IoT Security: A Comprehensive Literature Survey

Zubair Ahmed Khan[1]
Research Scholar, Computer Science & Engineering,
Kalinga University, Chhattisgarh, India
zubairashrafi786@hotmail.com
Dr. Asha Ambhaikar[2]
Professor (CS & IT) & Dean Students Welfare Kalinga University, Chhattisgarh, India
asha.ambhaikar@kalingauniversity.ac.in

Article Info
Page Number: 1249-1264
Publication Issue:
Vol. 70 No. 2 (2021)

Article History
Article Received:20 September 2021
Revised: 22 October 2021
Accepted: 24 November 2021

Abstract

The Internet of Things (IoT) is a new field that is expected to transform the way we live and work. However, IoT device and network security is a major concern and requires a comprehensive literature review of research gaps and methodologies. This survey helps identify the current state of research, knowledge gaps, and future research directions in IoT security. This research covers various aspects of IoT security including authentication, authorization, confidentiality, integrity, availability, privacy, and trust. This article also discusses various methods of his IoT security such as: Encryption, Access Control, Intrusion Detection, and Network Security. This survey will help researchers and practitioners understand the current state of IoT security research and identify challenges and opportunities for future research. Overall, this research is a valuable resource for anyone interested in IoT security research.

Keywords: IoT, Security, Research Gaps, Methodologies, Wireless Networks.

1. Introduction

What are the current research gaps in IoT security?

The current state of research on IoT security reveals a multitude of gaps that need to be addressed. Existing studies have covered a wide range of issues related to securing IoT devices; however, there is still a disconnect between the theoretical understanding of IoT security risks and practical implementation of security measures, as a "valley between threat models and their implementation" exists [1]. One significant gap is the lack of attention given to the physical aspects of IoT devices, with most security analyses focusing on cloud or network interaction, leaving simpler physical attacks overlooked [1]. Furthermore, there is a gap in evaluating the reliability and scalability of systems in heterogeneous IoT environments, highlighting the need for further research in this area [2]. Additionally, there is a lack of consideration for the important base of IoT devices, with current research focusing mainly on specific cases of hacking rather than overall device security [1]. There is also a need to address fundamental attacks affecting underlying hardware, which are not being adequately addressed in current research [1]. Moreover, investment decisions in cyber security are often made based on gut feeling and poor justification, indicating a gap in IoT cyber security risk management [3]. To bridge these gaps and improve IoT security, further research is needed, particularly in evaluating the functionality of IoT devices, network-based vulnerabilities, and resource allocation methods for managers [1].

What are the common methodologies used in IoT security research?

IoT security research employs various methodologies to ensure the security and privacy of IoT systems. Traditional methods are still used in some studies, but ML and DL techniques are the most commonly used approaches [4]. For instance, a semi-supervised learning-based distribution attack detection framework is used for IoT security research, while ML cyber attack and defense strategies using reinforcement learning algorithms have been proposed to improve the ability to detect cyber security attacks [4]. AI approaches, particularly IDSs, are widely used for providing security to IoT devices and networks. A DL method is adopted for wireless IDS using wrapper-based feature extraction, based on a feed-forward deep neural network [4]. Intelligent architectural frameworks are another common methodology for IoT security, and DL-based classification and technique has been used to detect cyber-attacks in IoT networks communications [4]. Anomaly detection techniques are also frequently used, and smart intrusion detection systems are one of the most common methodologies used in IoT security research [4]. IDS solutions are commonly used to protect IoT devices from cyber threats, and they can be categorized into three approaches: signature, anomaly, and hybrid IDS model. The signature-based approach is effective for known attacks, while the anomaly-based is effective for unknown attacks. Anomaly-based IDS detection is advantageous in IoT as it detects zero-day attacks and needs fewer human interventions [5]. The hybrid approach combines both signature-based and anomaly-based approaches [5]. Finally, AI methods are commonly used for the detection of cyber security attacks in IoT environments, and SLR validates the effectiveness of AI approaches for providing security and privacy in IoT environments [4]. In summary, various methodologies have been used in IoT security research, with AI-based methods being the most common approach.

Importance of IoT Security

The importance of IoT security cannot be overemphasized. With billions of his IoT devices deployed in various industries such as healthcare, finance and transportation, one security breach can have devastating consequences. For example, a hacker's access to medical equipment could endanger a patient's health. Therefore, it is imperative that IT leaders take proactive steps to ensure the security of IoT devices. Overall, this article will help researchers and practitioners understand the current state of his IoT security research and identify challenges and opportunities for future research.

