Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 123-132
MİLLİ TƏHLÜKƏSİZLİK ***NATIONAL SECURITY***

UOT 004 DOI: 10.30546/9878.2024.2.10.0036.

PRESERVING CONFIDENTIAL INFORMATION: A COMPREHENSIVE ANALYSIS OF SECURITY AND PRIVACY CONCERNS IN INTERNET OF THINGS (IOT) SYSTEMS

mayor Elshan Tanriverdiyev
National Defence University
elshantanriverdiyev@gmail.com

Abstract. This research paper conducts a thorough analysis of security and privacy concerns within internet of things (IoT) systems, aiming to identify vulnerabilities across its various layers perception, network, transport, and application – and develop strategies to mitigate these risks. The study is structured to first categorize major security threats and privacy issues within each IoT layer, followed by a comprehensive literature review to understand existing challenges and solutions. Further tasks include analyzing common attack vectors and assessing the effectiveness of proposed security measures through simulations and real-world case studies.

A variety of research methods were employed, including systematic literature reviews, case studies, experimental research, and simulation modeling to test and predict effectiveness of the solution.

The research results reveal key vulnerabilities within each IoT layer and catalog a comprehensive range of potential attack vectors by their targets and threat nature. It highlights significant shortcomings in existing security measures, and emphasizes the need for enhanced solutions tailored to these specific vulnerabilities.

The outcome of the research is the development of recommended security measures and best practices, specifically designed for IoT systems. These recommendations encompass layered security protocols, enhanced encryption methods, and dynamic authentication mechanisms. The study also proposes a framework for continuous security assessment and adaptation, aiming to foster the development of more resilient and secure IoT environments. This comprehensive approach not only addresses current security challenges but also prepares for future threats.

Keywords: internet of things, IoT Systems, IoT security issues, IoT security attacks

Introduction

In the realm of future technologies, the Internet of Things (IoT) has become a ubiquitous and frequently discussed concept. IoT comprises a network of intelligent objects, with these nodes serving as the central actors in the IoT network. Their primary function is information exchange and facilitating user communication. IoT stands at the forefront of the ongoing expansion of internet services, as it aims to integrate and connect an extensive array of objects and devices [1]. IoT entities encompass a wide range of devices, including laptops, smartphones, smartwatches, televisions, and automobiles. Each individual IoT node within the network possesses its distinct identity and designated role. The seamless cooperation among these nodes results in the formation of a robust and collaborative IoT network. Within IoT, objects are integrated into the physical environment and initiate data collection and sharing autonomously, free from human intervention. It was projected that the quantity of interconnected objects on the internet would soar to approximately 25 billion by the year 2020 [2]. IoT devices exhibit intelligence due to their access to data and information from interconnected devices, providing them with the capability to make real-time decisions and execute their functions intelligently. Figure 1 illustrates the fundamental concept of IoT systems [3]. In the near future, the proliferation of IoT networks is anticipated to continue, expand in scope, and assume greater significance within the realm of technology. As IoT continues to evolve, fresh security and privacy concerns emerge, alongside the exacerbation of conventional security and privacy issues. Two primary drivers of this phenomenon are the vast number of connected objects and the increasing diversity within the IoT landscape [4]. Within

IoT development communities, there is a diverse group of developers, some of whom possess limited familiarity with security standards. The inherent complexity and ambiguity surrounding IoT have consequently elevated IoT security to the top priority for both end-users and institutions [5].

