Journal of Namibian Studies, 33 S2(2023): 330–345 ISSN: 2197-5523 (online)

Cyber Security & IoT Vulnerabilities Threats Intruders and Attacks Research Review

Asma'a Alamareen[1], Malak Hamad Al-mashagbeh[2], Sara Abuasal[3]

[1]Computer Science Department, Zarqa University Zarqa, Jordan, aalamareen@zu.edu.jo

[2]Cyber Security Department, Zarqa University Zarqa, Jordan, malakmashagbah@gmail.com

[3]Software Engineer, Zarqa University Zarqa, Jordan, Sabuasal@zu.edu.jo

Abstract

The Internet of Things (IoT) is a system of various systems of hardware and software that is mostly dependent on online services and a variety of cutting-edge communication and sensing innovations. The introduction of 5G networks will see an increase in the global expansion of IoT, however security problems related to IoT innovation will additionally necessitate comprehensive analyses. This study will provide a comprehensive overview of the security difficulties in an Iot infrastructure, as well as current incidents of IoT technology assaults, interoperability used in IoT systems. For the inaugural study, all of the key aspects of IoT security are analysed and defined collectively. This study would be a great asset for prospective studies focusing on the creation of more secure IoT transmission methods for dealing with security and privacy in IoT.

1. Introduction

Cybersecurity is the use of information technology, rules and techniques to guard against hacking attacks on programs, networks, devices, data, and systems. Its purpose is to reduce the risk of cyberattacks and protect against the illegal use of systems, networks, and technology (Schatz et al., 2017). New guidelines and reporting systems make it tough to manage the risk of cyber security. The administration must assure the board that its cyber-risk strategies will reduce the risk of threats while also reducing the financial and operational consequences.

According to a McAfee and CSIS research focused on Vanson Bourne data, cybercrime damages the world economy more than a trillion dollars every year., ethical, social and Political motives may all inspire attackers. Cybersecurity is necessary for everyone with an Internet

connection. This is so that the majority of automated cyberattacks can take advantage of general vulnerabilities rather than those of specific websites or organizations (Lee et al., 2019).

2. Examples of cyber threats

• Malware, such as RATs (remote access Trojans), worms, botnet software, Trojans, spyware, viruses, ransomware, rootkits, and boot kits.

• Transfer of data using security holes.

• Form jacking is the process of inserting malicious code into online applications.

• crypto-hacking, or the installation of unlawful bitcoin mining equipment.

• DDoS (distributed denial-of-service) attacks try to shut down connections, platforms, and websites by flooding them with too much data.

• DNS (domain name system) attacks, where the DNS is manipulated to divert traffic to hostile webpages (Lallie et al., 2021).

3. Categories of cyber security

3.1. Technology that is essential cyber safety

Vital infrastructure firms are typically more vulnerable to assault than other businesses due to the fact that SCADA (supervisory control and data acquisition) companies rely on out-of-date technology. The NIS Regulations apply to important service providers in Britain's power, transportation, healthcare, and water industries, as well as electronic providers. The requirements compel businesses to take appropriate technical and organizational precautions to manage their potential risks (Pokkuluri and Usha, 2021).

3.2. Internet safety

Internet security involves correcting defects in your network protocols, firewalls, wireless access points, processors, network architecture, and operating systems.

3.3. Cloud safety

The emphasis in data protection is on protecting information, equipment, and applications in the cloud.

3.4. IoT (Internet of Things) security

IoT security comprises safeguarding systems and connected smart products. Connected devices are things that constantly link to the

Internet, such as heaters, smoke detectors, smart lights, and other devices.

3.5. Application safety

(Ferrag et al., 2020) say that "access control" is the process of fixing vulnerabilities caused by risky development processes when designing, putting together, and making out software or a website.

4. Increase the online defenses with these essential security precautions

4.1. User education

Personal mistakes are the most common source of information vulnerabilities. As a result, you must provide workers with the knowledge they need to mitigate risks. Employees will know how security concerns impact them and how to implement best practices via personnel awareness training. advice on practical situations.

