Fuzzy Systems and Soft Computing
ISSN : 1819-4362

SAFEGUARDING TOMORROW: A COMPREHENSIVE REVIEW OF INTERNET OF THINGS SECURITY MEASURES

M.Narmatha, Research Scholar, Sri Krishna Adithya College of Arts and Science, Coimbatore.
Dr. M. Lalithambigai, Associate Professor, Department of Computer Science, Sri Krishna Adithya College of Arts and Science, Coimbatore.

Abstract:
This review explores the critical security aspects of the Internet of Things (IoT), emphasizing the necessity of continuous security monitoring and the establishment of robust incident response plans. Throughout the exploration, a comprehensive and layered approach to IoT security is underscored, acknowledging the interconnectedness of devices and the dynamic nature of the threat landscape. The review delves into various security components, including device and communication security, network and cloud considerations, and physical security. It addresses vulnerabilities, such as default passwords, lack of device authentication, and inadequate encryption, while proposing cryptographic, intrusion detection, and machine learning-based solutions. The paper also discusses security requirements, common attacks, and challenges, emphasizing the need for collaboration, education, and adherence to industry standards in securing the IoT ecosystem.

Keywords: Internet of Things (IoT), Security, Security Requirements, Attacks, Solutions

1. The introduction

The Internet of Things (IoT) has emerged as a transformative paradigm, connecting billions of devices and enabling seamless communication across diverse applications. This review explores the critical security aspects associated with the proliferation of IoT, acknowledging its potential while recognizing the multifaceted challenges it poses. Delving into the layers of the IoT ecosystem, from device and communication security to network and cloud considerations, the review provides an insightful examination of the measures required to safeguard against unauthorized access, data breaches, and privacy infringements[1][2]. The exploration begins with an in-depth analysis of device security, emphasizing the significance of robust authentication mechanisms and secure boot processes. Communication security is then dissected, highlighting the pivotal role of encryption and integrity checks in protecting data as it traverses through interconnected devices and networks.[3] Network security principles, encompassing firewalls, intrusion detection systems, and network segmentation, are scrutinized as indispensable elements in fortifying the overall IoT architecture[1][4].

Cloud security considerations follow, focusing on the secure implementation of Application Programming Interfaces (APIs) and the encryption of data stored in cloud repositories. The review underscores the paramount importance of privacy in IoT, emphasizing data minimization strategies, user consent, and compliance with regional regulations as integral components of a comprehensive security framework [5]. Physical security is examined in terms of tamper resistance and secure boot mechanisms, recognizing the need for safeguarding IoT devices from unauthorized physical access and manipulation. Regulatory compliance with industry standards is emphasized as a crucial aspect of ensuring legal and ethical use of IoT technologies [6].

The remainder of the paper is organized as follows: Section 2 delves into the security issues and challenges of IoT, Section 3 explores the vulnerabilities in IoT security, Section 4 examines the security requirements, Section 5 discusses the attacks on IoT, Section 6 addresses the security solutions for IoT, and the final section concludes the paper.

2. Security Issues and Challenges in the Internet of Things (IoT) Environment

The IoT environment poses an array of security issues and challenges due to the interconnected nature of devices, networks, and data. The absence of standardized security protocols and practices within the IoT industry complicates the assurance of consistent security across all devices and platforms. Many IoT devices employ weak or default credentials, rendering them vulnerable to unauthorized access. Inadequate authorization mechanisms can result in unauthorized operations, while the transmission of data between IoT devices and the cloud, or between devices, may lack sufficient encryption, exposing it to eavesdropping and interception. Furthermore, IoT devices frequently collect and transmit substantial amounts of personal data, giving rise to privacy concerns. Unauthorized access to this data may lead to privacy breaches[7-9] Security is not always prioritized in the development of IoT device firmware and software by manufacturers, leaving vulnerabilities that can be exploited by attackers. Deployed in uncontrolled environments with potential physical accessibility to attackers, IoT devices may face tampering or theft without adequate physical security measures [10].