2. Current Research Topics in IoT Security

The current research on IoT security is focused on the following key areas:

(i). Authentication and Authorization

Authentication and authorization are crucial for securing IoT devices. Authentication ensures that only authorized users have access to the device, while authorization determines what actions users can perform once they are authenticated. Some of the authentication methods used in IoT security includes two-factor authentication, biometric authentication, and public key infrastructure (PKI) authentication.

(ii). Data Privacy and Confidentiality

Data privacy and confidentiality are also important aspects of IoT security. With the massive amounts of data produced by IoT devices, ensuring the privacy and confidentiality of this data is critical. Encryption is a widely used method for protecting IoT data, with some of the commonly used encryption methods including Advanced Encryption Standard (AES) and Transport Layer Security (TLS).

(iii). Device Security

Device security involves securing the physical devices themselves. This includes implementing measures such as firmware updates, secure boot, and intrusion detection systems to protect against potential threats.

(iv). Network Security

Network security is also essential for IoT security. This involves securing the network infrastructure used by IoT devices, including routers, switches, and firewalls. Some of the network security methods used in IoT security includes virtual private networks (VPNs), intrusion detection and prevention systems (IDPS), and firewalls.

(v). Application Security

Application security involves securing the software applications running on IoT devices. This includes implementing measures such as secure coding practices, regular software updates, and penetration testing to identify potential vulnerabilities in the application.

3. Literature Review on IoT Security

A literature review on IoT security is critical in identifying research gaps and methodologies used to address these gaps. A systematic literature review involves a rigorous and structured approach to reviewing literature. It involves identifying relevant studies, evaluating the quality of these studies, and synthesizing the results to draw meaningful conclusions.We will provide an overview of the literature review below.

SN	Author & Year	Research Findings
1	Fadhil Khalid, L.., & Y. Ameen, S. [7], 2021	The paper discusses the vulnerabilities of IoT integrations in daily life and proposes ways to enhance security, as IoT's growing popularity and internet connectivity increases the likelihood of security threats and attacks targeting users and systems.
2	Shivam Saxena, Bharat Bhushan, Mohd Abdul Ahad [8],2021	This paper explores the integration of blockchain technology with IoT systems as a solution to security vulnerabilities and privacy risks. The authors present a comprehensive survey of security improvements achieved by using blockchain in IoT systems, discuss integration challenges, and outline relevant blockchain-based IoT applications and future research directions.
3	Eduardo B. Fernandez, Hironori Washizaki, Nobukazu Yoshioka, Takao	IoT systems' complexity and heterogeneity lead to a variety of security threats. Patterns are an effective approach to address this issue, but existing IoT security

	Okubo [9], 2021	patterns are insufficient for a practical catalog. This paper surveys and classifies existing patterns and proposes building a unified catalog using modified pattern-based methodologies for distributed systems, with a focus on security.
4	X. Liang and Y. Kim [10], 2021	This paper provides an overview of IoT technology and its widespread use in various industries. It also discusses the security risks associated with the increasing use of IoT devices and presents recent security solutions for IoT security attacks.
5	Rasheed Ahmad, Izzat Alsmadi, [11], 2021	This paper provides a systematic literature review of recent research trends in IoT security and machine learning. The study identifies key research trends in the field and emphasizes the need to develop models that integrate state-of-the-art techniques and technologies from big data and machine learning to detect IoT attacks in real-time with accuracy and efficiency.
6	Leonardo Babun, Kyle Denney, Z. Berkay Celik, Patrick McDaniel, A. Selcuk Uluagac [12], 2021	This paper surveys popular IoT platforms, presenting a comprehensive evaluation framework based on seven technical comparison criteria: topology design, programming languages, third-party support, extended protocol support, event handling, security, and privacy. The authors analyze how different IoT platforms handle security and privacy vulnerabilities, and present possible solutions to strengthen security and privacy. The survey aims to assist IoT administrators, developers, and researchers in making informed decisions when implementing IoT solutions.
7	S. S. Gopalan, A. Raza and W. Almobaideen [13], 2020	The paper presents a survey and analysis of research on using AI for cybersecurity to protect IoT networks in healthcare. Security challenges in digital healthcare transformation are discussed, and the potential for cyberattacks to result in life-threatening consequences is highlighted. The paper identifies a niche opportunity for researchers to focus on in this space and provides a thorough analysis of related papers between 2014 and 2019.
8	L. D. Xu, Y. Lu and L. Li [14], 2021	This research paper analyzes the integration of blockchain with the Internet of Things (IoT) to enhance security, privacy, and reliability. The paper explores the suitability of blockchain's decentralization, consensus mechanism, data encryption, and smart contracts to prevent potential attacks and reduce transaction costs.