4.2. Application security

Web application bugs are a common point of entry for hackers. It is critical to concentrate on applications since they are becoming more significant for the firm..

4.3. Network security

Establishing information security entails protecting the safety and usability of your data and network. This is accomplished via the use of a network vulnerability scanner, which searches for safety flaws and flaws in your system..

4.4. Leadership commitment

Leadership commitment is the key to cyber resiliency. It is difficult to establish or maintain effective processes without it. Top executives must be willing to invest in cyber security measures such as security awareness.

4.5. Password management

In the United Kingdom, about half of all persons use the passwords "password," "123456," or "keypad." Create a strong password strategy to aid employees in establishing and keeping secure passwords. (Ahanger et al., 2018).

IoT stands for the Internet of Things, a network of objects having distinct element identification, embedded software intelligence, sensors, and a pervasive Internet connection. IoT takes advantage of the Web's telecom network to permit goods or items to interact with

the inventor, administrator, and/or other linked devices. It enables a deeper interface of the real environment with computer-based processes, increasing economic, efficiency, and accuracy benefits. It also enables objects to be detected (to provide specific data) and manipulated directly over the Internet. Each item has an embedded system that provides a proper identifier and compatibility within the existing network. (Wan et al., 2017).

The Internet of Things (IoT) is a new method that enables the collection and transmission of information in an automated way. To define it, the term "system of mobile networks linked with sensors, programming, and controllers" is used. As a result of technical breakthroughs such as computer vision, IoT technology has grown. IoT applications are becoming increasingly visible in almost every sector. Figure 1 depicts a handful of the most extensively utilized IoT applications. Every business is moving toward connected things to keep up with the pace of the current world. Nowadays, classrooms are interconnected, and children with disabilities and auditory difficulties may learn using linked mittens and iPads thanks to technological advances. Learning is no longer limited to traditional techniques. IoT technology may also be of great use to other children with impairments. In our fast-paced lives, homes and towns are becoming smarter to address humanity's core needs, such as safety, waste disposal, air quality improvement, and enjoyment. (Hassan et al., 2020).

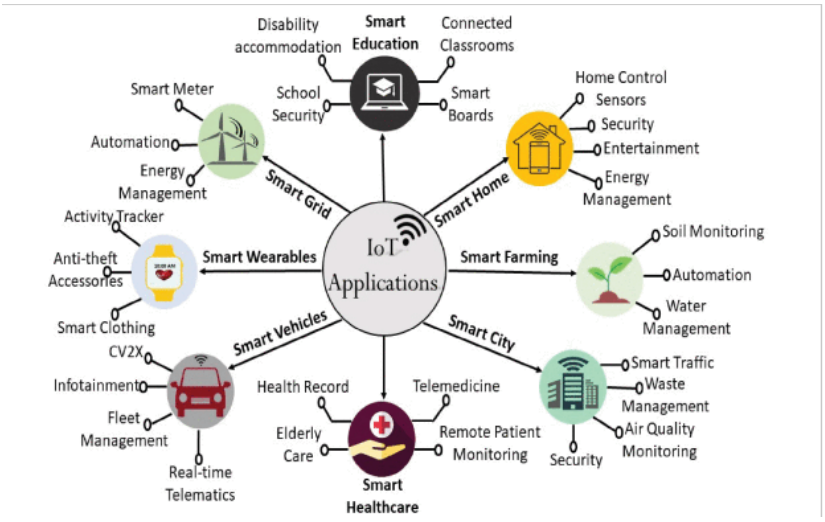

Figure 1. IoT applications.