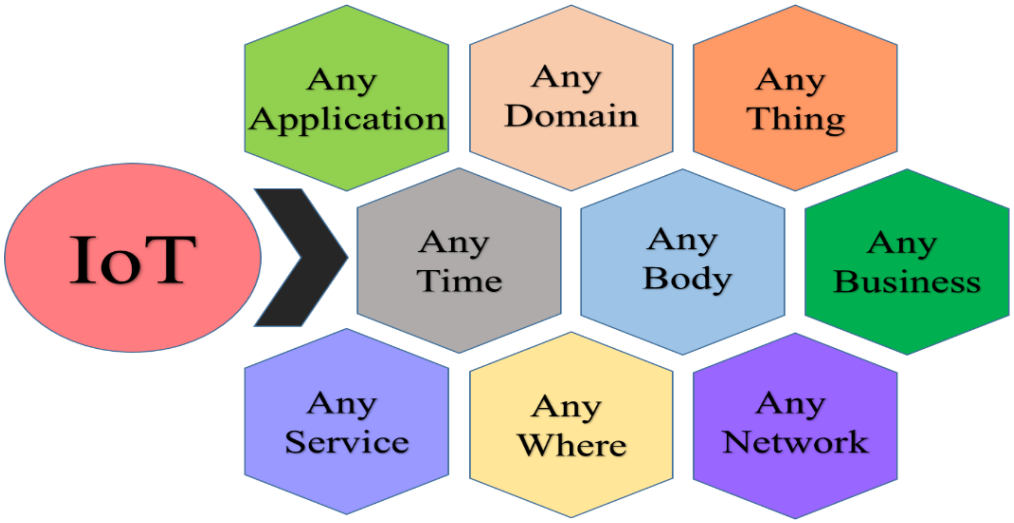

Figure 1. The fundamental concept of IoT systems

Much like any other technology, IoT is susceptible to attacks from malicious users or hackers. The extensive and intricate architecture of IoT creates vulnerabilities that hackers can identify and exploit, potentially leading to network breaches. These breaches can manifest in various ways, including network disruption, data misuse, and more. Given the critical role of IoT networks, it is imperative to fortify their security and address all potential vulnerabilities. Users are increasingly seeking the highest levels of security and privacy when utilizing IoT networks, given the sensitive information exchanged within these networks. Consequently, the subject of IoT security and privacy has gained prominence due to the integral role of IoT in our daily lives. IoT technology is omnipresent, appearing in forms such as smart wearables (e.g., smartwatches), smart homes, autonomous vehicles, precision agriculture systems, healthcare solutions, and more.

Security concerns within IoT networks stem from multiple sources. Some of these issues in security and privacy result from attacks on different layers of the IoT architecture. Additionally, attacks may exploit the network's communication characteristics to infiltrate and compromise network components, weakening their integrity. This paper conducts a thorough examination of IoT security and privacy issues, delving into their complexities. It seeks to shed light on the types of attacks that can target IoT systems, detailing how these attacks have detrimental effects. Furthermore, the paper outlines measures to prevent attacks and fortify IoT systems against potential threats. It serves the purpose of providing comprehensive insights into the state of IoT security and the possible risks faced by IoT users, thereby aiding in the development of stronger and more secure IoT systems, given their expanding use in everyday life.

1. Security and privacy concerns at different layers of IoT:

IoT consists of four primary layers, namely, the perception layer, network layer, transport layer (commonly referred to as the Middleware Layer), and the application layer. Each of these layers introduces its distinct privacy and security considerations. This section will provide an in-depth exploration of these IoT layers, highlighting the respective issues, challenges, and security aspects. Figure 2 illustrates the composition of IoT layers.

The perception layer encompasses distinct sets of data, divided into two primary components: the perception node and the perception network. The perception node assumes the role of data collection, while the perception network manages the transmission and administration of data. Within the perception layer, a diverse array of sensor technologies are integrated, such as Radio Frequency Identification (RFID) [6].

RFID systems encounter security and privacy challenges. The perception layer encompasses a variety of control and data collection modules, including sound sensors, vibration sensors, and temperature sensors. Within this layer, the primary role is to gather data from the environment through the use of sensors and actuators.

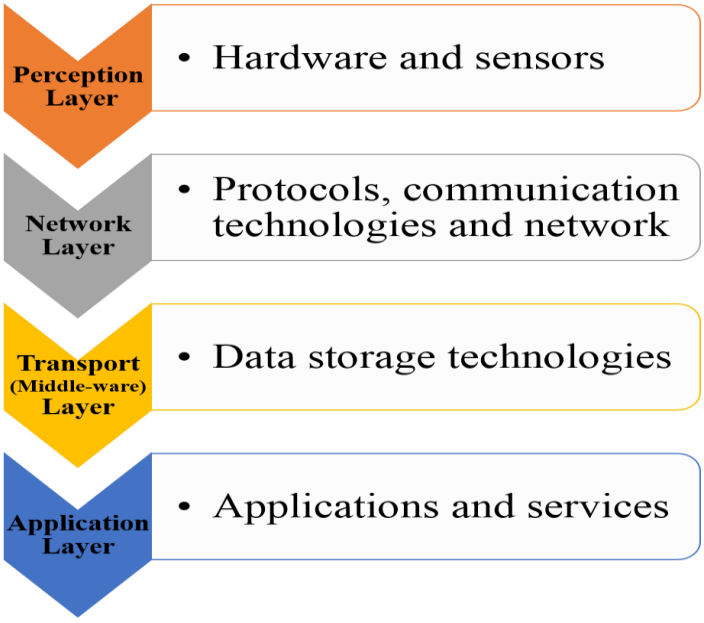

Figure 2. IoT layers

Subsequently, the perception layer undertakes the tasks of data verification, collection, and processing before forwarding the information to the subsequent layer, which is the network layer. It is worth noting that data collected within the perception layer may undergo pre-processing before transmission to the network layer. Additionally, this layer is responsible for regulating data sources, with IoT nodes serving as the primary data origin [7].

