World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

A review of hacking techniques in IoT systems and future trends of hacking on IoT environment

Nur A'fyfah Zaimy *, Mohamad Fadli Zolkipli and Norliza Katuk

School of Computing, Universiti Utara Malaysia, Kedah, Malaysia.

World Journal of Advanced Research and Reviews, 2023, 17(02), 723–731

Publication history: Received on 12 January 2023; revised on 21 February 2023; accepted on 23 February 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.17.2.0310

Abstract

This paper reviews Internet of Things (IoT) security and the rise in security issues due to hardware and software security flaws being exploited. Researching hacking methods in IoT environments is critical, as attacks go beyond technical safeguards. Therefore, this paper aims to provide insights into the future of IoT security and inform the development of effective prevention measures by analyzing hacking techniques and tools. The research highlights the urgency to improve IoT security and focuses on future trends in IoT hacking. It also emphasizes the necessity for robust security measures to protect IoT systems and devices from hacking.

Keywords: Internet of Things (IoT); Hacking techniques; Future trends; Security measures

1. Introduction

The Internet of Things (IoT) is a new technology that allows electronic devices and sensors to connect with one another over the Internet to make human lives easier [1]. IoT provides advanced solutions worldwide to various economic, governmental, and public or private sectors. IoT is steadily growing into a significant component of people's lives that is perceptible everywhere. IoT is a technology that brings together a variety of frameworks, intelligent devices and systems, and sensors [2].

The IoT innovation for smart home systems and appliances, including Internet-connected devices, house automation systems, and smart electricity management [3]. In addition, the Smart Health Sensing System (SHSS) is another valuable IoT achievement [4]. Small intelligent equipment and devices are incorporated into SHSS to support human health. These smart gadgets can examine and monitor various health conditions, fitness levels, calories expended in a gym, etcetera. Besides, it tracks severe medical conditions in hospitals and trauma centers. IoT has dramatically improved in this field and given such people's daily lives a positive beginning.

Furthermore, transportation is a significant component of human life. IoT has led to new developments that have improved its effectiveness, comfort, and dependability. For example, at numerous signalized junctions across metropolitan areas, intelligent sensors and drone gadgets are now in charge of managing traffic flow [5]. Additionally, new automobiles are entering the market with sensing devices already installed. These technologies may detect impending large traffic jams on a map and advise an alternative route with fewer traffic jams. IoT hence has a variety of uses in both life and technology.

However, the security of data and information in IoT is a critical concern and extremely valuable [6]. It is a crucial demanding issue to deal with as IoT has demonstrated its value and potential in facilitating humankind and industrial growth. Numerous security issues will arise as intelligent objects become more connected [2]. The Internet has become the primary source of security risks and cyberattacks. It has given hackers many ways to get in, making data and

[*] Corresponding author: Nur A'fyfah Zaimy

information less safe. The government, the commercial sector, and the average computer user worry that a criminal hacker will compromise their information or private data due to the Internet's rapid technological advancement, such as IoT technologies. These types of hackers, often known as black hat hackers, will steal the agency's data and secretly send it to the public Internet [7].

Hacking a computer refers to altering its hardware and software to serve purposes other than those intended by its creator [8]. Hackers are often used to describe people who try to break into computers. A hacker is a programmer who unauthorized accesses another person's computer system or data [7]. Nowadays, hackers are highly interested in advanced IoT technology [9] due to its increasing complexity and the valuable data it generates, making it a prime target for malicious attacks. Sadhu, Yanambaka, and Abdelgawad [10] state that many high-profile security lapses in recent years have shown the potential repercussions of these assaults on IoT technology, increasing concerns about the security of sensitive and personal data held on IoT devices.

An overview of hacking techniques utilized in IoT systems and potential future developments will be provided in this article. In addition, this study will also explain how to protect IoT systems from hacking. The research questions developed for this study's scope are listed below to ensure that the discussion stays within those confines.

RQ1: What are the common hacking techniques used in IoT systems?

RQ2: What are the future trends of hacking in IoT systems?

RQ3: What are the strategies to secure IoT systems from hacking?

