Internet of Things: Security Aspects & Emerging Technologies

Parvati Sharma

GBBS Institute, India

ABSTRACT

This survey aims to explore the security in Internet of Things (IoT). We focused on the impact of emerging technologies, such as 5G, the Industrial Internet of Things, blockchain, and artificial intelligence, on IoT security. We surveyed IT professionals from various sectors, including government, defense, healthcare, finance, transportation, and manufacturing. The survey uncovered several key findings about the current state of security in IoT. We found that: • Most organizations are unprepared for the security risks posed by emerging technologies in IoT. Only 55% of organizations have implemented appropriate security measures to protect their data in IoT. • Despite the security risks posed by emerging technologies in IoT, organizations lack sufficient investment in security measures. More than 50% of respondents cited lack of funding as the major obstacle towards implementing security measures. • Organizations largely lack the knowledge required to secure their data in IoT. Over 80% of the respondents indicated that their organization requires further training in security topics. Overall, our survey findings suggest that organizations are far from ready to address the security concerns posed by emerging technologies in IoT. We strongly recommend that organizations invest in the implementation of appropriate security measures and ensure that their teams are adequately trained to properly address security threats.

Keywords: IoT, Security & Privacy, Sensors, Machine Learning, Security Solutions

INTRODUCTION

The Internet of Things (IoT) refers to the network of interconnected devices, software applications, and physical objects that are able to communicate and interoperate with each other. While this can be a great benefit, it also brings with it a host of security issues [1]. Firstly, the data being connected is potentially more vulnerable to attack, as hackers are more likely to be able to access and exploit the systems and databases involved. Secondly, connected devices can be more vulnerable to hijacking, as the increased complexity of IoT systems allows for more ways for an attacker to access information and control systems [2]. Thirdly, the sheer number of connected devices and data sources can be overwhelming for security teams to manage, increasing the chances of a breach or malicious activity going unnoticed. Finally, the high degree of automation present in IoT networks can also result in certain security threats going undetected, or not being properly addressed [3].

To address these issues, organizations should take steps to secure their IoT networks. This includes using secure mechanisms to connect and authenticate all devices, controlling data flow between devices, and continuously monitoring the environment for any potential threats. Additionally, organizations should also ensure that all devices are updated with the latest security patches, detect any unauthorized activity, and limit physical access to the IoT infrastructure [4]. In order to protect the data, systems, and networks that make up the Internet of Things, security measures must be taken at every stage of the IoT process. This includes in the manufacturing stage, where the physical devices must be designed with security features in mind, and in the configuration and maintenance stages, where steps must be taken to ensure that the networks and devices are correctly set up and securely maintained over time [5]. It also includes addressing the threat of network intrusions by strengthening the visibility and control of the network, detecting and addressing any malicious activity, and preventing data breaches by implementing unified threat protection measures. Finally, organizations should also look to develop security policies and practices that are designed to not only protect the network and data, but to also ensure that the user's privacy and security are maintained [6].

At the manufacturing stage, IoT devices must include physical features and embedded software that ensure the networks and devices are secure. This includes the use of secure boot protocols to authenticate software updates, and the encryption of firmware and data [7]. Additionally, depending on the context and implementation of the IoT, components such as communications protocols, authentication, secure key stores, and secure messaging protocols may also be required. The configuration and maintenance stages of the IoT process are also critical steps to ensure secure operation. This includes securely configuring and deploying devices, software updates, and network settings [8]. Additionally, passwords, user access control, proper authentication, secure and constantly monitored network firewalls, and a robust monitoring system must also be in place [9]. Organizations should also develop security policies and best practices that address all aspects of the secure use of the IoT, such as user access control, data protection, and privacy protocols, bug repair and patch management, backup and recovery measures, and update processes. Finally, should an attack or breach occur, organizations must have the measures in place to detect and respond to it, while also limiting the potential scope of an attack [10].

IoT security is essential for a number of reasons. Firstly, as IoT devices are often used to access or store sensitive data, strong security protocols are necessary to prevent unauthorized access or manipulation of this data [11]. Secondly, if an IoT device or network is accessed or compromised, the results could be disastrous, from data theft to malicious actions such as Distributed Denial of Service (DDoS) attacks. Finally, IoT devices are often used to control and monitor physical processes, such as smart home and industrial automation systems, and having strong security in place allows these functions to be carried out without fear of interruption or manipulation [12]. There are a number of different measures that need to be taken to ensure the security and reliability of IoT devices and networks. Firstly, all components should be rigorously tested and verified, and all protocols and communication methods should be secured to ensure data protection. Secure boot protocols, encryption, secure communication channels, and authentication systems can all be integrated into the device to ensure they are kept secure [13].

Additionally, organizations must have the necessary responses in place should an attack or breach occur, such as an Incident Response Plan to limit the scope of the attack. Finally, organizations must establish security policies and best practices that address secure use of the IoT, such as data protection, policy and procedures for bug repair and patch management, and backup and recovery measures [14]. These measures can go a long way in ensuring the security and reliability of IoT networks and devices. More comprehensive security measures for IoT devices and networks include the implementation of monitoring and security software to detect suspicious activity, the implementation of secure access protocols, network segmentation and virtualization, the implementation of a digital identity management system, the implementation of encryption algorithms, secure edge devices, secure web traffic and secure coding practices [15]. Additionally, organizations must ensure secure patch management and secure updating of their IoT devices. Organizations must also utilize IT asset management software to enable secure control and visibility of the devices and software on the network and secure backups to enable rapid recovery in case of incident [16]. Finally, organizations should consider implementing secure identity trust frameworks, such as blockchain and identity access governance systems, to authenticate identity and grant access to prioritized functions. By taking these steps, organizations can ensure secure and reliable IoT networks and devices [17].