		The analysis focuses on security features, issues, technologies, approaches, and related scenarios in blockchain-embedded IoT, highlighting the potential for improving IoT security through blockchain integration.
9	Rachit, Bhatt, S. & Ragiri, P.R [15], 2021	This paper explores security challenges of currently deployed IoT standards and protocols. It provides a detailed review of IoT security aspects, covering identification of risks, security protocols, and security projects proffered in recent years. A security-specific comparative analysis of protocols, standards, and security models is presented, revealing the need for standardization at the communication and data audit level. The study highlights the need for protocols that can address multiple threat vectors and provides insights into the latest security research trends in IoT.
10	Mohanty, J., Mishra, S., Patra, S., Pati, B., Panigrahi, C.R. [16], 2021	The paper discusses security and privacy concerns in the Internet of Things (IoT) and provides a review of IoT architecture and protocols. The authors investigate security concerns associated with different IoT layers and protocols and provide possible solutions. They also suggest future directions for IoT security research.
11	Kakkar, L., Gupta, D., Saxena, S., Tanwar, S. [17], 2021	This paper provides an overview of the Internet of Things (IoT), its architecture, security conventions, and challenges. The three-layered architecture of IoT and potential security threats are discussed. The paper also reviews current scenarios and concerns of IoT security.
12	E. A. Shammar, A. T. Zahary and A. A. Al-Shargabi [18], 2021	This research paper discusses the potential of using blockchain technology for secure and decentralized Internet of Things (IoT) applications. The paper provides a comprehensive literature review of the integration of IoT and blockchain technology, highlighting current research issues and trends in the applications of blockchain-related approaches and technologies within the IoT security context. The paper also investigates the challenges and research efforts to overcome them in implementing blockchain for IoT security.
13	Ahmad, I., Saber Niazy, M., Ahmad Ziar, R., & Khan, S. [19], 2021	The growth of IoT is due to its wide range of usability, adaptability, and smartness, but security issues are a major concern. In this survey paper, the security attacks in different IoT layers are elaborated, and some IoT applications are presented. The study can help researchers and manufacturers to evaluate and decrease

		attacks on IoT devices.
14	M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani [20], 2020	This paper discusses security challenges in the rapidly developing Internet of Things (IoT) ecosystem, which currently lacks effective security measures. The authors propose the use of machine learning (ML) and deep learning (DL) methods to enhance IoT security and provide a comprehensive survey of recent advances in ML/DL methods. They review various IoT security threats and attack surfaces, as well as the opportunities, advantages, and shortcomings of ML/DL methods. This work can guide future research in IoT security.
15	Chanal, P.M., Kakkasageri, M.S. [21], 2020	The paper presents a brief overview of the Internet of Things (IoT) and its applications, highlighting the need for security and privacy measures due to the interconnection of trillions of intelligent objects. The paper reviews the major security and privacy challenges of IoT, including confidentiality, integrity, authentication, and availability, and discusses the design and development of security and privacy management schemes for resource-constrained devices like smart phones, WSNs, and RFIDs.
16	Mrabet H, Belguith S, Alhomoud A, Jemai A [22], 2020	This survey paper proposes a new compacted and optimized architecture for the Internet of Things (IoT) based on five layers and a new classification of security threats and attacks based on this architecture. The paper reviews various network and protocol technologies employed by IoT and presents solutions to security threats against them. The paper also addresses security features of IoT cloud platforms and presents future directions towards securing IoT.
17	Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos [23], 2020	This paper discusses the security challenges facing IoT platforms due to their widespread adoption and the need for dynamic security measures to address various types of attacks. Machine learning is proposed as a potential solution for detecting attacks and abnormal behavior in smart devices and networks, and the paper presents a comprehensive literature review on ML approaches for IoT security.
18	R. Yugha, S. Chithra [24], 2020	This paper surveys the challenges and open issues related to security and protocols in the Internet of Things (IoT). The paper discusses the enormous amount of data sensed by IoT devices and the use of machine learning and data analytics algorithms to process and

		predict events. It also highlights the challenges of routing information securely over the Internet with limited resources and examines research trends and simulation tools for analyzing IoT layer protocols.
19	V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar [25], 2019	This research paper discusses the security challenges and sources of threats in the Internet of Things (IoT) applications. The paper presents a detailed review of existing and emerging technologies, including blockchain, fog computing, edge computing, and machine learning, to achieve a high degree of trust and security in IoT environments. The goal is to achieve end-to-end secure IoT applications to enable automation, efficiency, and comfort for users.
20	X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao and W. Yu, [26], 2019	This paper discusses the security vulnerabilities and risks associated with the widespread adoption of IoT technologies in smart-world critical infrastructures and cyber-physical systems. The authors provide a detailed assessment of vulnerabilities from different perspectives and highlight key cyber-physical systems, including smart transportation, smart manufacturing, and smart grid. They also present a case study on potential attacks on the smart transportation system and provide best practices and countermeasures for generic IoT-based critical infrastructure systems.