2. The Techniques of Hacking in IoT

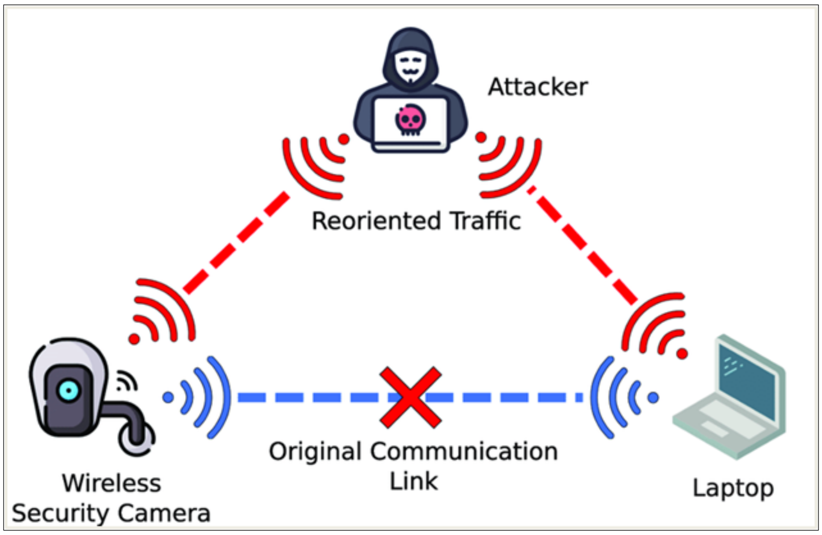
2.1. Man-in-the-Middle Attack

Before computers were invented, man-in-the-middle attacks already existed. For example, according to Cekerevac et al. [11], a hacking technique known as a man-in-the-middle (MITM) attack involves the hacker intercepting and changing traffic between two devices connected to a network. By placing the attacker's device between the target IoT device and the intended receiver, this attack can be carried out in an IoT system, giving the attacker access to the communication between these two devices and allowing them to be intercepted and modified. Figure 1 demonstrates the MITM attack [39].

The following is the framework of a man-in-the-middle attack on an IoT system:

- Initialization: The attacker selects a target IoT device and positions their attack device between the target device and the intended recipient.
- Interception: The attacker decodes and modifies the transferred data by intercepting [12] the communication between the IoT device and the recipient.
- Modification: To achieve the goals, the attacker alters the transferred data by adding malicious code or changing the communication's content.
- Redirection: The adversary redirects the message to the intended receiver, unaware that the message has been hijacked and altered [13].
- Execution: A successful MITM attack happens when the intended recipient runs the malicious code or altered material.

An IoT system might suffer major repercussions from a MITM assault, including losing private data, malware introduction, and device functionality modification [14].



Source: Adapted from [39]

Figure 1 The process of the Man-in-the-Middle (MITM) attack

2.2. Malware Attack

Malicious software, also known as malware, is a type of program or code typically distributed across a network [15]. A malware attack on an IoT system [16] is a hacking technique in which an adversary infects an IoT device with malicious software, giving them access to the device and enabling them to steal sensitive data or exploit it for malevolent reasons. Numerous malware, including spyware, could contaminate the IoT device's security settings. But ransomware is the most common and common type of malware assault on IoT systems [15]. As cited in Humayun et al. [17], a hacking tactic known as ransomware involves infecting an IoT device with malware that encrypts the device's data and requests money in exchange for the decryption key. Once fraudsters start to infect IoT devices with harmful software, a perfect cyber security arms race storm will be produced. The life cycle of ransomware begins when malicious code is inserted and spread throughout the IoT system; it continues until the victim is presented with a bill for the ransom. Several activities are carried out during this lifespan to successfully hijack the valuable files and resources of the IoT user.