IoT has completely changed the healthcare industry, whether it is via wearables, telemedicine, or patient monitoring from a distance. IoT in agriculture has improved soil monitoring and water management, changing the way conventional farming is done (Al-Mashhadani and Shujaa, 2022). By introducing linked automobiles, IoT has

revolutionized the field of smart vehicles. Additionally, the advent of IoT in electric grids has elevated energy management to new heights. After several developments, IoT has grown into a significant sector; Figure 2 shows the historical development of IoT. From the internet-connected refrigerator to the IoT-based smart city, the sector has advanced significantly and is now a crucial component of daily life. By establishing the Internet of Battlefields in 2017, IoT established its footprint in the military industry. The following year, it was implemented in the healthcare industry. The first Wi-Fi-capable rabbit was created in Japan in the year 2005. IoT reached a turning point in 2011 when it was included in the hype cycle for new technologies. Since then, it has appeared often, and as recently as 2017, IoT is still at the top of the hype cycle for Gartner. IoT security is now the main concern after the first significant IoT-based assault in 2016(Atitallah et al., 2020).

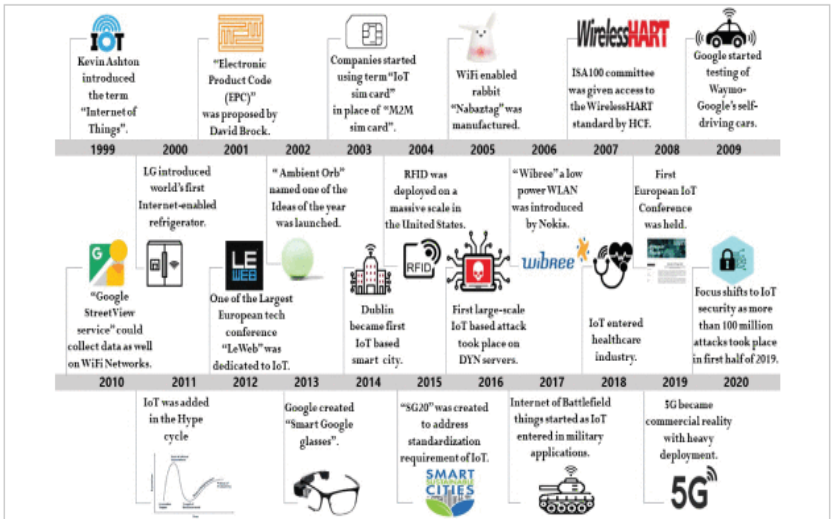

Figure 2. The historical development of IoT.

Scientific work tackling the security and privacy problems of IoT devices has made strides in recent years. Currently, most security strategies and processes proposed are based on standard network security techniques. However, establishing security mechanisms in an IoT system is more complex than in a traditional network due to the heterogeneity of the devices and protocols, in addition to the size or number of nodes in the system. There are detailed descriptions of the problems in implementing IoT security reduction due to physical connections, diversity, resource constraints, privacy, the large size, confidentiality, and a lack of security preparedness. in Hassan et al. (2019).

5. The three-layer architecture

5.1. Application layer

Between the middleware layer and the market layer is the framework layer. Consumers may access resources linked to applications via the platform layer. Numerous applications, such as those for smart homes, smart environments, smart vehicles, smart farming, smart logistics, smart transit, etc., might be included in this sheet.

5.2. Network layer

The term "transmission layer" is often used to describe the network layer. This layer gathers information from the perception layer and securely sends it to IoT devices. This layer controls a number of networking devices, including firewalls, hubs, and switches.

5.3. Perception layer

The vision layer is the first one. In essence, this layer manages the well-known items while gathering information from them. Numerous different forms of sensors are used to coordinate 2-D scanner tag markings and readers via camera, terminals, and remote sensors, including RFID labels, QR codes, and many more. This layer's main competency is thoroughly identifying the objects and gathering data (Saxena et al., 2020).

The power of IoT technology to collect information, connect, and process has completely changed how people live their lives. Protection and privacy are two major obstacles to the development of the Internet of Things. IoT assaults might be considered privacy invasions and put people's lives and privacy in peril. Another key issue with the development of the IoT has been the security and privacy of its users. IoT privacy and protection are topics of a lot of research, but the countermeasures they describe usually target a specific kind of attack. Additionally, it's critical to consider the IoT architecture as a whole and to provide comprehensive security. Each layer of the IoT architecture is covered in this paper's discussion of security vulnerabilities and privacy concerns. In accordance with numerous categorization criteria, the IoT attack is evaluated. Each layer of protection on the IoT architecture should be applied concurrently (Raghuvanshi et al., 2020).