1.1. Perception layer security and privacy issues:

IoT nodes face significant susceptibility to attacks, which has led to the development of a security node within the architecture of the perception layer (referred to as SNPL). The application layer primarily encompasses hardware components and sensors. Within the perception layer, there are various security and privacy concerns, which are outlined as follows:

1.1.1. Tag Cloning:

Tags are affixed to various objects, and, through certain hacking techniques, the data on these objects can be accessed, read, and even altered. This situation can result in tag cloning, where individuals with ill intent can effortlessly capture tags and produce duplicates, making it challenging for users to distinguish between the compromised and authentic tags.

1.1.2. Eavesdropping:

Eavesdropping refers to the interception of information exchanged between two nodes or communication devices, often involving a process known as data sniffing. The wireless nature of RFID technology renders it vulnerable to eavesdropping, making it relatively easy for hackers to intercept sensitive information flowing between the tag and the reader, or vice versa. Within the realm of wireless surveillance, there are two primary categories of eavesdropping attacks: passive and proactive. Proactive eavesdropping is employed with the aim of intensifying the eavesdropping rate.

1.1.3. Spoofing:

These attacks involve the transmission of inaccurate and deceptive information to the RFID system, with the intent of falsely representing it as originating from an authenticated and genuine source. This deceptive tactic grants attackers full access to the system, rendering it vulnerable. Spoofing attacks are a type of assault that can result in the creation of routing loops. Such attacks have the capability to both truncate and elongate source routes, achieved by either repelling or enticing network selection by

nodes. Spoofing attacks encompass various forms, including IP spoofing and RFID spoofing. RFID spoofing takes place when an attacker attempts to deceive the system and gain access to records, subsequently sending harmful data by employing the identification of an authorized tag. Attackers employ tactics aimed at persuading the application that they are genuine users, with the objective of assuming control over the IoT application.

1.1.4. RF Jamming:

Radio Frequency (RF) Jamming involves a deliberate non-compliance with lower-level protocols to disrupt ongoing legitimate communication. RF jamming can have various detrimental effects on communication by transmitting signals with diverse patterns. In this type of attack, RFID tags are compromised through a Denial of Service (DoS) attack, which introduces RF signals mixed with noise signals, disrupting communication. The source initiating jamming attacks may vary in power, from very potent, capable of damaging the entire network, to less powerful, causing harm to specific network segments. Security attacks and threats are pertinent across all layers of IoT. These attacks fall into two broad categories: active attacks, which directly impede service, and passive attacks, which observe IoT network information without obstructing network functions. Security attacks can also be categorized based on their source of origin, with external attacks stemming from sources outside the network, and internal attacks initiated by insiders. At all IoT layers, IoT objects and services are susceptible to Denial of Service (DoS) attacks, which aim to render the network inaccessible to authorized users [8].

Within the perception layer, three primary security issues are prominent. The first issue pertains to the strength of wireless signals. In this layer, signals are transmitted between sensors using wireless technologies, and the effectiveness of this communication can be compromised by interference from disruptive waves. The second issue is associated with IoT devices, where sensor nodes can be incapacitated either by the device owner or by potential attackers. This vulnerability is due to the outdoor and external nature of IoT systems, making them susceptible to physical attacks on both the IoT nodes and the IoT system. The third issue revolves around the dynamic nature of network topology within IoT. IoT nodes frequently move across various locations, resulting in a constantly shifting network topology. In the perception layer, RFID and sensors play a critical role. However, these components have limited storage, power capacity, and computational capabilities, making them susceptible to security breaches and attacks.

Altering, spoofing, or replaying the identity information of an IoT device can instigate a replay attack [9]. In a timing attack, hackers scrutinize the time required for encryption to deduce the encryption key. Node capture attacks transpire when an attacker gains control over IoT nodes, capturing their data and information. Attackers exploit the confidentiality of the perception layer by employing replay attacks, timing attacks, and node capture attacks. To threaten the integrity of data in the perception layer, assailants may add an extra node that transmits malicious data to the IoT network. Initiating a Denial of Service (DoS) attack is attainable by draining the energy of IoT nodes and preventing them from entering sleep mode, which is designed to conserve energy. Security issues within the perception layer can be mitigated through the implementation of point-to-point or end-to-end encryption measures.