2.3. Distributed Denial of Services (DDoS)

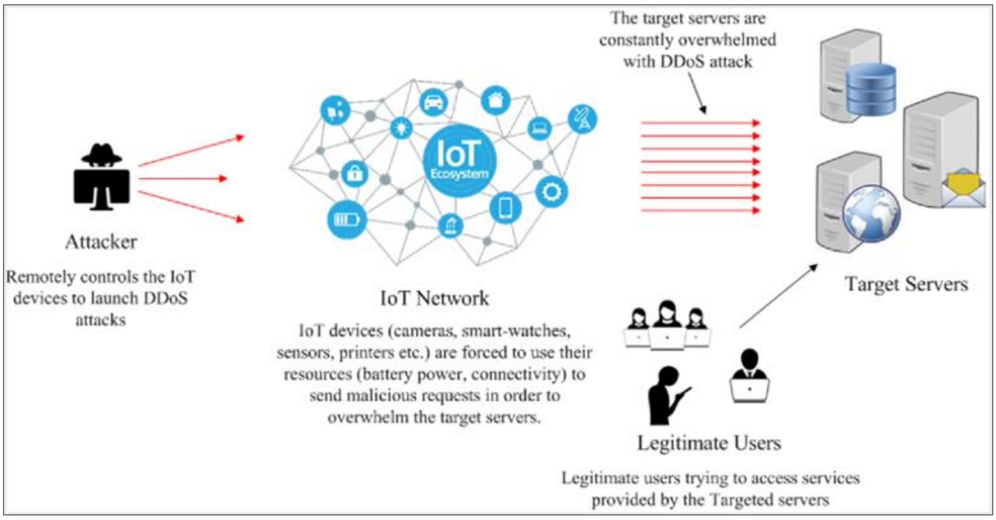
In a distributed denial of service (DDoS) attack, a target system is bombarded with excessive traffic volume, making it unreachable to authorized parties and frequently infiltrated by malware on numerous devices [18]. DDoS assaults can seriously threaten IoT systems and devices [19] because of the high number of connected devices and their frequently lacking security mechanisms, which render them open to attack. It is a hostile activity that obstructs network, server, or device workflow. The primary objectives are to destroy the infrastructure and block the data flood. The vulnerability of IoT systems and devices allowed for the successful execution of this assault. DDoS attacks achieve their objectives by obstructing required destination access during the regular workflow. Figure 2 illustrates the DDoS attack [40].

The following are the steps of a DDoS attack on IoT systems and devices [19]:

i. To execute a DDoS assault, the attacker must seize control of the network and the IoT devices that assist it. The hacker is assisted in taking control by the malware program (such as zombies or bots).

ii. The hacker remotely controls each bot before directing it to the target source's IP address. As a result, the target port or server overflows due to the hacker sending the equipped robots hundreds of commands.

iii. Lastly, the service was shut down.


The target servers are constantly overwhelmed with DDoS attack
Attacker
Remotely controls the IoT devices to launch DDoS attacks
IoT Ecosystem
IoT Network
IoT devices (cameras, smart-watches, sensors, printers etc.) are forced to use their resources (battery power, connectivity) to send malicious requests in order to overwhelm the target servers.
Target Servers
Legitimate Users
Legitimate users trying to access services provided by the Targeted servers

Source: Adapted from [40]

Figure 2 The process of Distributed Denial of Services (DDoS)

2.4. Eavesdropping Attack

A hacking technique known as an eavesdropping attack [20], often referred to as a spying or wiretapping attack, involves the attacker intercepting and monitoring communication between two parties without their consent or awareness. Due to the vast number of connected devices and their frequently lacking security features, eavesdropping attacks can seriously threaten the privacy and security of IoT devices and systems [21]. The most common form of eavesdropping is via wireless communication.

Intercepting communication between a smart home [22], such as a thermostat and a user's smartphone application, illustrates an eavesdropping assault against the IoT. In this case, an intruder may intercept the communication between the thermostat and the mobile application and acquire private data, like the user's home address and preferred temperature levels. The attacker could subsequently use this information for illicit activities like identity theft or financial fraud.

Another situation is an attacker eavesdrops on conversations between a wearable fitness device and the software that goes along with it. In this situation, the attacker might obtain private information about the user's exercise routines and habits, thereby endangering their security and privacy.