Compromised or counterfeit devices can emerge at various points in the supply chain, from manufacturing to distribution. IoT devices can be co-opted into botnets, unleashing distributed denial of service (DDoS) attacks on other systems or networks. The lack of compatibility between devices from different manufacturers adds complexity to implementing comprehensive security measures across a diverse IoT ecosystem [11]. IoT devices often lack mechanisms for receiving and installing security patches and updates, leaving vulnerabilities unaddressed even when patches are available. Attackers may initiate denial of service (DoS) attacks on IoT devices or their associated networks, disrupting their normal operation. The escalating number of IoT devices amplifies the complexity of managing security at scale, potentially resulting in oversights and vulnerabilities. The interconnected nature of IoT introduces multiple attack surfaces, including devices, networks, cloud services, and user interfaces. Attackers can exploit these surfaces, moving laterally across different domains of the IoT ecosystem to compromise devices and data at multiple levels. Compliance with various regional, industry-specific, and data protection regulations adds complexity to security efforts in IoT deployments [12].

Social engineering tactics may be employed by attackers to manipulate users into revealing sensitive information or taking actions compromising security. The evolving threat landscape continuously introduces new attack vectors and techniques, necessitating adaptive security measures. Addressing these security issues in the IoT environment requires a comprehensive and multi-layered security strategy, encompassing strong authentication, encryption, intrusion detection, and regular security audits. Collaboration among IoT stakeholders, industry standards development, and ongoing security education are crucial elements in mitigating these challenges [13].

3. Vulnerabilities in Internet of Things Security

The IoT environment presents various vulnerabilities and loopholes due to its open, shared, and wireless nature, lack of human supervision, resource constraints of participating devices, and the complex interoperability of IoT devices and ecosystems. The section below discusses some of the vulnerabilities in the IoT ecosystem [6, 9, 14-17]. The following figure 1 represents the vulnerabilities in IoT.

Default and Weak Passwords:

Default usernames and passwords on most IoT devices make it easy for attackers to guess and exploit credentials, gaining unauthorized access. Despite the importance of changing passwords regularly, users often neglect this, providing attackers with an opportunity. Additionally, easily guessable passwords give attackers an added advantage.

Lack of Device Authentication:

Authentication ensures the identity of participating devices. The absence of proper authentication allows unauthorized devices to join and leave the network at will, impersonating legitimate devices. This compromises the overall security of the IoT environment, allowing unauthorized participation in network activities.