6. Literature Review

In 2015, Ur Rehman gave his consent for the terrorist group "Islamic State of Iraq and Greater Syria" (ISIS) to create a cyberattack unit. In this Internet sector known as the "Cyber Caliphate," which has as its main objectives evil and the disclosure of sensitive information, attacks on internet resources, including banks, research institutes, public organizations, and others, are frequent. The level of danger

that electronic crimes pose to society may be used to determine the cost of reasonable and efficient remedies.

A bank or other financial institution might be adequately protected for as little as $510,000, according to experts in electronic document security in the US. However, the security system of a large financial institution, valued at least $ 15 million (excluding hardware and software expenditures) and serving up to 80,000 customers, is classified as reliable (excluding the wages of state workers' own security firm). Information security threats may take many different shapes. Cyberterrorism's primary objective is to seriously disrupt public order. Since the continued advancement of civilization depends on the faultless functioning of computer systems, this phenomenon is closely related to the growth of the information infrastructure. Actions taken with the intention of destroying them cause more severe damage and evoke a significant public reaction. This refers to targeted cyberterrorism that poses a threat to people, society, and the state by scaring the public and authorities and having real or prospective repercussions on cybernetic social, technological, and political systems. In the last ten years, there has been a lot of concern about the use of terrorists to carry out terrorist activities utilizing modern information resources, notably the Internet.

Ng et al. 2017 revealed that Controls for operational conditions, rules for the locations of first threat entrances, and controls for very well-designed dissemination strategies comprise the proposed cyberfinancial security infrastructure. Figure 3 depicts the methods that optimize and validate the risks. This framework's dissemination techniques, methodologies, and entrance point are linked to the information security defensive mechanism. By dividing the physical region used for cyberbanking from the outside physical space, the entry point designates the network's access point. Routers and firewalls are set up at the network's entry.

The management policies and network firewall define and configure the propagation mechanisms and procedures. The efficiency, verification, and operational requirements of the framework have an influence on application security. To suit operational demands, the concept of least privilege may be used. Implementing vulnerability checks may help with application optimization and validation. Controls that address operating circumstances include software and hardware procurement, secured hardware and software installations on workstations, laptops, and hosts, and continuing vulnerability evaluation and repair. Some of the tactics that address first attack entry points are cyber security defensive strategies, security testing, portable and wireless device administration, data recovery capabilities strategies, and security skill evaluation and training. Rules

for known propagation strategies may be specified in firewalls, switches, and routers. Controlling network port, service, and protocol access; controlling administrator rights; and putting border protection in place; maintaining security audit logs; monitoring and analyzing Controls that maximize and validate risks include account management and monitoring, security incident response tools, and data recovery tools.

Figure 3. Cyber banking security framework.

According to Malik et al. (2019) The Internet of Things (IoT) has brought in a new paradigm in which a network of talking and collaborating equipment and gadgets drive new process improvements in enterprises. IoT cybersecurity attacks are widespread and getting more regular, causing a slew of issues for people and businesses in terms of compliance, reputation, economics, and company operations. The unprecedented development of IoT devices in industries such as smart grids, environmental control, patient monitoring equipment, smart manufacturing, and transportation is partly to blame for the steep increase in cyberattacks. The dynamic and transitory nature of device connections, the variety of individuals capable of interacting within IoT networks, and resource constraints make IoT security management more difficult.,.

Sha, et al. (2018) endorsed that because each layer of the IoT architecture has unique security concerns and interacts with other layers, security solutions should be considered throughout the design. By performing a literature review of cybersecurity technologies through the lens of IoT architecture, we may get a systematic and thorough knowledge of IoT cybersecurity. Despite the fact that many IoT devices are meant to be small and low-power, they often collect huge amounts of environmental information in real time and use a number of energy-saving measures. Making reliable

decisions based on data is often accomplished via the use of technology such as machine learning. However, due to the devices' resource constraints, it has proven challenging to incorporate computation-intensive privacy and security measures into lightweight IoT devices.