The security of IoT devices has become a major concern in recent years. The vast array of devices that are connected to the internet has created a complex security landscape that is constantly evolving. As a result, researchers have been working tirelessly to create methodologies that can be used to secure these devices.

The methodologies used to secure IoT devices have evolved over time. In the early days of IoT, security was not a major concern, and as a result, many devices were shipped with default passwords and no encryption. However, as the IoT landscape has evolved, researchers have developed more sophisticated methodologies to secure these devices.

Some of the methodologies used to secure IoT devices include device authentication, encryption, and access control. Device authentication involves verifying the identity of the device before allowing it to access the network. Encryption is used to protect the data that is transmitted between the device and the network. Access control is used to limit the access that each device has to the network and the data that is stored on the network.

In addition to these methodologies, researchers are also exploring new approaches to IoT security such as blockchain technology, machine learning, and artificial intelligence. These new approaches have the potential to revolutionize the way in which we secure IoT devices and make them more resilient to cyber-attacks.

Overall, the methodologies used to secure IoT devices have come a long way in recent years. As the IoT landscape continues to evolve, it is likely that new and more sophisticated methodologies will be developed to address the security challenges posed by these devices.

4. A Comprehensive Approach to Securing IoT Devices

(i). A comprehensive approach to securing IoT devices

Securing IoT devices is a complex task that requires a comprehensive approach. It involves securing the physical device as well as the software and networks that the device is connected to. A comprehensive approach to securing IoT devices includes several key components.

Firstly, it is important to implement strong authentication and access controls for IoT devices. This involves ensuring that only authorized users or devices are able to access the device or network. This can be achieved through the use of strong passwords, biometric authentication or other means of identity verification.

Secondly, it is important to secure the communication channels that IoT devices use. This involves encrypting data in transit and ensuring that the communication channels are properly authenticated and authorized. This can be achieved through the use of secure protocols such as SSL/TLS, IPSec and SSH.

Thirdly, it is important to implement strong security measures on the device itself. This includes ensuring that the device is running up-to-date software and firmware, and that any vulnerabilities are patched as soon as possible. It is also important to ensure that the device has strong encryption and other security features built into it.

Finally, it is important to have a comprehensive security monitoring and incident response plan in place. This involves monitoring IoT devices and networks for any signs of suspicious activity, and responding quickly and effectively to any security incidents that do occur. This can be achieved through the use of security monitoring tools and techniques, and by having a well-defined incident response plan in place.

(ii)The Role of Machine Learning in IoT Security

The Internet of Things (IoT) is a rapidly growing technology that has enabled a wide range of devices to communicate with each other. While IoT has brought about many benefits, it has also opened a new avenue for cybercriminals to exploit vulnerabilities in IoT devices. This is where machine learning comes in handy in IoT security.

Machine learning is a field of artificial intelligence that focuses on developing algorithms that can learn from and make predictions on data. It can be used in IoT security to detect anomalies in the data that could indicate a potential cyber-attack. These anomalies could be patterns of data that are not typical of the device's normal behavior or a sudden increase in data traffic.

Machine learning models can also be trained to detect and prevent attacks by analyzing data from multiple sources. This could include data from the device itself, network traffic, or even external data sources. The model can then identify patterns and detect potential threats before they can cause any harm.

Another benefit of machine learning in IoT security is its ability to adapt to new threats. As cybercriminals become more sophisticated in their attacks, machine learning models can be trained to recognize these new threats and adapt accordingly.

In conclusion, machine learning plays a crucial role in IoT security by detecting anomalies, preventing attacks, and adapting to new threats. As the IoT continues to grow, it is essential that we continue to develop and implement machine learning techniques to ensure the security of IoT devices and networks.

(iii) Best Practices for Securing IoT Devices

Securing IoT devices is crucial in protecting sensitive data and ensuring the safety of your network. The following best practices can help you to secure your IoT devices:

1. Use strong passwords and change them frequently. IoT devices often come with default passwords that are easy to guess. Change these passwords immediately to something that is difficult to crack.
2. Keep your devices up to date. Manufacturers often release security patches to fix vulnerabilities. Make sure to install these updates regularly to stay protected.
3. Segment your network. By creating separate networks for your IoT devices, you can limit the impact of a security breach. This can also help to reduce the spread of malware.
4. Disable unnecessary features. Some IoT devices come with features that you may not need. By disabling these features, you can reduce the surface area for attacks.
5. Monitor your network. Use intrusion detection systems and other monitoring tools to keep an eye on your network for unusual activity. This can help you to detect and respond to attacks in a timely manner.