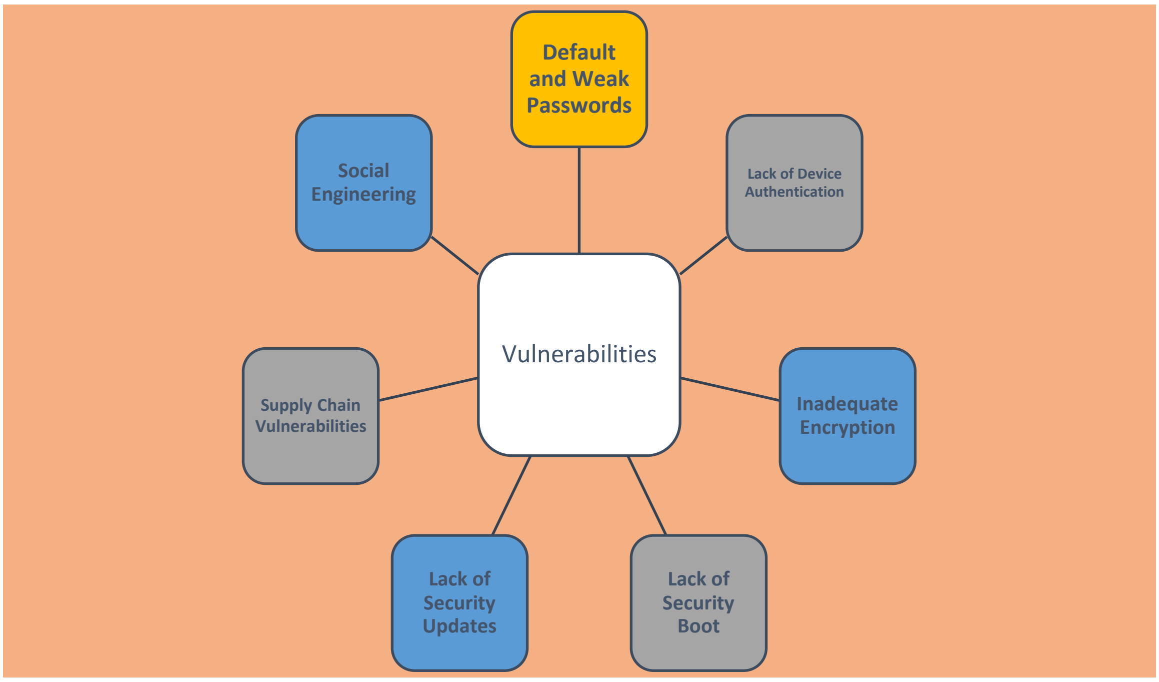

Figure 1. Vulnerabilities in IoT

Inadequate Encryption:

Proper security mechanisms should encrypt data during transfer, but many data transfers between servers and IoT devices lack proper encryption. This issue allows attackers to intercept and eavesdrop on data, compromising the confidentiality of the information.

Lack of Security Boot and Firmware/Software Vulnerabilities:

In the IoT environment, securing devices during booting is crucial. Unfortunately, this often goes overlooked, leading to the possibility of unauthorized or tampered software or firmware running on IoT devices. Neglecting security in software and firmware development introduces vulnerabilities that can be exploited, knowingly or unknowingly.

Weak Configured Network Security and Physical Security Issues:

Proper network configuration during IoT installation is essential, including intrusion detection and prevention systems, network segmentation, and firewall protection. Inadequate network security opens the door to various security violations. Moreover, many IoT devices are deployed in unattended environments with poor physical security, increasing the risk of theft, damage, or tampering.

Supply Chain Vulnerabilities:

As IoT devices move from manufacturers to distributors, there is a risk of tampering and counterfeiting. Handling IoT products with care during transportation is essential to avoid these issues.

Denial of Service Attacks and Privacy Concerns:

Denial of service attacks, disrupting IoT communication and functionalities, is a significant concern. The IoT ecosystem deals with sensitive data transmitted over unsecured environments, leading to potential unauthorized access and privacy breaches.

Lack of Security Updates:

Regular security updates are crucial for all network environments, including IoT. The absence of security patches and updates can result in unaddressed vulnerabilities, leading to security violations.

Interoperability Challenges:

Manufacturers often neglect compatibility issues, focusing on productivity. This lack of consideration creates inconsistent security mechanisms across IoT devices, providing attackers with opportunities to infiltrate the IoT environment.

Regularity and Compliance Challenges:

The IoT deployment environment may not comply with industry-specific and data protection regulations, adding complexity to IoT security concerns.

Social Engineering and Phishing:

Attackers use social engineering concepts to break security mechanisms and manipulate user data, revealing sensitive information.

To address these vulnerabilities, the IoT environment should implement strong authentication mechanisms, conduct regular security audits, adopt a multi-layered security architecture, and incorporate intrusion detection systems. Collaboration with education sectors, industry standard development, and IoT stakeholders is crucial to jointly eliminate security vulnerabilities [16][17].

4. Security Requirements of IoT Environment

Security requirements constitute essential elements in any network-based environment. Researchers emphasize that the success of network-related applications relies on effective security measures. The security of the IoT environment is a primary concern due to the interconnection of numerous IoT devices providing seamless network services to users. Consequently, all IoT-related applications must meet security requirements, which are multifaceted, encompassing organizational, operational, and technical aspects. The following section discusses some major security requirements [18-25]. The following figure 2 depicts the security requirements of IoT.