Xu et al. (2018) reported that Many IoT devices are lightweight and low-power, gathering vast amounts of environmental data in real-time and using a range of energy-saving approaches. Making reliable decisions based on data is often accomplished via the use of technology such as machine learning. Because of the gadgets' limited capabilities and resources, integrating integer arithmetic security and privacy measures into lightweight IoT devices has proven problematic. One of the most significant security concerns at the perceptual layer is the copying of device circuits for intrusions. RFID tag clones, for example, might be used to launch distributed denial-of-service (DDoS) attacks.. Physically unclonable functions (PUFs) have been utilized to generate cryptographic keys for chips as well as for authentication and identification.

PUFs increase security by preventing device cloning, detecting and certifying devices, and resisting manipulation. Because IoT device parts are often manufactured with limited resources, lightweight PUF designs are required. PUFs cannot be duplicated, although a PUF key that has been retrieved may. As a consequence, various PUF-based authentication systems are proposed. PUFs with lightweight cryptography, for example, may be used to efficiently validate a single tag. To strengthen IoT cybersecurity, it is required to do activities manually, develop staff skills and tool sets, and raise problems with makers and other third parties. IoT cybersecurity must address security systems, data protection, and personal privacy. The acceptability of IoT devices is determined by their security level, but since these gadgets are dynamic and varied, building a product certification framework is difficult from both a legal and a technical aspect..

According to Luo et al. (2018), People's privacy must be protected when handling personally identifiable information (PII) by securing their devices and data. Building trust and promoting the uptake of IoT systems are dependent on the incorporation of privacy protection methods early in the development process. A large percentage of IoT systems are low-energy and small and light, making it challenging to ensure security and privacy. To protect patients' privacy in IoT-based healthcare systems from advanced attacks such as collusion attacks and data leakage, researchers developed a framework called Privacy Protector.

Khosravi-Farmad et al. (2020) reported the This section examines research that applies quantitative methodologies to manage cybersecurity risk. The quantitative approaches often restrict the scope of the investigation to a cyber-risk evaluation. A Bayesian decision network (BDN) was used to build a paradigm for controlling network security risk. The framework covers many critical operations that must be carefully carried out in order to increase the security level of a network, such as risk analysis, risk mitigation, risk verification, and risk monitoring. Only a few examples of the sorts of information necessary for managing security risks that BDN models include information on vulnerabilities, risk-reducing treatments, and the outcomes of putting them into effect on vulnerabilities. The risk management procedure's cost-benefit evaluation is carried out using updated Bayesian inference techniques. Their study shows that their technique significantly improves network security via accurate risk analysis and effective risk minimization. Another risk assessment approach called "AVARCIBER" extends the identical properties of ISO 27005. Beginning the risk analysis, identifying and assessing assets, detecting cybersecurity threats, estimating the level of damage for the security vulnerabilities (dimension) tuples, quantifying the risk, and adopting countermeasures are all phases in putting the technique into action. The whole technique is not unique in comparison to ISO 27005. However, more in-depth activities and useful instructions are available. A case study was used to assess the efficacy of the framework's use..

Neshenko et al. (2019) claim Enterprise Common Internet of Things applications include information sharing and collaboration, big data and business analytics, as well as management and monitoring of connected devices. The application domain influences the security management solutions that are most appropriate, and some examples of this include smart metering, home automation, smart transportation, and smart health. For instance, smart health deals with particularly sensitive data and necessitates the highest degree of protection for both privacy and security. Cyberattacks on one program may have an effect on the security of other associated applications since many Internet of Things apps are managed by third-party service providers. CoAP, MQTT, and XMPP security, incorrect security patches, insufficient authentication, and poor audit procedures are examples of the challenges that arise with regard to data safety. Access control, security systems, heterogeneous wireless identification, secret information control, and information security protection are some of the solutions that have been developed in response to the concerns about information security that have been discussed before.