By following these best practices, you can help to secure your IoT devices and protect your network from cyber threats. Remember, security is an ongoing process, so make sure to stay vigilant and keep your devices up to date with the latest security patches.

(iv). Aspects of IoT Security

The security of the Internet of Things (IoT) involves protecting the network of devices connected to the internet. There are several aspects to consider when addressing IoT security, including authentication and access control, data privacy, device integrity and firmware updates, and network security. Authentication and access control ensure that only authorized users can access and control IoT devices. Data privacy involves protecting personal information collected by IoT devices. Device integrity and firmware updates ensure that devices remain secure and up-to-date with the latest security patches. Network security involves protecting the communication channels between IoT devices and other networked devices, as well as protecting against unauthorized access to the network. Overall, a comprehensive approach to IoT security requires a combination of technological and organizational measures.

1. Authentication

Authentication is a crucial aspect of IoT security, as it ensures that only authorized users can access and control IoT devices. Authentication can be achieved through various methods, such as passwords, digital certificates, and biometric authentication. It is essential to use strong and unique passwords that are not easily guessable, and regularly change them. Digital certificates provide a more secure authentication method by using public key cryptography to ensure the authenticity of the device and user. Biometric authentication, such as fingerprints or facial recognition, adds an extra layer of security to authentication. Overall, authentication is critical for preventing unauthorized access to IoT devices and protecting sensitive data.

2. Authorization

Authorization is another essential aspect of IoT security, which determines the level of access that a user or device has to IoT resources. It is important to ensure that users and devices have the appropriate level of access based on their role and responsibility. For example, an employee may need access to certain IoT devices or data, but not others. Authorization can be achieved through various methods, such as role-based access control (RBAC) and attribute-based access control (ABAC). RBAC assigns permissions based on predefined roles, while ABAC assigns permissions based on specific attributes such as time, location, and device type. A comprehensive approach to IoT security requires a combination of authentication and authorization to prevent unauthorized access and protect sensitive data.

3. Confidentiality

Confidentiality is a critical aspect of IoT security, which ensures that sensitive data transmitted between devices remains protected and not disclosed to unauthorized users. Encryption is an effective method of maintaining confidentiality by converting data into a code that can only be decrypted with a specific key. End-to-end encryption is particularly important for IoT devices, as it ensures that data is protected throughout its journey from device to device. Additionally, it is essential to use secure communication protocols, such as Transport Layer Security (TLS), to prevent unauthorized access to data in transit. Overall, confidentiality is crucial for protecting sensitive data and maintaining the trust and integrity of IoT systems.

4. Integrity

Integrity is a crucial aspect of IoT security, which ensures that data transmitted between devices is accurate and has not been tampered with. Data integrity can be maintained through various methods, such as digital signatures and checksums. Digital signatures use public key cryptography to ensure the authenticity of data and verify that it has not been modified. Checksums use a mathematical algorithm to verify the integrity of data by comparing the original checksum with the received checksum. Additionally, it is essential to regularly update device firmware and software to fix security vulnerabilities and maintain device integrity. Overall, data integrity is critical for preventing malicious attacks and maintaining the trust and reliability of IoT systems.

5. Availability

Availability is a crucial aspect of IoT security, which ensures that IoT devices and services are accessible and operational when needed. Denial of service (DoS) attacks are a common threat to availability, which can disrupt IoT systems by overwhelming them with traffic. It is important to implement security measures such as firewalls, intrusion detection systems, and network segmentation to prevent and mitigate DoS attacks. Additionally, redundancy and failover mechanisms can ensure that critical services remain operational in the event of a failure. Regular maintenance and updates can also help ensure that IoT devices remain available and operational. Overall, availability is critical for maintaining the functionality and reliability of IoT systems.

5. Privacy

Privacy is a critical aspect of IoT security, which ensures that personal information collected by IoT devices is protected and not disclosed to unauthorized users. It is essential to implement data minimization practices, such as collecting only the necessary information and storing it securely. Additionally, it is important to obtain user consent for data collection and usage and provide transparent privacy policies. Privacy-enhancing technologies such as differential privacy and homomorphic encryption can also help protect personal information. Regularly auditing and testing IoT systems can help identify potential privacy vulnerabilities and ensure compliance with privacy regulations. Overall, protecting privacy is crucial for maintaining the trust and confidence of users and ensuring the ethical use of IoT data.