2.5. Physical Attack

Any hacking method that includes physically accessing and compromising an IoT device or system is known as a physical assault. Andrea, Chrysostomou and Hadjichristofi [23] state that these assaults target the hardware elements of the IoT system. To be successful, the attacker must be physically present near or inside the IoT system. Aside from that, this category also includes attacks that compromise the hardware's operation or lifespan.

An instance of a physical attack on the IoT is when an attacker gets access to an IoT-connected security camera [24] in the organization and tampers with it to gain unauthorized access to the network to which it is connected. In this scenario, the attacker could physically gain access to the surveillance camera by stealing or entering it during a repair or maintenance visit and installing malware or changing its configuration to compromise its security.

Another scenario is when a hacker accesses a smart home system and tampers with the linked devices, like smart locks or security cameras, to obtain illegal access to the network and steal confidential data.

3. Future Trend of Hacking in IoT

3.1. Targeting Internet of Medical Things

In recent years, cyber threats have increased in the healthcare sector. Medical professionals now frequently discuss the importance of safeguarding patients' electronic health records from potential threats. The Internet of Medical Things (IoMT), a sector currently seeing significant growth, is likewise not excluded from the possibility of hacking [25]. A rising number of healthcare devices are becoming hacker-prone, endangering individual users and entire networks. Among the hacking trends that are anticipated to target the IoMT are ransomware attacks [26], insider threats [25], social engineering attacks [27] and physical and network attacks [28].

In addition, there are several reasons why The IoMT could be hacked [25], including:

- Increased network connectivity: The IoMT contains many connected systems and devices, which expands the attack surface for hackers.
- Sensitive data: Medical devices and systems frequently gather and retain valuable information on a person's health, which is highly useful to cybercriminals trying to steal it for personal benefit or to use it for ransom.
- Lack of security measures: Since many medical devices were not created with cybersecurity, IoT systems may be missing essential security features like encryption, robust authentication methods, and software upgrades.

In conclusion, the future trend of hacking in the IoMT is anticipated to be influenced by the growth in the value of medical data, the proliferation of connected medical devices, and emerging hacking techniques.

3.2. Attacking Smart Homes and Cities

The idea of a "smart city" is made a reality by integrating cutting-edge computing and sensing technology with diverse processes, services, and infrastructure. The essential factors in the significant development of smart city infrastructure are the IoT and Cyber-Physical Systems (CPS) [29]. By gathering and analyzing the IoT sensors' data [30], cities can enhance their real-time operations and better serve their residents. However, the implementation of IoT has also broadened the potential attack surface for online crimes like hacking [29]. As a result, smart city infrastructure stands the risk of being targeted by crooks looking to compromise with daily city activity. Frick, Abreu and Malkin [31] found that smaller components of smart city infrastructure, such as traffic lights and CCTV systems, were more prone to assault than more significant infrastructure, like intelligent waste and water management systems. Hackers may acquire access and perhaps compromise a more critical component of the city infrastructure if there are vulnerabilities at any point in a network.

For instance, if a hacker can access an intelligent traffic management system, they may be able to shut it down and cause gridlock in the city's traffic. As a result, people would be unable to move around, causing widespread disruption that could endanger public safety. In summary, growing connectivity, sensitive data, a lack of security precautions, intricate networks, and reliance on technology make smart cities and residences a possible target for hacking in the future [32].

3.3. Advanced Persistent Threats

Based on the most recent study by Al-Matarneh [33], advanced persistent threat (APT) is a group of long-term, covert, and prolonged threats that target, invade, and exploit organizations, businesses, or states. The goal is to obtain valuable proprietary data for industrial espionage purposes or to engage in political activism. It also can result in losses of over USD$500 billion annually [33]. APT is a kind of hacking technique that has been widely utilized and abused over the past several years and will continue to become more common in future hacking [34]. APT has been used to characterize a wide range of activities, including various cybercrime campaigns, hacking methodologies, or even specific malware pieces, as well as attacks on well-known companies or nation-states.