Neisse et al. (2019) claim For At the processor layer, public cloud and fog nodes have both grown into ubiquitous technologies. These techniques are used to store and analyze enormous amounts of data

produced simultaneously by a number of IoT devices. The fog computing system processes data collected via the use of connected devices while accounting for delay. In cloud computing, DS may be used on a cloud node to detect invasions. In fog computing, a hybrid technique that combines intrusion detection systems (IDS) (Pillai and Hemamalini, 2022), virtualized honeypot devices (VHD), and Markov chains yields promising results in both detecting hostile devices and reducing false alarm rates. These two objectives may be achieved by combining IDS, VHD, and Markov chains.

The processing layer may employ blockchain technology to broadcast and store information in the form of a shared blockchain for each user or node in the system. Suppliers, smarter energy, and healthcare systems are among the IoT uses that stand to profit the most from blockchain technology. Blockchain technology may be used to provide IoT security certificates in order to simplify the safe and hands-free setup of Internet of Things devices.

As per Roopak et al. (2019), The secure transfer of data across networks is critical to the operation of gadgets, computing nodes, and the entire IoT network. Furthermore, the network layer is critical to the overall proper functioning of IoT security. Using a system that detects intrusions enables the detection of assaults, the deployment of preventive actions, and packet monitoring (IDS). For the objective of intrusion detection, the IDS employs a variety of approaches. These methods include statistical analysis for anomaly detection, evolutionary algorithms for intrusion classification based on error messages, behavior patterns, and attempted interferences, procedure confirmation for the classification of dubious behavioral patterns, the random forest technique for data analysis, and deep learning for network breach pattern recognition. Deep learning models identify DDoS assaults with an accuracy rate of 97.16%, ranking them the most effective alternative..

Based on Matheu et al. (2019) To improve the cybersecurity of the Internet of Things (IoT), some operations must be performed manually, staff expertise and tool sets must be expanded, and issues with producers and other third parties must be addressed. Gadget safety, information protection, and individual privacy must all be considered in order to adequately protect the Internet of Things. The accreditation of an Internet of Things device's safety level is required for the device to be regarded as appropriate; however, the dynamic and variable structure of IoT devices has made building a cybersecurity certification framework problematic from both a technical and legal standpoint.,.

Based on Esteves et al. (2017), The key emphases of the organizational component of the issue include support from senior

management for security measures, expenditures in safety, safety training, and other activities of the organization. One of the reasons these tasks are crucial for improving the performance of cybersecurity for the internet of things is that they are identified as having a beneficial influence on the attitudes and behaviors of insiders and employees, as well as outsiders and customers of IoT services. A company's capacity to respond to cyberattacks is quickly becoming a critical element of business risk management. [Cyberattacks] [Cyberattacks] To properly design and implement a security strategy, you must have the full support of high management.

Organizations must revise their cybersecurity plans as the threat environment evolves. In order to link their IoT cyber risk management with IT risk management and corporate risk management, they must build cybersecurity governance and operational plans. Four implementation tiers are suggested by the NIST Cybersecurity Framework in relation to an organization's cybersecurity capabilities. The desired degree of implementation tiering must be determined, and security plans must be developed based on the organization's current cybersecurity capabilities.

According to Loi et al. (2020) reported that When the cybersecurity techniques at this tier utilize the word "internal," they are related to the inner cyber technology systems. When it comes to discovering and implementing appropriate IoT smart solutions, the company may benefit from the assistance of IoT cybersecurity technology companies that are part of the IoT cyber ecosystem. Internal cybersecurity technology should be employed to satisfy both the company's business cybersecurity goals and the internet of things' cybersecurity aims.

Hildebrandt specifies three different types of cybersecurity technology: those that assure data confidentiality, those that identify and manage online hazards and vulnerabilities, and those that recognize and solve crimes. Identification, which includes accreditation and credential management, is intimately linked to cybersecurity technologies. Authentication also covers credential management. Common IoT security technologies include firewall rules, DDoS remediation, device verification, managerial staff, highly secure encryption techniques and text categorization, secure firmware and software, public key infrastructure (PKI), intrusion prevention and detection processes, incident management systems, and secure software and firmware.