6. Trust

Trust is a critical aspect of IoT security, which ensures that users have confidence in the reliability and security of IoT systems. Trust can be established through various methods, such as third-party certifications, security audits, and transparency in data usage and collection. It is essential to implement security best practices, such as secure communication protocols, data encryption, and access control, to prevent security breaches and data leaks. Additionally, it is crucial to provide timely and accurate information about security incidents and vulnerabilities and take appropriate measures to mitigate them. Overall, building trust is critical for the adoption and success of IoT systems, and it requires a comprehensive and proactive approach to security.

(v). Methods of Securing IoT security

Securing IoT devices and systems requires a comprehensive approach that involves multiple security methods. One method is network segmentation, which isolates IoT devices from other devices and networks to prevent unauthorized access. Another method is secure communication protocols, such as Transport Layer Security (TLS), which encrypts data in transit to prevent interception and tampering. Additionally, access control methods, such as role-based access control (RBAC) and attribute-based access control (ABAC), limit access to devices and data based on user roles and attributes. Regular firmware updates and security audits can also help identify and address security vulnerabilities.

1. Encryption

Encryption is a critical aspect of IoT security that ensures the confidentiality and integrity of data transmitted between IoT devices. Encryption converts data into an unreadable format using complex mathematical algorithms that can only be deciphered with a specific key. End-to-end encryption is particularly important for IoT devices, as it ensures that data is protected throughout its journey from device to device. In addition to encryption, it is essential to use secure communication protocols such as Transport Layer Security (TLS) to prevent unauthorized access to data in transit. Overall, encryption is a fundamental method for securing IoT systems and protecting sensitive data from unauthorized access and disclosure.

2. Access Control

Access control is a critical aspect of IoT security that limits access to devices and data based on user roles and attributes. Role-based access control (RBAC) and attribute-based access control (ABAC) are two common access control methods used in IoT systems. RBAC restricts access to devices and data based on predefined roles, such as administrator, user, or guest. ABAC, on the other hand, considers user attributes such as location, time of day, and device type to determine access levels. Access control helps prevent unauthorized access to IoT devices and data and limits the impact of security breaches. Overall, access control is a fundamental method for securing IoT systems and protecting sensitive data from unauthorized access and disclosure.

3. Intrusion Detection

Intrusion detection is a critical aspect of IoT security that detects and responds to security threats and attacks. Intrusion detection systems (IDS) monitor network traffic and system activity for suspicious behavior and alert administrators to potential security breaches. Host-based IDS monitors system activity on individual devices, while network-based IDS monitors network traffic between devices. Intrusion prevention systems (IPS) can also be used to automatically block malicious traffic and prevent security breaches. Regular security audits and vulnerability assessments can also help identify potential security threats and vulnerabilities. Overall, intrusion detection is a fundamental method for securing IoT systems and protecting against security threats and attacks.

4. Network Security

Network security is a critical aspect of IoT security that focuses on protecting the communication channels between IoT devices and systems. Secure communication protocols, such as Transport Layer Security (TLS), encrypt data in transit to prevent interception and tampering. Network segmentation isolates IoT devices from other devices and networks to prevent unauthorized access. Firewalls can also be used to monitor and control network traffic and prevent unauthorized access to devices and data. Regular firmware updates and security audits can help identify and address network vulnerabilities. Overall, network security is a fundamental method for securing IoT systems and protecting against security threats and attacks.

5. The Future of IoT Security

Looking forward, IoT security research needs to address several challenges and explore emerging technologies to secure IoT devices and networks. Future research should aim to develop comprehensive security frameworks that are tailored to the unique challenges of IoT environments, while minimizing the impact on performance and functionality [29]. To achieve this, researchers should explore the potential of emerging technologies such as blockchain and machine learning. For example, high-performance and scalable cryptographic schemes can be used to secure data in blockchain-based IoT systems [30]. Integration of blockchain technology, cryptographic and hashing schemes into IoT is also favored by a number of researchers [30]. Further research is needed to address security challenges in IoT that are not adequately addressed by existing solutions [29]. Additionally, privacy and security solutions for IoT are still being proposed or at conceptual levels, and there are new and promising research opportunities in the IoT security field [30][31]. Microservices-based architecture can be used to minimize security threats and attacks related to IoT data by offering extensible, reusable, and reconfigurable security features for IoT applications [31]. Ongoing challenges exist in the field of IoT security research, and identifying these flaws will help set future research directions for IoT security [31][32]. Researchers have also proposed different approaches for assessing the security of IoT devices and networks, including structuring dependencies of security to measure the implication of system security from an extensive perception, assessing platforms of IoT from application provider perceptions, and offering a framework of layer-based packet capturing for inspecting IoT devices' privacy and security [29]. Lastly, machine learning algorithms have shown substantial enactment in diverse applications and fields such as text recognition, facial recognition, and detection of spam, thus researchers can leverage these techniques to improve the ability to detect cybersecurity attacks [29].