The perception layer constitutes the foundational tier in IoT systems, situated at the lowest level of the IoT layer hierarchy. This layer serves multiple security functions and serves four primary purposes: safeguarding data privacy and sensitive information, enabling authentication, and assessing potential risks. Authentication is a crucial security objective essential for safeguarding systems against intrusion from hackers and malicious entities. Cryptography provides a means to implement authentication, employing algorithms capable of generating digital signatures to fortify protection against attacks, including collision attacks and brute force attempts. The protection and security of data are paramount during both collection and transmission to subsequent layers. Achieving data privacy can be accomplished through the utilization of symmetric and asymmetric encryption algorithms. These encryption algorithms are particularly advantageous for sensor deployment due to their minimal power consumption. Ensuring location anonymity and identity protection is essential for securing sensitive information. This can be effectively accomplished through the K-Anonymity approach, which shields

user data, identity, and location information from potential exposure and harm. Risk assessment holds a significant role within IoT security, primarily because it aids in the identification of novel threats to systems. Furthermore, it assists in the formulation of security strategies that can be categorized as optimal, ultimately serving as a preventative measure against potential security breaches. In the event that an intrusion is detected, the RFID reader issues a kill-command to the RFID tag to halt unauthorized access to the data stored on the tag [10].

2. IoT Network Layer security and privacy issues:

Following the perception layer in the IoT layers framework, the subsequent layer is the network layer. This layer assumes responsibility for ensuring the security of information and facilitating the transmission of data within the network.

The network layer encompasses a spectrum of technologies including mobile devices, the internet, and cloud computing. Within this layer, Wireless Sensor Networks (WSN) are responsible for reliably transmitting data from sensors to their intended destinations. It also plays a crucial role in facilitating data exchange between IoT devices and hubs and serves as the foundation for data routing. Various technologies such as WiFi, Bluetooth, 3G, and LTE are employed in the network layer to manage internet operations, including switching, routing, and gateways. Network gateways act as intermediaries between IoT nodes, facilitating the process of transmitting, aggregating, and filtering data. The network layer consists of an array of protocols, communication technologies, and the corresponding hardware. In practice, the network layer plays a pivotal role in establishing connections between IoT nodes and IoT applications, allowing for data flow and interaction. Each node or device within the IoT system has a unique identity to enable data traceability. Network components like switches, hubs, routers, and gateways are crucial in connecting IoT nodes and devices with each other. One of the primary security concerns at the network layer is the potential for a Denial of Service (DoS) attack. These attacks are initiated by malicious actors with the intent of rendering services unavailable to legitimate users.

2.1. Sybil Attack:

A Sybil attack involves an attacker attempting to compromise the system by manipulating a node to possess multiple identities, leading to the dissemination of false information. In a Sybil attack, malicious entities can employ multiple identities within the same network, often presenting duplicated or erroneous identification for the purpose of deceiving other IoT nodes.

2.1.1. Sinkhole Attack:

A sinkhole attack revolves around the strategy of making compromised nodes appear appealing to nearby nodes, causing data to be directed toward these compromised nodes and, ultimately, leading to dropped packets. The system, under the influence of this attack, falsely assumes that data has been successfully transmitted to its destination, while, in reality, the system's traffic is disrupted. Sinkhole attacks can potentially trigger a Denial of Service (DoS) scenario due to the increased energy consumption associated with routing through malicious nodes. In a sinkhole attack, a malicious node can deceive IoT nodes by providing fraudulent routing information, redirecting the packets of other nodes through it. The process of a sinkhole attack operates in a clandestine manner, typically escaping the network's detection mechanisms, as attackers aim to mislead the system into believing that all transmitted data has reached its intended receiver.

2.1.2. Denial of Service (DoS) Attack:

A Denial of Service (DoS) attack transpires when an attacker seeks to inundate a network with an excessive volume of meaningless traffic, depleting the system's resources. As a result, the system's network becomes inaccessible to its users. In this type of attack, the attacker sends a barrage of requests to a server, overwhelming it with requests, ultimately causing the server to become unresponsive or go offline.