Rea-Guaman et al. (2020) examined the risk identification step detects cyber threats, IoT assets, and security flaws. The vulnerabilities and threat categories for each IoT asset are identified (e.g., IoT device 1—vulnerability 1—threat type 1, IoT device 2—vulnerability 1—threat type 2, etc.). In order to identify IoT risks, one

must comprehend how hackers carry out cyberattacks. Intruders have two types of attitudes Exploration and exploitation have similar characteristics. Intruders often employ both cognitive and instinctual reasoning throughout the exploratory phases of their quest, and they depend heavily on experimenting. As soon as they have control over a system, they develop an exploitative attitude in order to move closer to their objectives. The CKC framework is another useful tool for risk identification.:. A lot of people use the CKC framework to detect and stop cyberattacks. When guarding against the hostile actions of the adversary, breaking the chain early is more successful. The study of the CKC framework's seven phases may be used to pinpoint specific dangers.

According to Boja et al.'s (2018) study, The Typical Vulnerabilities and Exposures (CVE) system provides a way to look up vulnerabilities and exposures that are known to the public. The Federal Cyber-Security The federally funded research and development center (FFRDC), run by MITRE Corporation, is funded by the US Department of Homeland Security's Cyber Security Division. CVEs are used by the safety content automation protocols, and these IDs can be found in both the MITRE system and the US National Security Vulnerabilities. The Federal Cyber-Security The federally funded research and development center (FFRDC), run by MITRE Corporation, is funded by the US Department of Homeland Security's Cyber Security Division. CVEs are used by the security content automation protocols, and these IDs can be found in both the MITRE system and the US National Security Vulnerabilities. All of the important information and technology problems that have been found to date are documented and stored in the CVE vulnerability database. When a new security hole is found, it is quickly written down and given a unique number in the CVE list. People who work in the cybersecurity field now use the CVE vulnerability database as a resource.

Since 1999, 112,044 different CVEs have been made public, and the number keeps going up. We looked at all of the CVEs that could be used and took the information from IoT devices that was most relevant to this location.CVEs were chosen for the time period from 2012 to 2018 because the Internet of Things (IoT) market is still fairly new and because modern information technology is always changing.

7. Conclusion

In this research, we first looked at the privacy and security risks associated with IoT networks. IoT innovation has seen a spike in latest generations due to significant expansion in rapid internet access, sensor technologies, communication devices, and improved

engineering viewpoint. This expansion has led to a variety of security and privacy concerns. In this research, we provided the relevant facts regarding the majority of these difficulties while attempting to identify underlying threads between them. We examined current assaults on IoT infrastructure to validate the ramifications of these problems. The latest results would be used to create a blueprint for creating a modern secured IoT system and limiting the hazards linked to current IoT platforms. Blockchain technologies inside IoT networks and cloud system integration might be critical in future studies efforts to improve the privacy and security of IoT systems. These topics might help the continuing investigation identify further potential for IoT technology.

Bibliography

Ahanger, T. A., & Aljumah, A. (2018). Internet of Things: A comprehensive study of security issues and defense mechanisms. IEEE Access, 7, 11020-11028.

Al-Mashhadani, M., & Shujaa, M. (2022). IoT security using AES encryption technology based ESP32 platform. Int. Arab J. Inf. Technol., 19(2), 214-223.

Boja, C., Zamfiroiu, A., Iancu, B., Georgescu, T. M., Cartas, C., & Toma, C. (2018). Avant-Garde Technology Hub for Advanced Security—Technical Study; Military Technical Academy: Bucharest. Romania.

Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. MIT Sloan Management Review, 58(3), 71.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.

Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian decision network-based security risk management framework. Journal of Network and Systems Management, 28(4), 1794-1819.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.