APTs are becoming prominent because they are very good at getting past conventional security measures and avoiding detection for extended periods. APT frequently uses malware, social engineering, and other techniques [34] to get into an IoT target's systems and avoid detection. APT damage could account for 60–65% of downtime, network interruption, and financial losses. In conclusion, APT pose a substantial threat to enterprises and are a key trend in hacking's future since they can result in severe losses and harm if not swiftly identified and remedied.

4. Strategies to Secure IoT from Hacking

It is crucial to utilize prevention methods against assaults to address the issue of cyberattacks in the IoT. The IoT security threat is complicated and calls for a multifaceted strategy. The following approaches can be used by businesses to protect IoT systems and devices:

4.1. Use of Blockchain Technology

Various characteristics of blockchain technology make it an excellent choice for securing IoT devices [35]. The most significant one is its capacity to safely store vast volumes of data using cryptographic hash algorithms. Blockchain networks are also decentralized and anonymous, which makes them hard to hack. It guarantees that every node in a blockchain network can carry out any action without disclosing its identity to other nodes. Furthermore, unlike distributed ledgers offered by Google File System (GFS) or MongoDB, records kept in a blockchain network are immutable once it was added and cannot be changed or removed. Since blockchain is a shared, append-only ledger that includes cryptographic hashes, it is the best way to keep data secure and private. Also, existing cryptographic protocols are easy to use in a blockchain setting, which makes them more ideal for IoT networks than public key cryptography solutions (for example, transport layer security).

4.2. Change Passwords Regularly and Making Them Strong

Frequently switching and updating passwords for various online and electronic accounts is now the standard [36]. As advanced as the IoT has been, it should already be the norm. It is crucial to ensure that each other IoT device has its password, that passwords are updated at least many times per year, and that special codes that are challenging to decipher are used. Overreliance on password managers will increase the likelihood that any or all credentials may be compromised. Instead of depending on password managers, users should employ a more conventional approach to write down and store their passwords securely.

4.3. Software Update and Patch Management

Smart or IoT gadgets are becoming increasingly popular, including smart TVs, speakers, cameras, and medical equipment. However, they are also a fertile ground for security and privacy risks exploiting weak software components, putting users and other hosts on the network in danger. IoT systems and devices must therefore undergo routine patching and software updating to resolve vulnerabilities [37] and stop hackers from abusing them. Organizations should also have a solid patch management procedure to guarantee that updates are applied on time.

4.4. Strong Authentication and Access Control

A safe, reliable system must start with proper authentication. Every IoT device needs to be verified by industry-standard protocols like RADIUS, OTP/CHAP, or 802.1x (EAP)[35]. Furthermore, ensuring that all communications are private and can only be decoded by authorized entities is a must. Also, the devices must either employ a specific security protocol over transport layer security to communicate with their associated gateway or their traffic must be appropriately encrypted within its protocol stack. Additionally, these IoT devices should never transfer sensitive data in clear text when communicating with their associated gateway or other devices to guard against hacker snooping attacks that could use the data gathered for illegal purposes like system takeover.

4.5. Threat Intelligence and Monitoring

Previous IoT security mechanisms are inadequate for dealing with present security problems due to the rapid rise of numerous attacks and threats. Security for the next generation of the IoT must be continuously enhanced and modernized, and it can only be accomplished with the help of artificial intelligence (AI) technologies [38], particularly machine and deep learning solutions. Based on machine learning (ML) and deep learning technologies, IoT security intelligence effectively defends IoT devices against various cyberattacks by deriving insights from raw data. The most frequent IoT threats include, for instance, DoS attacks, malicious assaults, spoofing attacks, jamming, eavesdropping, data tampering, man-in-the-middle attacks, etcetera. Thus, the existing machine learning can undertake threat and risk prediction, malware analysis, and anomaly or intrusion detection and prevention, which could help minimize threats to IoT security. To sum up, the next-generation IoT system urgently needs to be protected by an intelligent security system built on cutting-edge technologies that can handle these security challenges, like machine and deep learning.

