video-conferencing-apps-including-zoom-grew-150-first-half-2021-05-08-2021/, Accessed on November 2021.

[3] Sensor tower blog, Usage of Mobile Video Conferencing Apps Including Zoom Grew 150% in the First Half of 2021, https://sensortower.com/blog/video-conferencing-apps-mau-growth , Accessed on November 2021.

[4] Karl KA, Peluchette JV, Aghakhani N. Virtual Work Meetings During the COVID-19 Pandemic: The Good, Bad, and Ugly. Small Group Research. May 2021. doi:10.1177/10464964211015286

[5] Khan, N. A., Brohi, S. N., & Jhanjhi, N. Z. (2020). UAV's applications, architecture, security issues and attack scenarios: a survey. In Intelligent computing and innovation on data science (pp. 753-760). Springer, Singapore.

[6] N. A. Khan, S. N. Brohi and N. Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic", 2020.

[7] Singh, J., & Singh, J. (2021). A survey on machine learning-based malware detection in executable files. Journal of Systems Architecture, 112, 101861.

[8] Amer, E., Zelinka, I., & El-Sappagh, S. (2021). A Multi-Perspective malware detection approach through behavioral fusion of API call sequence. Computers & Security, 110, 102449.

[9] S. J. Hussain, U. Ahmed, H. Liaquat, S. Mir, N. Jhanjhi and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1-6, doi: 10.1109/ICCISci.2019.8716471.

[10] Nawaz, A. (2021). Feature Engineering based on Hybrid Features for Malware Detection over Android Framework. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2856-2864.

[11] K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," 2019 International Conference on Computer and Information

Sciences (ICCIS), 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.

[12] Ben Lutkevich, Types of Malware, Tech Target, https://searchsecurity.techtarget.com/definition/malware, Access on November 2021.

[13] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139-154.

[14] Ubing, A. A., Jasmi, S. K. B., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Phishing website detection: An improved accuracy through feature selection and ensemble learning. International Journal of Advanced Computer Science and Applications, 10(1), 252-257.

[15] Elijah, A. V., Abdullah, A., Jhanjhi, N., Supramaniam, M., & Abdullateef, B. (2019). 'Ensemble and deep-learning methods for two-class and multi-attack anomaly intrusion detection: An empirical study. Int. J. Adv. Comput. Sci. Appl, 10(9), 520-528.

[16] Abbasi, A., Dobolyi, D., Vance, A., & Zahedi, F. M. (2021). The phishing funnel model: A design artifact to predict user susceptibility to phishing websites. Information Systems Research, 32(2), 410-436.

[17] Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019, pp. 1-9, doi: 10.1109/MACS48846.2019.9024821.

[18] Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., & Boutaba, R. (2021). Man in the Middle Attack Mitigation in Internet of Medical Things. IEEE Transactions on Industrial Informatics.

[19] Noor Qureshi, How to make sure no man-in-the-middle attack can harm you, https://thehacktoday.com/how-to-make-sure-no-man-in-the-middle-attack-can-harm-you/, Accessed on November 2021.

[20] The new network, 2017: The year of widespread SDN adoption and DDoS attack mitigation, https://www.networkworld.com/article/3156344/2017-widespread-sdn-adoption-and-ddos-attack-mitigation.html, Accessed on November 2021.

[21] Vivek Ganti, et.al, DDoS attack trends for 2021 Q2, https://blog.cloudflare.com/ddos-attack-trends-for-2021-q2/, Accessed on November 2021

[22] Mishra, A., Gupta, N., & Gupta, B. B. (2021). Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommunication systems, 77(1), 47-62.

[23] Gopi, R., Sathiyamoorthi, V., Selvakumar, S. et al. Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. Multimed Tools Appl (2021). https://doi.org/10.1007/s11042-021-10640-6

[24] Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A review of intrusion detection system using machine learning approach. International Journal of Engineering Research and Technology, 12(1), 8-15.

[25] Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment," 2018 4th International Conference on Computer and Information Sciences (ICCOINS), 2018, pp. 1-5, doi: 10.1109/ICCOINS.2018.8510588.

[26] Lim, M., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Hidden link prediction in criminal networks using the deep reinforcement learning technique. Computers, 8(1), 8.

[27] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019, pp. 1-7, doi: 10.1109/MACS48846.2019.9024768.

[28] Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2019). Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. Journal of King Saud University-Computer and Information Sciences.

[29] N. Zaman and F. A. Almusalli, "Review: Smartphones power consumption & energy saving techniques," 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), 2017, pp. 1-7, doi: 10.1109/ICIEECT.2017.7916593.

[30] D. A. Shafiq, N. Z. Jhanjhi, A. Abdullah and M. A. Alzain, "A Load Balancing Algorithm for the Data Centres to Optimize Cloud Computing Applications," in IEEE Access, vol. 9, pp. 41731-41744, 2021, doi: 10.1109/ACCESS.2021.3065308.

Seungjin, L., Abdullah, A., & Jhanjhi, N. Z. (2020). A review on honeypot-based botnet detection models for smart factory. International Journal of Advanced Computer Science and Applications, 11(6), 418-435.