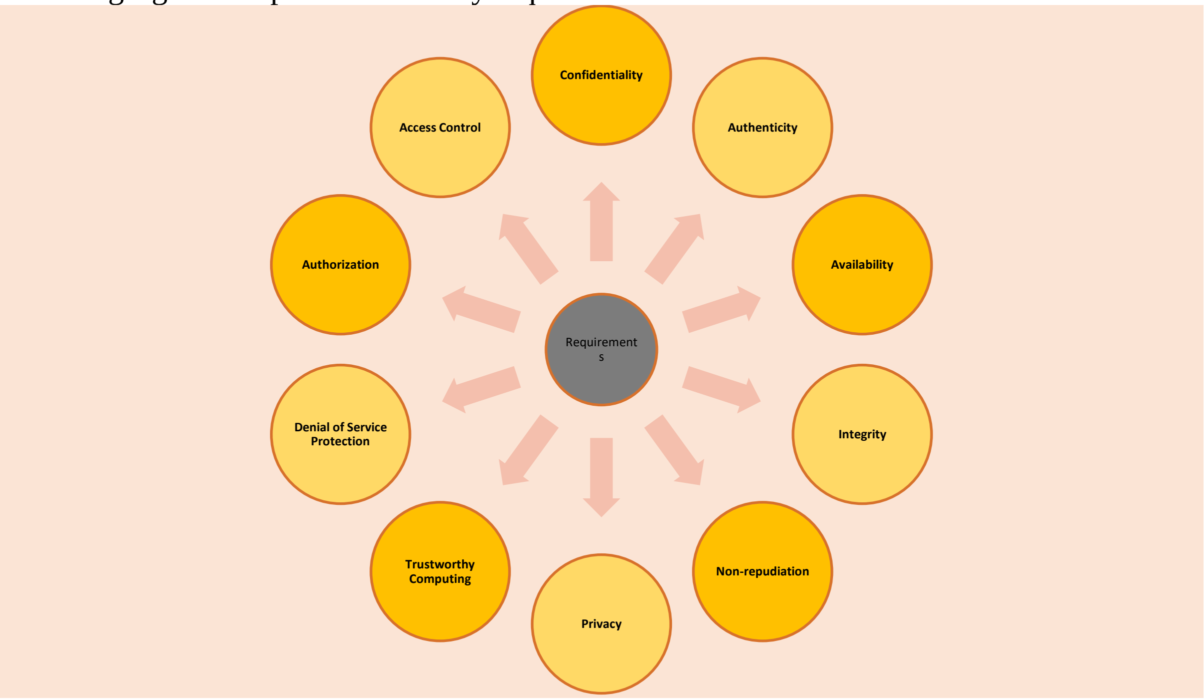

Figure 2. Security requirements

Confidentiality:

In the IoT ecosystem, certain sensitive information requires confidentiality to protect data from unwanted access. This applies to both storage and transmission. For example, cryptographic keys and access credentials, including usernames and passwords, must be kept confidential. Confidentiality is crucial in wireless communication within the IoT, especially when dealing with sensitive data like healthcare information, surveillance images, and business data.

Integrity:

Considered one of the most critical security requirements, integrity safeguards against unlawful modification of data. Core IoT applications in healthcare, industry automation control, and transportation demand integrity. For instance, data collected by sensors from the external environment should not be modified to prevent unexpected flaws in the IoT ecosystem.

Availability:

Ensures data availability at all times, even during network crashes in the IoT environment. Timely availability is also crucial. Unavailability of data in applications such as home and office automation, retail, and surveillance can lead to financial damage.

Authenticity:

Ensures the identity of participating devices in the IoT environment, verifying transmitted data at the receiving end. This requirement is essential for confirming that data is transmitted by trusted resources over the network, preventing the injection of fake data and the introduction of illegitimate devices.

Non-repudiation:

Similar to authentication, but here, the sender of the data must prove its identity to third parties. This is important where multiple parties are involved, especially in transport and healthcare applications.

Access Control:

Ensures that access to IoT devices is restricted and not freely available. For example, restricting access to one's home automation system from unknown individuals. Access to surveillance cameras, process control systems, and industrial automation should be restricted from unauthorized access.

Authorization:

Enables users to access specific resources or services. For example, certain services in publicly available applications like transport and healthcare are restricted. In healthcare applications, customers may be restricted from viewing patients' personal information while being allowed to see the types of treatments provided.