2.1.3. Malicious code injection:

A malicious code injection attack transpires when an attacker attempts to manipulate a sensor node into introducing malicious code into the system, resulting in network shutdown. This subsequently grants the attacker complete control over the network. Code injection enables attackers to incorporate malicious

code into input fields, allowing them to execute the code and gain unauthorized access to the application. This form of attack can manifest when injecting malicious JavaScript code into an HTML document, potentially leading to hijacking and the spread of botnets.

2.1.4. Man-in-the-Middle Attack:

The Man-in-the-Middle attack is akin to an eavesdropping attack, with its focus centered on the communication channel. In this attack, an unauthorized user can intercept and manipulate communication between two other parties. Additionally, the unauthorized user has the capacity to assume the identity of the victim and utilize the channel for information acquisition.

In a Passive Man-in-the-Middle attack, an eavesdropper taps into the communication using a Poisson channel. In the context of traffic analysis, passive monitoring and eavesdropping can compromise the privacy and confidentiality of IoT networks. These three attacks are frequent due to the remote access mechanism and data exchange. Man-in-the-Middle and eavesdropping attacks are especially likely to occur in the network layer. The security of communication channels becomes compromised if the keying material of IoT devices is intercepted.

IoT communication fundamentally differs from typical internet communication because IoT extends beyond machine-to-human interactions to include machine-to-machine communication. This expansion introduces compatibility and security challenges, particularly in the context of heterogeneous network components [10]. Standard network protocols are often inadequate for addressing these diverse elements. In an IoT network, various objects are interconnected to gather information about users, a feature that malicious actors may exploit to misuse user information. Consequently, safeguarding IoT network objects is as crucial as protecting the network itself. These objects should possess the capability to take proactive measures in self-defense against network-initiated attacks. This requires the implementation of robust protocols and software within the network, enabling objects to respond to abnormal behaviors or conditions that threaten both the objects and network security.

Network layers encompass both wired and wireless communication capabilities. The openness of wireless communication channels exposes the network layer to a multitude of potential attacks. Security within the network layer can be categorized into three types: authentication, routing security, and data privacy. The implementation of authentication and encryption measures is effective in thwarting unauthorized access to nodes, consequently preventing the dissemination of false information. The most common threat encountered is the Denial of Service (DoS) attack, which disrupts the network by flooding it with an excess of meaningless traffic within communication channels. Routing algorithms play a crucial role in ensuring the privacy of data transmitted between sensors and the system. To enhance the system's error detection capabilities and fortify it against potential failures, multiple data routing paths need to be established. Security control mechanisms must be integrated to monitor the system and shield it from various forms of intrusion. To verify that received data at one end matches the original data transmitted from the other end, data integrity methods should be implemented. The security issues within the transport layer can be categorized as follows:

2.2. IoT Transport (Middle-ware) Layer security and privacy issues:

Following the network layer in IoT systems, the subsequent layer is the Transport (Middle-ware) Layer. Within this layer, data storage technologies, such as cloud computing, are employed. This layer facilitates ubiquitous access for the perception layer, and it is divided into three distinct layers: local area, core network, and access network.

2.2.1. Unauthorized Access:

Unauthorized system access may transpire when an attacker engages in data deletion or restricts access to IoT services, thereby inflicting harm on the IoT system. The Transport (Middle-ware) layer offers dual interfaces, one for data storage and another for applications. Attackers can gain unethical entry to infiltrate the network by exploiting misconfigured access control rights.

2.2.2. DoS Attack:

A Denial of Service (DoS) attack is characterized by the generation of a substantial volume of superfluous traffic aimed at incapacitating the system. Attackers execute these attacks to render the

network service unavailable for a specific duration [10]. Numerous DoS attacks can be launched to target the IoT system, with their objective being the depletion of service provider resources and network bandwidth. The complexity and heterogeneity of IoT networks render the transport layer susceptible to DoS attacks.

2.2.3. Malicious Insider:

Insiders possess the capability to manipulate and modify data to serve their personal interests. A Malicious Insider attack transpires when an insider manipulates data for their personal gain or the benefit of third parties. One potential method to safeguard IoT systems against malicious insider attacks involves the implementation of the Isabelle insider framework. This framework is designed to identify any policy violations that may occur [11].