In conclusion, protecting IoT devices from hacking demands a thorough strategy considering technical, organizational, and cultural security issues. Implementing blockchain technology, routinely changing passwords, managing software updates and patches, enforcing strong authentication and access controls, and using threat intelligence and monitoring can all help to minimize risk and guarantee the security of IoT systems and devices.

5. Conclusion

In conclusion, the rise of IoT systems has made organizations need to stay vigilant against hacking threats. A comprehensive understanding of the common hacking techniques used in IoT systems and the future trends in IoT systems is crucial to secure IoT systems from hacking. This review also highlights the need for organizations to adopt strong security measures, such as blockchain technology, routine password changes for IoT devices and systems, software updates and patch management, strong authentication and access control, and threat intelligence and monitoring, to secure the IoT systems from hacking.

As IoT systems evolve and widely used, organizations must stay informed and implement robust security measures to protect against hacking threats. The increasing reliance on IoT systems in various industries, including critical infrastructure, makes it imperative for organizations to adopt a proactive and comprehensive approach to securing IoT systems from hacking. By doing so, organizations can ensure their sensitive information and systems' confidentiality, integrity, and availability.

Compliance with ethical standards

Acknowledgements

The authors thank all School of Computing members who invented this study. This study was conducted for the Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia.

Disclosure of conflict of interest

A group study that all authors contributed to. No conflict of interest.

References

[1] Kumar S, Tiwari P, Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. Internet of Things is a revolutionary approach for future technology enhancement: a review. 2019; 6(1): 1-21.

[2] Sfar AR, Chtourou Z, Challal Y, "A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges," in *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*, 2017, pp. 101-105.

[3] Zhou J, Cao Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: Challenges. Security and privacy for cloud-based IoT: Challenges. 2017; 55(1): 26-33.

[4] Mishra A, McDonnell W, Wang J, Rodriguez D, Li C. Intermodulation-based nonlinear smart health sensing of human vital signs and location. Intermodulation-based nonlinear smart health sensing of human vital signs and location. 2019; 7(158284-158295.

[5] Behrendt F. Cycling The Smart and Sustainable City: Analyzing EC policy documents on Internet of Things, Mobility and Transport, and Smart Cities. Cycling The Smart and Sustainable City: Analyzing EC policy documents on Internet of things, mobility and transport, and smart cities. 2019; 11(3): 763.

[6] Minoli D, Sohraby K, Kouns J, "IoT security (IoTSec) considerations, requirements, and architectures," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2017, pp. 1006-1007.

[7] Kumar S,Agarwal D. Hacking attacks, methods, techniques and their protection measures. Hacking attacks, methods, techniques and their protection measures. 2018; 4(4): 2253-2257.

[8] Jordan T. A genealogy of hacking. A genealogy of hacking. 2017; 23(5): 528-544.

[9] Khera M. Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. 2017; 11(2): 207-212.

[10] Sadhu PK, Yanambaka VP, Abdelgawad A. Internet of Things: Security and Solutions Survey. Internet of Things: Security and Solutions Survey. 2022; 22(19): 7433.

[11] Cekerevac Z, Dvorak Z, Prigoda L, Cekerevac P. Internet of things and the man-in-the-middle attacks–security and economic risks. Internet of things and the man-in-the-middle attacks–security and economic risks. 2017; 5(2): 15-25.

[12] Mallik A. Man-in-the-middle-attack: Understanding in simple words. Man-in-the-middle-attack: Understanding in simple words. 2019; 2(2): 109-134.

[13] Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. A survey of man in the middle attacks. 2016; 18(3): 2027-2051.

[14] Javeed D, MohammedBadamasi U, Ndubuisi CO, Soomro F, Asif M. Man in the middle attacks: Analysis, motivation and prevention. Man in the middle attacks: Analysis, motivation and prevention. 2020; 8(7): 52-58.

[15] Podder P, Mondal M, Bharati S, Paul PK. Review on the security threats of Internet of things. Review on the security threats of Internet of things. 2021;

[16] Ngo Q-D, Nguyen H-T, Le V-H, Nguyen D-H. A survey of IoT malware and detection methods based on static features. A survey of IoT malware and detection methods based on static features. 2020; 6(4): 280-286.