Lee, L. (2019). Cybercrime has evolved: it's time cyber security did too. Computer Fraud & Security, 2019(6), 8-11.

Loi, M., & Christen, M. (2020). Ethical frameworks for cybersecurity (Vol. 21, pp. 73-95). Cham, Switzerland: Springer.

Luo, E., Bhuiyan, M. Z. A., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M. (2018). Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Communications Magazine, 56(2), 163-168.

Malik, V., & Singh, S. (2019). Security risk management in IoT environment. Journal of Discrete Mathematical Sciences and Cryptography, 22(4), 697-709.

Matheu, S. N., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2019). Toward a cybersecurity certification framework for the Internet of Things. IEEE Security & Privacy, 17(3), 66-76.

Neisse, R., Hernández-Ramos, J. L., Matheu, S. N., Baldini, G., & Skarmeta, A. (2019, October). Toward a blockchain-based platform to manage cybersecurity certification of IoT devices. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 1-6). IEEE.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733.

Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. Journal of Financial Regulation and Compliance.

Pillai, N. S. R., & Hemamalini, R. R. (2022). Hybrid User Acceptance Test Procedure to Improve the Software Quality. INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY, 19(6), 956-964.

Pokkuluri, K. S., & Usha, D. N. (2021). A secure cellular automata integrated deep learning mechanism for health informatics. Int. Arab J. Inf. Technol., 18(6), 782-788.

Raghuvanshi, A., Singh, D. U. K., Panse, P., Saxena, M., & Veluri, R. K. (2020). Internet of Things: Taxonomy of Various Attacks. European Journal of Molecular & Clinical Medicine, 7(10), 3853-3864.

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. Cluster Computing, 23(3), 1827-1843.

Roopak, M., Tian, G. Y., & Chambers, J. (2019, January). Deep learning models for cyber security in IoT networks. In 2019 IEEE 9th annual computing and communication workshop and conference (CCWC) (pp. 0452-0457). IEEE.

R. Hassan, F. Qamar, M. K. Hasan, A. Hafizah, M. Aman and A. S. Ahmed, "Internet of Things and its applications: A comprehensive survey", Symmetry, vol. 12, no. 10, pp. 1674, 2020.

Saxena M. (2020). Novel framework and service model for internet of things in context of smart cities. International research journal of modernization in engineering technology & Science. 2(9), 1730-1735.

S. B. Atitallah, M. Driss, W. Boulila and H. B. Ghézala, "Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions", Comput. Sci. Rev., vol. 38, Nov. 2020.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 8.

Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future generation computer systems, 83, 326-337.

ur Rehman, T. (2021). Cybersecurity for E-Banking and E-Commerce in Pakistan: Emerging Digital Challenges and Opportunities. Handbook of Research on Advancing Cybersecurity for Digital Transformation, 163-180.

Wan, J., Gu, X., Chen, L., & Wang, J. (2017, October). Internet of things for ambient assisted living: challenges and future opportunities. In 2017 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC) (pp. 354-357). IEEE.

Xu, H., Ding, J., Li, P., Zhu, F., & Wang, R. (2018). A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors, 18(3), 760.

Anis S Mokhtar, Nurhayo Asib, A. R. R. . R. M. A. . (2022). Development of Saponin based Nano emulsion formulations from Phaleria macrocarpa to Control Aphis gossypii. Journal Of Advanced Zoology, 43(1), 43–55. Retrieved from http://jazindia.com/index.php/jaz/article/view/113

Faisal, H. T. ., Abid, M. K. ., & Abed, A. . (2022). Study Of Some Biochemical Parameters in Dose During Pregnancy in Goats. Journal Of Advanced Zoology, 43(1), 01–06. https://doi.org/10.17762/jaz.v43i1.109

Mokhtar, A. R. R. A. S. . (2022). Development Of Saponin Based Wettable Powder Formulation from Phaleria macrocarpa To Control Pomacea maculate. Journal Of Advanced Zoology, 43(1), 17–31. Retrieved from http://jazindia.com/index.php/jaz/article/view/111