The future of IoT security is both exciting and daunting. As more and more smart devices are connected to the internet, we are seeing an exponential increase in the amount of data being generated and transmitted through these devices. This presents significant security risks that need to be addressed.

The use of AI and machine learning will play a crucial role in the future of IoT security. These technologies will enable devices to detect and prevent security breaches in real-time, making them more secure and less vulnerable to attacks.

Another important aspect of the future of IoT security is the need for collaboration between various industries and stakeholders. This includes manufacturers, policymakers, and researchers, who need to work together to develop and implement security standards and protocols. This will help to ensure that IoT devices are built with security in mind from the ground up.

Finally, the future of IoT security will also involve the development of new technologies and methodologies to address emerging threats. This will require ongoing research and development, as well as a willingness to adapt and evolve in response to new challenges.

Overall, the future of IoT security is complex and multifaceted, but by working together and leveraging the latest technologies and methodologies, we can build a secure and sustainable IoT ecosystem for the future.

6. Conclusion and Final Thoughts on IoT Security

In conclusion, IoT security is a complex issue that requires multidisciplinary approaches to address. The proliferation of IoT devices and their interconnectedness creates a vast attack surface that can be exploited by malicious actors. Therefore, it is crucial to develop effective security solutions that can mitigate these risks and safeguard IoT systems and data.

To achieve this, researchers, policymakers, and industry stakeholders need to collaborate and share expertise and knowledge to bridge the research gap and develop robust security methodologies. This can be done through open-source collaboration, standardization of security protocols, and the development of security frameworks.

Furthermore, end-users must also play a role in securing their IoT devices by adopting best practices such as changing default passwords, updating firmware regularly, and limiting device permissions. In conclusion, IoT security is an ongoing concern that requires continuous efforts to remain vigilant and adapt to changing threats. By adopting a collaborative and proactive approach, we can ensure that IoT systems and data remain secure and can continue to benefit society in meaningful ways.

In conclusion, IoT security is a crucial component of our digital world. The research gap and methodologies discussed in our article are critical to understanding and addressing IoT security issues. We hope this article has provided you with valuable insights into the importance of IoT security and the various methodologies employed to secure IoT devices. As IoT continues to expand, it is vital that we continue to bridge the research gap and develop new and innovative security measures to keep our devices and data safe. Remember, security is not a one-time event, but a continuous process that requires ongoing attention and effort.

References

[1] Aufner, P. The IoT security gap: a look down into the valley between threat models and their implementation. Int. J. Inf. Secur. 19, 3–14 (2020). https://doi.org/10.1007/s10207-019-00445-y

[2] Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors 2022, 22, 2087. https://doi.org/10.3390/s22062087

[3] Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 2020, 12, 157. https://doi.org/10.3390/fi12090157

[4] Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics 2022, 11, 198. https://doi.org/10.3390/electronics11020198

[5] Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Nafea, I.; Ghaleb, F.A.; Saeed, F.; Nasser, M. Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. Appl. Sci. 2021, 11, 8383. https://doi.org/10.3390/app11188383

[6] Fadhil Khalid, L. ., & Y. Ameen, S. . (2021). SECURE IOT INTEGRATION IN DAILY LIVES: A REVIEW. Journal of Information Technology and Informatics, 1(1), 6–12. Retrieved from https://qabasjournals.com/index.php/jiti/article/view/23

[7] Fadhil Khalid, L. ., & Y. Ameen, S. . (2021). SECURE IOT INTEGRATION IN DAILY LIVES: A REVIEW. Journal of Information Technology and Informatics, 1(1), 6–12. Retrieved from https://qabasjournals.com/index.php/jiti/article/view/23

[8] Shivam Saxena, Bharat Bhushan, Mohd Abdul Ahad,Blockchain based solutions to secure IoT: Background, integration trends and a way forward,Journal of Network and Computer Applications, Volume 181, 2021, 103050, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2021.103050.

[9] Eduardo B. Fernandez, Hironori Washizaki, Nobukazu Yoshioka, Takao Okubo,The design of secure IoT applications using patterns: State of the art and directions for research, Internet of Things,Volume 15,2021,100408,ISSN 2542-6605,https://doi.org/10.1016/j.iot.2021.100408.

[10] X. Liang and Y. Kim, "A Survey on Security Attacks and Solutions in the IoT Network," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, 2021, pp. 0853-0859, https://doi: 10.1109/CCWC51732.2021.9376174.