2.3. IoT Application Layer security and privacy issues:

The final layer within the IoT framework, subsequent to the Transport (Middle-ware) Layer, is the application layer. This layer plays a vital role in structuring the application layer's services, is visible to end users, and represents the topmost layer. Its purpose is to fulfill the vision of creating smart environments and IoT-based systems, ensuring authenticity, integrity, and confidentiality. However, security issues can arise due to the absence of standardized processes for managing application development and their interactions [12]. It becomes challenging to guarantee data privacy and authentication for applications that employ diverse authentication mechanisms. The application layer encompasses various service domains, such as connected cars and healthcare, each of which must address its specific security threats and establish corresponding security measures. The Application Layer provides user access to IoT applications. Security measures can be integrated into the application layer by incorporating security policies in the functional architecture. Security concerns within the application layer can be mitigated through the implementation of security measures such as firewalls, antivirus software, and intrusion detection systems. These security issues within the application layer can be categorized as follows:

2.3.1. Malicious Code Injection:

Malicious code injection transpires when an attacker inserts malicious code into the system to pilfer user data. Hackers initiate this attack by exploiting vulnerabilities in the system's graphical user interface (GUI), either within the software or on the device itself, to execute actions such as Cross-Site Scripting (XSS) attacks, deploying Trojans that disrupt normal operations, or executing remote code. Unlike traditional attacks that can be deterred with antivirus tools, malicious code injection presents a challenge since it may either activate automatically or necessitate the attacker's intervention to initiate the attack on the system.

2.3.2. DoS Attack:

In recent times, Denial of Service (DoS) attacks have evolved to become more sophisticated than their earlier counterparts. These attacks employ a smokescreen tactic to carry out their malicious activities, deceiving users regarding the actual location of the attack. This strategy leads users to believe that the attack is occurring in a different part of the system, ultimately diverting their attention [13]. As a consequence, DoS attacks can place unencrypted sensitive user information into the hands of hackers. DoS attacks operate within the application layer, much like their actions across other layers, with the shared objective of disrupting service availability. DoS attackers possess the capability to undermine the availability of services or applications.

2.3.3. Spear-Phishing Attack:

The Spear-Phishing attack begins when an attacker attempts to launch an assault on users through emails sent to the victims. The goal is to entice victims into opening the email, with the aim of acquiring additional sensitive data from them. Spear-Phishing is a multi-step procedure that entails the attacker gathering information about a specific target or a group of targets.

2.4. Sniffing Attack:

A Sniffing attack happens when an attacker introduces a sniffer application into the system, allowing them to gather information about the network, ultimately compromising the system. Sniffing

can take various forms, including DNS poisoning, ARP poisoning, DHCP attacks, MAC flooding, and password sniffing [14]. Sniffers initiate their monitoring activities at the data link layer, and once the data link layer is compromised, other upper layers become involved in the sniffing process.

There are no universally applicable rules and standards in place to regulate the development and interactions of IoT applications. This lack of uniformity gives rise to several security concerns related to IoT applications. These applications employ diverse authentication mechanisms, making it challenging to ensure data privacy, identity verification, and seamless integration of various IoT applications. As the number of connected devices participating in information sharing within the IoT network increases, it places a growing burden on applications responsible for data analysis. This, in turn, affects the availability of services. When designing IoT applications, three critical considerations must be addressed: understanding how users interact with the application, managing the volume of data, and determining the system administrator. IoT application users should be equipped with tools that grant them control and management over their data disclosure preferences. Users should also possess knowledge about the usage, timing, and entities accessing their data.

Security measures within the Transport (Middle-ware) layer and application layer are categorized into four distinct areas: risk assessment, authentication, data security, and intrusion detection. Authentication serves as a safeguard against malicious users attempting to gain unauthorized access to the system by verifying their identities. The Middle-ware layer leverages various key technologies, such as cloud technologies, which can be susceptible to compromise and insider threats. Additionally, virtualization, a technology utilized in this layer, is exposed to data security threats and DoS attacks. Intrusion detection technologies function by raising alerts when any unusual events occur within the system. This is achieved by continuously logging and monitoring the activities of potential intruders. Intrusion detection technologies encompass various approaches, including data mining and anomaly detection. Risk assessment plays a pivotal role in justifying security strategies and enhancing the overall security structure. Encryption technologies can be deployed to prevent data theft and misuse, serving as a means to safeguard data and thwart malicious activities initiated by attackers and malicious users.