Denial of Service Protection:

Protects against denial-of-service attacks where an attacker floods the network with unwanted service requests, overloading communication or servers. This requirement safeguards the IoT environment from corruption or modified services caused by such attacks.

Trustworthy Computing:

A fundamental requirement ensuring that systems or devices in the IoT environment operate as per user expectations in all situations. Authorization and access control depend on this requirement, and its satisfaction is necessary for achieving those requirements. This ensures the healthy state of the system or devices in the IoT environment.

Privacy:

Pertinent to applications handling sensitive or private data, this requirement safeguards users' personal information. For instance, in home automation, it protects users' living habits, and in transport applications, it secures users' location information. Similarly, in retail applications, it protects user preferences during product purchases. In these situations, privacy plays a vital role in safeguarding information from unauthorized access or views.

5. Attacks on the IoT Environment

The Internet of Things (IoT) environment comprises multiple layers, from the device layer to the application layer, and attacks can target each of these layers. Below are common attacks that can impact various layers of the IoT environment [18,25-30]

Physical Tampering:

This attack primarily focuses on the hardware components of IoT devices. Attackers tamper with the physical components of IoT devices, taking advantage of their deployment in unattended environments with low physical protection. For instance, an attacker may open an IoT device, altering its hardware components and connections.

Eavesdropping:

As much of IoT communication occurs wirelessly, attackers seize the opportunity to intercept communication among IoT devices without proper permission, leading to unauthorized interception. For example, attackers may tap communication channels to capture transmitted data.

Jamming:

This attack exploits the wireless transmission capabilities of IoT. Attackers intentionally interfere with wireless signals transmitted over the air, disrupting communication. For instance, IoT devices can be blocked by sending interfering signals.

Physical Destruction:

This attack is closely related to physical tampering, involving the intentional destruction or damage of IoT devices. Attackers may target sensors, actuators, and communication infrastructure within the IoT, causing destruction or damage.

Power Attacks:

Since IoT devices operate on batteries, attackers manipulate power sources to damage or disrupt device operations. Malfunctions can result from underpowering or overloading, for instance.

Environmental Interference:

Natural resources, such as earthquakes, floods, and storms, can affect IoT operations. Weather conditions interfere with wireless communication signals.

Interception:

Attackers intercept wireless communication and capture transmitted data among IoT devices using specialized equipment and analysis.

Impersonation:

Attackers impersonate legitimate IoT devices to gain unauthorized access to communication, spoofing the identity of legitimate devices.

These attacks can be prevented by monitoring suspicious activities in the IoT environment, securing the design of IoT hardware devices, and implementing effective encryption mechanisms.

Man-in-the-Middle Attack:

Attackers inject malicious content or eavesdrop on communication between devices, intercepting the communication.

Replay Attack:

Attackers retransmit or capture authenticated data, disrupting communication to gain unauthorized access over IoT devices.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack:

Attackers flood communication with unwanted information, overloading channels, making them unavailable to legitimate users, resulting in low network performance.

Spoofing:

Attackers impersonate a trusted source or device, gaining trust from other devices to send false commands and disrupt normal network activities.

Interference:

Attackers jam radio frequencies, disrupting wireless communication signals.

Traffic Analysis:

Attackers analyze and monitor communication patterns, gaining insights to compromise IoT environment security by studying the timing and frequency of messages.

Command Injection:

Attackers compromise or control IoT devices by sending authorized or malicious commands.

6. Security Solutions for the Internet of Things (IoT) Environment

Researchers have devised numerous solutions to address security vulnerabilities in the IoT environment. Each solution operates on its own principle and can be applied based on the deployment of applications. These solutions can be broadly classified into four categories: cryptographic-based solutions, intrusion detection-based solutions, machine learning-based solutions, and trust-based solutions. The following section will discuss each category one by one [31-40].

Cryptographic-based Solutions:

Cryptographic techniques employ robust security mechanisms and algorithms to ensure security requirements such as confidentiality and integrity. They authenticate devices and protect transmitted and stored data. Cryptographic-based solutions fall into several types:

Public Key Cryptography: Uses private and public key pairs to establish secure and trusted communications, providing encryption, digital signatures, and authentication.