[31] A Almusaylim, Z., Jhanjhi, N. Z., & Alhumam, A. (2020). Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors, 20(21), 5997.

[32] Kraticakal, SQL Injection Attack: A Major Application Security Threat, https://www.kratikal.com/blog/sql-injection-attack-a-major-application-security-threat/, Accessd on November 2021.

[33] Jhanjhi, N. Z., Almusalli, F. A., Brohi, S. N., & Abdullah, A. (2018, October). Middleware Power Saving Scheme for Mobile Applications. In 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA) (pp. 1-6). IEEE.

[34] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi and L. T. Jung, "SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications," 2020 International Conference on Computational Intelligence (ICCI), 2020, pp. 305-310, doi: 10.1109/ICCI51257.2020.9247818.

[35] M. Humayun, N. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian and B. Selvaraj, "Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things," in IEEE Access, vol. 8, pp. 183665-183677, 2020, doi: 10.1109/ACCESS.2020.3028764.

[36] N. Zaman, A. B. Abdullah and L. T. Jung, "Optimization of energy usage in Wireless Sensor Network using Position Responsive Routing Protocol (PRRP)," 2011 IEEE Symposium on Computers & Informatics, 2011, pp. 51-55, doi: 10.1109/ISCI.2011.5958882.

[37] Soosahabi, R. (2021). SPARROW: A Novel Covert Communication Scheme Exploiting Broadcast Signals

in LTE, 5G & Beyond. arXiv preprint arXiv:2108.12161.

[38] Norah Saud Al-Musib, Faeiz Mohammad Al-Serhani, Mamoona Humayun, N.Z. Jhanjhi, Business email compromise (BEC) attacks, Materials Today: Proceedings, 2021, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.03.647. (https://www.sciencedirect.com/science/article/pii/S2214785321027425)

[39] S. K. Mishra et al., "Energy-Aware Task Allocation for Multi-Cloud Networks," in IEEE Access, vol. 8, pp. 178825-178834, 2020, doi: 10.1109/ACCESS.2020.3026875.

[40] A Almusaylim, Z., Jhanjhi, N. Z., & Alhumam, A. (2020). Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors, 20(21), 5997.

[41] Teoh, A. A., Ghani, N. B. A., Ahmad, M., Jhanjhi, N., Alzain, M. A., & Masud, M. (2022). Organizational Data Breach: Building Conscious Care Behavior in Incident Response. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 40(2), 505-515.

[42] Almulhim, M., Islam, N., & Zaman, N. (2019). A lightweight and secure authentication scheme for IoT based e-health applications. International Journal of Computer Science and Network Security, 19(1), 107-120.

[43] A. P. Singh et al., "A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5779-5789, Aug. 2021, doi: 10.1109/TII.2020.3037889.

[44] Khan, N. A., Jhanjhi, N. Z., Brohi, S. N., & Nayyar, A. (2020). Emerging use of UAV's: secure communication protocol issues and challenges. In Drones in Smart-Cities (pp. 37-55). Elsevier.

[45] Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers, 8(4), 79.

[46] S. Ali et al., "Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based," in IEEE Access, vol. 8, pp. 148007-148020, 2020, doi: 10.1109/ACCESS.2020.3014671.

[47] Zaman, N., & Ahmad, M. (2017). Towards the evaluation of authentication protocols for mobile command and control unit in healthcare. Journal of Medical Imaging and Health Informatics, 7(3), 739-742.

[48] Ren, A. L. Y., Liang, C. T., Hyug, I. J., Broh, S. N., & Jhanjhi, N. Z. (2020). A Three-Level Ransomware Detection and Prevention Mechanism. EAI Endorsed Transactions on Energy Web, 7(27).

[49] Jabeen, T., Jabeen, I., Ashraf, H., Jhanjhi, N., Mamoona, H., Mehedi, M., & Sultan, A. (2022). A Monte Carlo Based COVID-19 Detection Framework for Smart Healthcare. Computers, Materials, & Continua, 2365-2380.

[50] Egele, M., Kirda, E., & Kruegel, C. (2009, April). Mitigating drive-by download attacks: Challenges and open problems. In International Workshop on Open Problems in Network Security (pp. 52-62). Springer, Berlin, Heidelberg.

[51] Sharma, P., Johari, R., & Sarma, S. S. (2012). Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. International Journal of System Assurance Engineering and Management, 3(4), 343-351.

[52] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT—A Survey," in IEEE Access, vol. 9, pp. 16849-16865, 2021, doi: 10.1109/ACCESS.2021.3052850.

[53] Zaman, N., & Abdullah, A. B. (2012). Energy optimization through position responsiverouting protocol (prrp) in wireless sensor network. International Journal of Information and Electronics Engineering, 2(5), 748.

[54] Jayakumar, P., Brohi, S. N., & Zaman, N. (2020). Top 7 lessons learned from COVID-19 pandemic.