Conclusion

IoT technology significantly enhances communication capabilities and interactions among users, driving advancements in smart homes, agriculture, and other areas vital for modern living. Despite these advantages, the susceptibility of IoT systems to security breaches by malicious entities poses a severe risk, particularly in terms of accessing and compromising sensitive data. This reality highlights the urgent need to develop robust security strategies and measures to protect IoT infrastructures and the private data they handle. Security and privacy issues within IoT are critical concerns that vary widely in severity and nature, including both internal and external threats. Although the forms of these attacks differ, they uniformly threaten substantial damage. This research paper thoroughly reviews the literature on IoT security and privacy, addressing the specific security concerns within each layer of IoT architecture and detailing the types of security attacks and their preventive countermeasures. Additionally, it critically assesses the ongoing challenges in IoT security and privacy, emphasizing the need for continuous improvement in security practices to safeguard against evolving threats.

References

1. Singh, D., G. Tripathi, and A.J. Jara, “A survey of Internetof Things: Future Vision, Architecture, Challenges and Services,” 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, Mar 2014.

2. Alsamani, B., Lahza, H. A Taxonomy of IoT: Security and Privacy Threats // 2018 International Conference on Information and Computer Technologies (ICICT) / – USA, – March, – 2018, – p. 72-77,

3. Solangi, Z. A., Solangi, Y. A., Chandio, Aziz, Abd., Hamzah, M. S., Shah., A. The future of data privacy and security concerns in Internet of Things // 2018 IEEE International Conference on Innovative Research and Development (ICIRD, – Thailand, – May – 2018, – p. 1-4

4. Zhang, Z. K., Yi Cho, M. C., Wang, C. W., Hsu, C. W., Chen, C. K., Shieh, S. IoT Security: Ongoing Challenges and Research Opportunities // IEEE 7th International Conference on Service-Oriented Computing and Applications, – Japan, – November 17-19, – 2014, – p. 230-234.

5. Sarrab, M., S. Alnaeli, M. Critical Aspects Pertaining Security of IoT Application Level Software Systems // 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON Vancouver, BC, Canada, November 2018, – p. 960-964.

6. Alabaa, F. A., Internet of Things security: A survey / F.Alabaa, A.M.Othmana, I.A.T.Hashema, F.Alotaibi // – Amsterdam: Journal of Network and Computer Applications – 2017. April.Vol. 88, – p. 10-28.

7. Yang, Y. A Survey on Security and Privacy Issues in Internet-of-Things / Y.Yang, L.Wu, GYin, L.Li, H.Zhao // – New York: IEEE Internet of Things Journal – 2017. № 5. Vol.4. – p. 1250-1258.

8. Wang, Y., Attebury, G., Ramamurthy, B. A Survey of Security Issues In Wireless Sensor Networks // – USA: IEEE Communications Surveys & Tutorials – 2006. № 2. Vol.8, – p. 2-23.

9. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures // 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), – London, – December 14-16, – 2015, – p. 336-341.

10. Farooq, M.U. A Critical Analysis on the Security Concerns of Internet of Things (IoT) / M.U.Farooq, Waseem, M., Khairi,A., Mazha,r S // USA: International Journal of Computer Applications (0975 8887), – 2015. №7. Vol.111. – p. 1-6.

11. Khan, A. Y. Malicious Insider Attack Detection in IoTs Using Data Analytics / A.Khan, Y.R.Latif, S.Latif, S.Tahir, T.Saba // – New York: – 2020. January. Vol. 8. – p. 11743-11753.

12. Assiri, A., Almagwashi, H. IoT Security and Privacy Issues // Riyadh: 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), – April – 2018, – p. 1-5.

13. Ortiz, V. B. Internet of Things (IoT): A Survey on Privacy Issues and Security // – New York: International Journal of Scientific Research – 2015. №3. Vol.1. – p. 168-173.

14. Anu, P., Vimala, Dr.S. A survey on sniffing attacks on computer networks // 2017 International Conference on Intelligent Computing and Control (I2C2), – India, – June – 2017, – p. 1-5.

Xülasə
Məxfi məlumatların qorunması: əşyaların interneti (IoT) sistemlərində təhlükəsizlik və məxfilik problemlərinin ətraflı təhlili
Elşən Tanrıverdiyev

Tədqiqat işinin məqsədi əşyaların interneti (IoT) sistemləri daxilində təhlükəsizlik və məxfilik problemlərinin hərtərəfli təhlil edilməsi, onun müxtəlif təbəqələrində – qavrayış, şəbəkə, nəqliyyat və tətbiqetmədə boşluqların müəyyənləşdirilməsi və bu risklərin azaldılması məqsədilə strategiyanın hazırlanmasıdır. Məqsədə müvafiq olaraq, tədqiqat işində əvvəlcə hər bir IoT təbəqəsi daxilində əsas təhlükəsizlik təhdidlərini müəyyən etmək və məxfilik problemlərini kateqoriyalara ayırmaq, mövcud problemləri və həlli yollarını anlamaq üçün mövcud ədəbiyyatların nəzərdən keçirilməsi kimi vəzifələr qarşıya qoyulur. Əlavə vəzifələrə ümumi hücum vektorlarının təhlili və simulyasiyalar, real dünya nümunələri vasitəsilə təklif olunan təhlükəsizlik tədbirlərinin effektivliyinin qiymətləndirilməsi daxildir.