Secure Key Exchange: Achieved through protocols like Elliptic Curve Diffie-Hellman and Diffie-Hellman, protecting data from unwanted access.

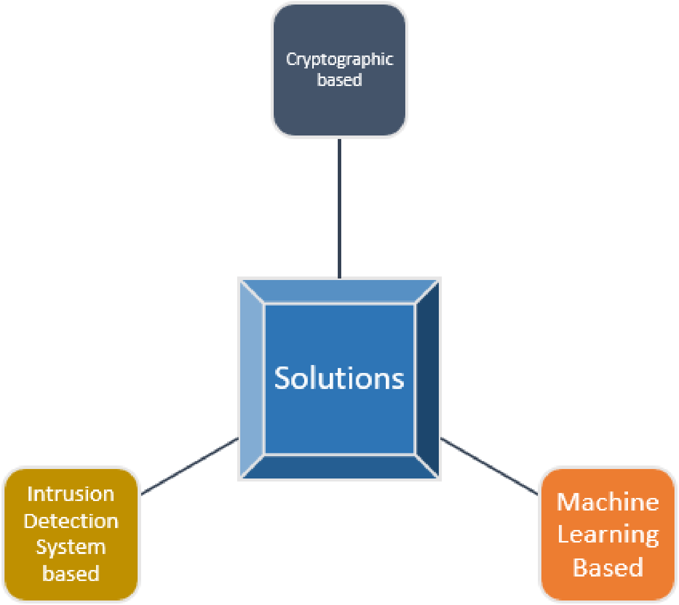

Figure 3. Security solutions

Secure Socket Layer/Transport Layer Security: Secures data transmission channels, encrypting data during transmission between servers and IoT devices.

Data Encryption: Utilizes both symmetric and asymmetric encryption algorithms like Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) to ensure data confidentiality.

Digital Signatures: Ensures device identity and data authenticity using private and public keys.

Hash Functions: Guarantees data integrity by creating fixed-length hashes (digests) from data.

Secure Boot: Uses cryptographic techniques to ensure the integrity of secure software boot-up, preventing the execution of unauthorized code.

Code Signing: Ensures only authorized and genuine software runs on IoT devices, utilizing private and public keys.

Hardware Security Modules and Secure Elements: Dedicated hardware modules protect cryptographic keys from software-based attacks in IoT applications.

Blockchain Technology: Decentralized networks with immutable ledgers ensure integrity in sensitive applications.

Quantum Safe Cryptography: Prevents quantum attacks using resistant cryptographic algorithms.

Intrusion Detection System (IDS) based Solutions:

Intrusion Detection Systems play a crucial role in enhancing security by identifying potential threats, anomalies, and unauthorized access in the IoT environment. IDS solutions include:

Network-based IDS (NIDS): Monitors traffic flow among IoT devices and other network segments to identify suspicious behavior and attack signatures.

Host-based IDS (HIDS): Deployed in end devices, monitors individual IoT elements for abnormal or suspicious behavior.

Anomaly-based IDS: Identifies unknown threats and zero-day vulnerabilities by setting baselines for normal behavior.

Signature-based IDS: Identifies documented and well-known attacks using predefined patterns or signatures.

Behavior-based IDS: Oversees the behavior of IoT elements over time, identifying multifaceted and complex attacks.

Machine Learning and AI-based IDS: Utilizes ML and AI algorithms to identify suspicious behavior and detect new threats in the IoT ecosystem.

Cloud-based IDS: Leverages cloud platforms for threat analysis, ensuring centralization, scalability, and reduced computational burden on IoT devices.

Machine Learning Algorithms-based Solutions:

Several machine learning algorithms enhance IoT device security by identifying vulnerabilities, anomalies, and threats in real-time. Notable machine learning algorithms role in IoT include:

Anomaly Detection: Learns normal behavior to identify unusual activities and threats in the IoT ecosystem.

Behavioral Analysis: Identifies unauthorized activities and compromised devices using predefined learned patterns.