[17] Humayun M, Jhanjhi N, Alsayat A, Ponnusamy V. Internet of things and ransomware: Evolution, mitigation and prevention. Internet of things and ransomware: Evolution, mitigation and prevention. 2021; 22(1): 105-117.

[18] Mirkovic J,Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. A taxonomy of DDoS attack and DDoS defense mechanisms. 2004; 34(2): 39-53.

[19] Munshi A, Alqarni NA, Almalki NA, "Ddos attack on IoT devices," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020, pp. 1-5.

[20] Wang Q. Defending wireless communication against eavesdropping attacks using secret spreading codes and artificial interference. Defending wireless communication against eavesdropping attacks using secret spreading codes and artificial interference. 2021; 103(102175.

[21] Li X, Wang H, Dai H-N, Wang Y, Zhao Q. An analytical study on eavesdropping attacks in wireless nets of things. An analytical study on eavesdropping attacks in wireless nets of things. 2016; 2016(

[22] Davis BD, Mason JC, Anwar M. Vulnerability studies and security postures of IoT devices: A smart home case study. Vulnerability studies and security postures of IoT devices: A smart home case study. 2020; 7(10): 10102-10110.

[23] Andrea I, Chrysostomou C, Hadjichristofi G, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*, 2015, pp. 180-187.

[24] Costin A, "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," in *Proceedings of the 6th international workshop on trustworthy embedded devices*, 2016, pp. 45-54.

[25] Perwej Y, Akhtar N, Kulshrestha N, Mishra P. A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends. A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends. 2022; 9(1): d346-d371.

[26] Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. 2021; 166(110-124.

[27] Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J*, et al.* A survey on security threats and countermeasures in Internet of medical things (IoMT). A survey on security threats and countermeasures in Internet of medical things (IoMT). 2022; 33(6): e4049.

[28] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IoMT) systems security. Recent advances in the internet-of-medical-things (IoMT) systems security. 2020; 8(11): 8707-8718.

[29] Rani S, Kataria A, Chauhan M, Rattan P, Kumar R, Sivaraman AK. Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: state-of-art work. Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: state-of-art work. 2022; 62(4671-4676.

[30] Sharma R,Arya R. Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. 2022; e4571.

[31] Frick KT, Abreu G, Malkin N, "The cybersecurity risks of smart city technologies: What do the experts think?," in *white paper, CLTC White Paper Series*, ed: UC Berkeley, 2021.

[32] Ma C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. Smart city and cyber-security; technologies used, leading challenges and future recommendations. 2021; 7(7999-8012.

[33] Al-Matarneh FM. Advanced Persistent Threats and Its Role in Network Security Vulnerabilities. Advanced Persistent Threats and Its Role in Network Security Vulnerabilities. 2020; 11(1): 11-20.

[34] Hudson B. Advanced persistent threats: Detection, protection and prevention. Advanced persistent threats: Detection, protection and prevention. 2014;

[35] Shafiq M, Gu Z, Cheikhrouhou O, Alhakami W, Hamam H. The rise of "Internet of Things": review and open research issues related to detection and prevention of IoT-based security attacks. The rise of "Internet of Things": review and open research issues related to detection and prevention of IoT-based security attacks. 2022; 2022(1-12).

[36] Surya L. Security challenges and strategies for the IoT in cloud computing. Security challenges and strategies for the IoT in cloud computing. 2016; 2394-3696.

[37] Prakash V, Xie S, Huang DY. Software Update Practices on Smart Home IoT Devices. Software Update Practices on Smart Home IoT Devices. 2022;

[38] Sarker IH, Khan AI, Abushark YB, Alsolami F. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. 2022; 1-17.

[39] Staddon E, Loscri V, Mitton N. Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. Applied Sciences. 2021, 11(6): 1-39.

[40] Shah Z, Ullah I, Li H, Levula A. Blockchain Based Solutions to Mitigate Distributed Denial of Services (DDoS) Attacks in Internet of Things (IoT): A Survey. Sensors. 2022, 22(3): 1-26.