[11] Rasheed Ahmad, Izzat Alsmadi,Machine learning approaches to IoT security: A systematic literature review ,Internet of Things,Volume 14,2021,100365,ISSN 2542-6605, https://doi.org/10.1016/j.iot.2021.100365.

[12] Leonardo Babun, Kyle Denney, Z. Berkay Celik, Patrick McDaniel, A. Selcuk Uluagac,A survey on IoT platforms: Communication, security, and privacy perspectives,Computer Networks,Volume 192,2021,108040,ISSN 1389-1286 , https://doi.org/10.1016/j.comnet.2021.108040.

[13] S. S. Gopalan, A. Raza and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 2021, pp. 1-6, https://doi: 10.1109/ICCSPA49915.2021.9385711.

[14] L. D. Xu, Y. Lu and L. Li, "Embedding Blockchain Technology Into IoT for Security: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10452-10473, 1 July1, 2021, https://doi: 10.1109/JIOT.2021.3060508.

[15] Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. *SN Appl. Sci.* **3**, 121 (2021). https://doi.org/10.1007/s42452-021-04156-9

[16] Mohanty, J., Mishra, S., Patra, S., Pati, B., Panigrahi, C.R. (2021). IoT Security, Challenges, and Solutions: A Review. In: Panigrahi, C.R., Pati, B., Mohapatra, P., Buyya, R., Li, KC. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 1199. Springer, Singapore. https://doi.org/10.1007/978-981-15-6353-9_4

[17] Kakkar, L., Gupta, D., Saxena, S., Tanwar, S. (2021). IoT Architectures and Its Security: A Review. In: Goyal, D., Gupta, A.K., Piuri, V., Ganzha, M., Paprzycki, M. (eds) Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-15-9689-6_10

[18] . E. A. Shammar, A. T. Zahary and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," in IEEE Access, vol. 9, pp. 156114-156150, 2021, https:// doi: 10.1109/ACCESS.2021.3129697.

[19] Ahmad, I., Saber Niazy, M., Ahmad Ziar, R., & Khan, S. (2021). Survey on IoT: Security Threats and Applications. *Journal of Robotics and Control (JRC), 2*(1), 42-46. doi: https://doi.org/10.18196/jrc.2150

[20] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, https:// doi: 10.1109/COMST.2020.2988293.

[21] Chanal, P.M., Kakkasageri, M.S. Security and Privacy in IoT: A Survey. *Wireless Pers Commun* **115**, 1667–1693 (2020). https://doi.org/10.1007/s11277-020-07649-9

[22] Mrabet H, Belguith S, Alhomoud A, Jemai A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*. 2020; 20(13):3625. https://doi.org/10.3390/s20133625

[23] Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos,Machine learning based solutions for security of Internet of Things (IoT): A survey,Journal of Network and Computer Applications,Volume 161,2020,102630,ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102630

[24] R. Yugha, S. Chithra,A survey on technologies and security protocols: Reference for future generation IoT,Journal of Network and Computer Applications,Volume 169,2020,102763,ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2020.102763..

[25] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in *IEEE Access*, vol. 7, pp. 82721-82743, 2019, https://doi: 10.1109/ACCESS.2019.2924045.

[26] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao and W. Yu, "Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities," in *IEEE Access*, vol. 7, pp. 79523-79544, 2019, https://doi: 10.1109/ACCESS.2019.2920763.

[27] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, https://doi: 10.1109/ACCESS.2019.2924045.

[28] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020, https:// doi: 10.1109/COMST.2019.2962586.

[29] Zitian Liao, Shah Nazir, Habib Ullah Khan, Muhammad Shafiq, "Assessing Security of Software Components for Internet of Things: A Systematic Review and Future Directions", Security and Communication Networks, vol. 2021, Article ID 6677867, 22 pages, 2021. https://doi.org/10.1155/2021/6677867

[30] Alfa, A.A., Alhassan, J.K., Olaniyi, O.M. et al. Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions. J Reliable Intell Environ 7, 115–143 (2021). https://doi.org/10.1007/s40860-020-00116-z

[31] Maha Driss, Daniah Hasan, Wadii Boulila, Jawad Ahmad,Microservices in IoT Security: Current Solutions, esearch Challenges, and Future Directions,Procedia Computer Science,Volume 192,2021,Pages 2385-2395,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2021.09.007.

[32] Muhammad Adil, Muhammad Khurram Khan, Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions, Sustainable Cities and Society, Volume 75, 2021,103311,ISSN 2210-6707,https://doi.org/10.1016/j.scs.2021.103311.