Predictive Maintenance: Predicts IoT device failures for proactive maintenance.

Malware Detection: Blocks malicious code execution and detects unknown malware using network traffic and behavioral analysis.

Threat Intelligence and Monitoring: Provides frequent monitoring of threats and updates databases based on threat intelligence.

User and Entity Behavior Analytics: Tracks IoT entities and user behavior, detecting deviations in security mechanisms.

Adaptive Access Control: Analyzes risks associated with users and IoT devices to grant access only to authorized users, adjusting dynamically based on security postures.

Network Traffic Analysis: Involves real-time analysis of data to prevent network-based attacks, especially Denial of Service and Distributed Denial of Service attacks, by detecting network traffic patterns.

7. Conclusion

In conclusion, this review serves as a comprehensive guide to the security challenges inherent in the Internet of Things, providing insights into the current state of IoT security practices. As IoT continues to revolutionize industries, understanding and addressing its security implications are imperative for harnessing its full potential while mitigating risks to privacy and data integrity.

References:

[1]. Jing, Qi, et al. "Security of the Internet of Things: perspectives and challenges." *Wireless Networks* 20 (2014): 2481-2501.

[2]. Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." *Journal of Network and Computer Applications* 88 (2017): 10-28.

[3]. Suo, Hui, et al. "Security in the internet of things: a review." *2012 international conference on computer science and electronics engineering*. Vol. 3. IEEE, 2012.

[4]. Weber, Rolf H. "Internet of Things–New security and privacy challenges." *Computer law & security review* 26.1 (2010): 23-30.

[5]. Adat, Vipindev, and Brij B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." *Telecommunication Systems* 67 (2018): 423-441.

[6]. Gan, Gang, Zeyong Lu, and Jun Jiang. "Internet of things security analysis." *2011 international conference on internet technology and applications*. IEEE, 2011.

[7]. Sadique, Kazi Masum, Rahim Rahmani, and Paul Johannesson. "Towards security on internet of things: applications and challenges in technology." *Procedia Computer Science* 141 (2018): 199-206.

[8]. Alizadeh, Morteza, Karl Andersson, and Olov Schelen. "A survey of secure internet of things in relation to blockchain." *Journal of Internet Services and Information Security (JISIS)* 10.3 (2020): 47-75.

[9]. Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." *2015 IEEE symposium on computers and communication (ISCC)*. IEEE, 2015.

[10]. Li, Shancang, Theo Tryfonas, and Honglei Li. "The Internet of Things: a security point of view." *Internet Research* 26.2 (2016): 337-359.

[11]. Ning, Huansheng, Hong Liu, and Laurence T. Yang. "Cyberentity security in the internet of things." *Computer* 46.4 (2013): 46-53.

[12]. El-Masri, Mazen, and Eiman Mutwali Abdelmageed Hussain. "Blockchain as a mean to secure Internet of Things ecosystems–a systematic literature review." *Journal of Enterprise Information Management* 34.5 (2021): 1371-1405.

[13]. Ogonji, Mark Mbock, George Okeyo, and Joseph Muliaro Wafula. "A survey on privacy and security of Internet of Things." *Computer Science Review* 38 (2020): 100312.

[14]. Alizadeh, Morteza, Karl Andersson, and Olov Schelen. "A survey of secure internet of things in relation to blockchain." *Journal of Internet Services and Information Security (JISIS)* 10.3 (2020): 47-75.

[15]. Kaushal, Rajesh Kumar, et al. "Using mobile computing to provide a smart and secure Internet of Things (IoT) framework for medical applications." *Wireless Communications and Mobile Computing* 2022 (2022): 1-13.

[16]. HaddadPajouh, Hamed, et al. "A survey on internet of things security: Requirements, challenges, and solutions." *Internet of Things* 14 (2021): 100129.

[17]. Ande, Ruth, et al. "Internet of Things: Evolution and technologies from a security perspective." *Sustainable Cities and Society* 54 (2020): 101728.

[18]. Echeverría, Aarón, et al. "Cybersecurity model based on hardening for secure internet of things implementation." *Applied Sciences* 11.7 (2021): 3260.