Təhlükəsizlik həllinin effektivliyini yoxlamaq və proqnozlaşdırmaq üçün nəzəri və müqayisəli təhlil, eksperiment və simulyasiya modelləşdirmə də daxil olmaqla, müxtəlif tədqiqat metodlarından istifadə edilmişdir.

Aşağıdakı nəticələr əldə edilmişdir: Hər bir IoT təbəqəsindəki əsas boşluqlar aşkar edilmiş, potensial hücum vektorlarının geniş spektri müəyyən olunmuşdur. Mövcud təhlükəsizlik tədbirlərindəki əhəmiyyətli çatışmazlıqlar aşkarlanaraq uyğun təkmil həllər təklif olunmuşdur.

Tədqiqatın yekun nəticəsi olaraq, IoT sistemləri üçün nəzərdə tutulmuş tövsiyə olunan təhlükəsizlik tədbirləri və ən yaxşı təcrübələr işlənib hazırlanmışdır. Bu tövsiyələr laylı təhlükəsizlik protokollarını, təkmil şifrələmə üsullarını və dinamik audentifikasiya mexanizmlərini əhatə edir. Tədqiqatda, həmçinin daha davamlı və təhlükəsiz IoT mühitlərinin inkişafını təşviq etmək məqsədilə təhlükəsizliyin qiymətləndirilməsi və uyğunlaşdırılması üçün həllər təklif edilir. Qeyd olunan kompleks yanaşmanın yalnız mövcud təhlükəsizlik məsələlərinə deyil, həm də gələcək təhdidlərdən qorunmaq üçün effektivliyi qeyd olunmuşdur.

Açar sözlər: əşyaların interneti, IoT Sistemləri, IoT təhlükəsizlik problemləri, IoT təhlükəsizlik hücumları

Аннотация

Защита конфиденциальной информации: комплексный анализ вопросов безопасности и конфиденциальности в Системах Интернета Вещей (IoT)

Эльшан Танрывердиев

Это исследовательская работа проводит тщательный анализ проблем безопасности и конфиденциальности в системах Интернета вещей (IoT), целью которого является выявление уязвимостей на различных слоях IoT – восприятие, сеть, транспорт и приложения, и разработка стратегий для снижения этих рисков. Исследование начинается с категоризации основных угроз безопасности и проблем конфиденциальности на каждом слое инфраструктуры IoT, за которой следует всесторонний обзор существующих исследований по безопасности IoT для понимания текущих вызовов и решений. Дополнительные задачи включают анализ распространенных векторов атак и оценку эффективности предложенных мер безопасности посредством симуляций и исследований реальных случаев.

Были использованы различные методы исследования, включая систематические обзоры литературы, кейс-стади, экспериментальные исследования и моделирование симуляций для тестирования и прогнозирования эффективности решений по безопасности.

Результаты исследования раскрывают ключевые уязвимости на каждом слое архитектуры IoT и составляют подробный каталог потенциальных векторов атак, классифицируя их по целям и характеру угроз. Он подчеркивает значительные недостатки в существующих мерах безопасности, подчеркивая необходимость в усиленных решениях, адаптированных к этим конкретным уязвимостям.

Итогом исследования стала разработка рекомендованных мер безопасности и передовых практик, специально предназначенных для систем IoT. Эти рекомендации включают в себя слоистые протоколы безопасности, усовершенствованные методы шифрования и динамичные механизмы аутентификации. Исследование также предлагает рамки для постоянной оценки и адаптации мер безопасности, направленные на создание более устойчивых и безопасных сред IoT. Этот комплексный подход не только решает текущие проблемы безопасности, но и подготавливает к будущим угрозам.

Ключевые слова: интернет вещей, интернет вещей системы, проблемы безопасности интернета вещей, атаки на безопасность интернета вещей.

Məqalə redaksiyaya daxil olmuşdur:29.01.2024
Təkrar işlənməyə göndərilmişdir:12.02.2024
Çapa qəbul edilmişdir: 02.04.2024