[55] One Login, Six type of passwords attaks and how to stop them, https://www.onelogin.com/learn/6-types-password-attacks, Accessed on November 2021

[56] S. M. Muzammal, R. K. Murugesan and N. Z. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4186-4210, 15 March15, 2021, doi: 10.1109/JIOT.2020.3031162.

[57] C. Diwaker et al., "A New Model for Predicting Component-Based Software Reliability Using Soft Computing," in IEEE Access, vol. 7, pp. 147191-147203, 2019, doi: 10.1109/ACCESS.2019.2946862.

[58] Alferidah, D. K., & Jhanjhi, N. Z. (2020, October). Cybersecurity Impact over Bigdata and IoT Growth. In 2020 International Conference on Computational Intelligence (ICCI) (pp. 103-108). IEEE

[59] A. Ullah et al., "A Survey on Continuous Object Tracking and Boundary Detection Schemes in IoT Assisted Wireless Sensor Networks," in IEEE Access, vol. 9, pp. 126324-126336, 2021, doi: 10.1109/ACCESS.2021.3110203.

[60] Humayun, M., Jhanjhi, N. Z., & Alamri, M. Z. (2020). Smart secure and energy efficient scheme for e-health applications using IoT: a review. International Journal of Computer Science and Network Security, 20(4), 55-74.

[61] M. Lim, A. Abdullah, N. Jhanjhi and M. Khurram Khan, "Situation-Aware Deep Reinforcement Learning Link Prediction Model for Evolving Criminal Networks," in IEEE Access, vol. 8, pp. 16550-16559, 2020, doi: 10.1109/ACCESS.2019.2961805.

[62] Humayun, M., & Jhanjhi, N. Z. (2019). Exploring the relationship between GSD, knowledge management, trust and collaboration. Journal of Engineering Science and Technology (JESTEC), 14(2), 820-843.

[63] M. Satheesh Kumar, S. Vimal, N.Z. Jhanjhi, Shanmuga Sundar Dhanabalan, Hesham A. Alhumyani, Blockchain based peer to peer communication in autonomous drone operation, Energy Reports, 2021, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.073.

[64] Maggi, F., Volpatto, A., Gasparini, S., Boracchi, G., & Zanero, S. (2011, December). A fast eavesdropping attack against touchscreens. In 2011 7th International Conference on Information Assurance and Security (IAS) (pp. 320-325). IEEE.

[65] Penta Security, Top 5 AI-powered Cyber Threats & How to Prevent Them, https://www.pentasecurity.com/blog/top-5-ai-powered-cyber-threats-how-to-prevent-them/, Access on November 2021

[66] Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2021). Performance enhancement in wireless body area networks with secure communication. Wireless Personal Communications, 116(1), 1-22.

[67] V. Singhal et al., "Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned Railway Level Crossings," in IEEE Access, vol. 8, pp. 113790-113806, 2020, doi: 10.1109/ACCESS.2020.3002416.

[68] Brohi, S. N., Jhanjhi, N. Z., Brohi, N. N., & Brohi, M. N. (2020). Key applications of state-of-the-art technologies to mitigate and eliminate COVID-19.

[69] N. Zaman, K. Ragab, A.B. Abdullah, Wireless Sensor Networks and Energy Efficiency: Protocols Routing and Management, IGI, Globa, Hershey, PA, USA (2012)

[70] Mamoona Humayun, NZ Jhanjhi, Ahmed Alsayat, Vasaki Ponnusamy, Internet of things and ransomware: Evolution, mitigation and prevention, Egyptian Informatics Journal, Volume 22, Issue 1, 2021, Pages 105-117, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2020.05.003.

[71] Almusaylim, Z.A., Zaman, N. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless Netw 25, 3193–3204 (2019). https://doi.org/10.1007/s11276-018-1712-5

[72] M. J. Iqbal et al., "Smart Home Automation Using Intelligent Electricity Dispatch," in IEEE Access, vol. 9, pp. 118077-118086, 2021, doi: 10.1109/ACCESS.2021.3106541.

[73] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

[74] Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and mitigation of dos and ddos attacks in iot-based stateful sdn: An experimental approach. Sensors, 20(3), 816.

[75] Pan, Y., White, J., Schmidt, D., Elhabashy, A., Sturm, L., Camelio, J., & Williams, C. (2017). Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems.

[76] Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25, 36-49.

[77] Atlam H.F., Wills G.B. (2020) IoT Security, Privacy, Safety and Ethics. In: Farsi M., Daneshkhah A., Hosseinian-Far A., Jahankhani H. (eds) Digital Twin Technologies and Smart Cities. Internet of Things (Technology, Communications and Computing). Springer, Cham. https://doi.org/10.1007/978-3-030-18732-3_8

ABDULELLAH A. ALABOUDI received the master's degree and the Ph.D. degree in computer sciences from the University of Staffordshire, U.K. He is currently working at Shaqra University, Saudi Arabia, as an Assistant Professor. He has vast experience as a Business Process Reengineer and project management. An ample number of peer-reviewed articles are in his credit. His research interests include the Internet of Things, cybersecurity, software engineering, wireless networks, and machine learning.