[19]. Awotunde, Joseph Bamidele, and Sanjay Misra. "Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks." *Illumination of artificial intelligence in cybersecurity and forensics*. Cham: Springer International Publishing, 2022. 21-44.

[20]. Azrour, Mourade, et al. "Internet of things security: challenges and key issues." *Security and Communication Networks* 2021 (2021): 1-11.

[21]. Ahmad, Usman, et al. "A novel deep learning model to secure internet of things in healthcare." *Machine intelligence and big data analytics for cybersecurity applications* (2021): 341-353.

[22]. Jurcut, Anca, et al. "Security considerations for Internet of Things: A survey." *SN Computer Science* 1 (2020): 1-19.

[23]. Sadhu, Pintu Kumar, Venkata P. Yanambaka, and Ahmed Abdelgawad. "Internet of things: Security and solutions survey." *Sensors* 22.19 (2022): 7433.

[24]. Omolara, Abiodun Esther, et al. "The internet of things security: A survey encompassing unexplored areas and new insights." *Computers & Security* 112 (2022): 102494.

[25]. Ahmid, Maroua, and Okba Kazar. "A comprehensive review of the internet of things security." *Journal of Applied Security Research* 18.3 (2023): 289-305.

[26]. Das, Sangjukta, and Suyel Namasudra. "Lightweight and efficient privacy-preserving mutual authentication scheme to secure internet of things-based smart healthcare." *Transactions on Emerging Telecommunications Technologies* (2023): e4716.

[27]. Rekha, Shashi, et al. "Study of security issues and solutions in Internet of Things (IoT)." *Materials Today: Proceedings* 80 (2023): 3554-3559.

[28]. Cui, Hui, and Xun Yi. "Secure Internet of Things in cloud computing via puncturable attribute-based encryption with user revocation." *IEEE Internet of Things Journal* (2023).

[29]. Sarker, Iqbal H., et al. "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions." *Mobile Networks and Applications* 28.1 (2023): 296-312.

[30]. Swessi, Dorsaf, and Hanen Idoudi. "A survey on internet-of-things security: threats and emerging countermeasures." *Wireless Personal Communications* 124.2 (2022): 1557-1592.

[31]. Du, Hongyang, et al. "Rethinking wireless communication security in semantic Internet of Things." *IEEE Wireless Communications* 30.3 (2023): 36-43.

[32]. Ravikumar, K. C., et al. "Challenges in internet of things towards the security using deep learning techniques." *Measurement: Sensors* 24 (2022): 100473.

[33]. Khan, Abdullah Ayub, et al. "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review." *IEEE Access* (2022).

[34]. Zhang, Xixi, et al. "An Automatic and Efficient Malware Traffic Classification Method for Secure Internet of Things." *IEEE Internet of Things Journal* (2023).

[35]. Rizzardi, Alessandra, Sabrina Sicari, and Alberto Coen-Porisini. "Analysis on functionalities and security features of Internet of Things related protocols." *Wireless Networks* 28.7 (2022): 2857-2887.

[36]. Abbas, Ghulam, et al. "Safety, Security and Privacy in Machine Learning Based Internet of Things." *Journal of Sensor and Actuator Networks* 11.3 (2022): 38.

[37]. Dhar, Shalini, Ashish Khare, and Rajani Singh. "Advanced security model for multimedia data sharing in Internet of Things." *Transactions on Emerging Telecommunications Technologies* (2022): e4621.

[38]. Gaurav, Akshat, Konstantinos Psannis, and Dragan Peraković. "Security of cloud-based medical internet of things (miots): A survey." *International Journal of Software Science and Computational Intelligence (IJSSCI)* 14.1 (2022): 1-16.

[39]. Kaur, Barjinder, et al. "Internet of things (IoT) security dataset evolution: Challenges and future directions." *Internet of Things* (2023): 100780.

[40]. Alqarawi, Ghaida, et al. "Internet-of-things security and vulnerabilities: case study." *Journal of Applied Security Research* 18.3 (2023): 559-575.