IoT Security Threats

IoT security threats refer to malicious activities aimed at gaining unauthorized access to the IoT systems, such as smart homes and connected vehicles, by exploiting the vulnerabilities in their unprotected networks and system architecture [18]. These threats are typically targeted at exploiting weak points in the system architecture and networks to gain access to the data or control over the system. These attacks can be carried out at the network, application, or device layer. Some common examples of IoT security threats are device hijacking, distributed denial of service (DDoS) attacks, man-in-the-middle (MITM) attacks, unauthorized data manipulation, and malicious firmware updates [19]. To mitigate these risks, organizations and users should implement strong authentication systems, use secure protocol techniques and encryption, and ensure proper segmentation of the network. Additionally, it is important to keep firmware and system components updated and patched, as well as auditing and monitoring systems for suspicious or malicious activities. 1. Network-level threats.2. Application-level threats. 3. Device-level threats. 4. Unauthorized Data Manipulation. 5. Malicious Firmware Updates [20,21].

Network-level threats are malicious activities that originate from the network infrastructure, such as a hacker trying to gain access to a closed network. Examples of this type of threat can include IP spoofing, which is the practice of forging an IP address to appear to originate from a trusted source, malicious malware such as worms, viruses, Trojans, and rootkits, brute force attacks, phishing attacks and distributed Denial of Service (DDoS) attacks. Other examples of network-level threats include man-in-the-middle attacks, ARP poisoning, spoofing of MAC addresses, DNS poisoning, SYN floods and other forms of DoS attacks, and infiltration through open ports and vulnerable services. These threats are designed to disrupt the network by accessing sensitive data, disabling network services and potentially gaining access to other networks and systems [22].

Application-level threats are malicious activities that target applications and the data that is stored within them. These threats can compromise various data and components, depending on the application that is being targeted. Examples of application-level threats include SQL injection attacks, cross-site scripting, malicious code execution, buffer overflow attacks, malicious remote access, and data manipulation. Other examples include bypassing authentication protocols, credential theft, malware infection, data harvesting, and data exfiltration. These threats can cause serious damage to the integrity of both the data and software running on the targeted application, and can also be used to gain access to other applications or networks. Device-level threats are malicious activities that target the hardware components of connected devices [23]. Such threats include hardware tampering, hardware theft, tampering with firmware, and hardware disruption. These threats can not only disrupt or steal data, but can also render machines useless. More sophisticated threats, such as hardware Trojans, are also possible. Hardware Trojans are malware that is designed to stay hidden on devices and intercept sensitive data while avoiding detection. Additionally, hardware Trojans can be used to steal data from devices, spy on the user, gain access to networks, and disrupt operations. Such threats are becoming increasingly sophisticated, and can do a great deal of damage if not identified and addressed in time [24]. Unauthorized data manipulation refers to malicious activities that target the data stored on a device. This could include attacks that modify, delete, or corrupt data that is stored either on the device or in an external location. These attacks can range from unauthenticated users changing data within the system to sophisticated, targeted attacks that are designed to manipulate specific data. While this type of attack can be done physically, it is more commonly done via malware, such as ransomware. In some cases, attackers may use more nefarious methods such as inserting malicious code into the data, allowing them to further manipulate the data or gain access to the system. Unauthorized data manipulation can lead to the loss of valuable data or even to personal harm if the data is sensitive in nature. In order to defend against such threats, organizations should ensure that their devices and systems are properly secured and that they are regularly monitored for suspicious activity. In addition, employees should receive regular training on data security best practices, as well as investigating any suspicious incidents that may occur [25].

Malicious firmware updates refer to malicious firmware or software updates created by attackers to exploit security vulnerabilities in a device. These malicious updates are designed to infect the device, allowing the attacker access to the device’s data and even control over its functions. They can also be used to spread malware, exfiltrate data, or even interfere with device operations. In order to effectively defend against malicious firmware updates, organizations should ensure that their firmware and applications are regularly updated and patched. This should also be done for endpoints that are not connected to the corporate network, as these systems can be vulnerable to attack as well [26]. Additionally, organizations should take steps to ensure that only authorized personnel can install updates, by using authentication protocols such as two-factor authentication. Further, organizations should ensure that their network and systems are regularly monitored for any suspicious activity related to firmware updates and security vulnerabilities. Finally, any employee-issued device should be regularly scanned for malware and malicious software, to identify and prevent any malicious firmware updates before they can do any harm [23,24].

IoT security solutions

IoT security solutions are a variety of different tools and practices that organizations can use to protect their Internet of Things (IoT) devices and networks from malicious actors and malicious activities. These solutions involve a combination of hardware and software, such as Network Segmentation and Virtualization, Encryption and Identity Access Governance, secure access protocols, secure web traffic and secure coding practices, secure patch and update management, secure edge devices and firewalls and secure monitoring and logging solutions [27].

Network segmentation and virtualization help to isolate the IoT devices and networks to prevent unknown users from gaining access. Secure access protocols help to ensure that only authorized users can access the IoT, and there are various encryption algorithms available to protect data transmitted between the various elements. Identity access governance solutions are also available to provide authentication and authorization to access certain network functions and data.

Secure web traffic and coding practices ensure that if the IoT devices are connected to the internet, the data is protected from unauthorized access and manipulation. Secure patch and update management ensures that devices are protected from the latest vulnerabilities and malware, and secure edge devices and firewalls are used to prevent external attacks from succeeding. Finally, secure monitoring and logging help to detect and respond to any malicious activities or intrusions. By implementing these security solutions, organizations can reduce the risk of their IoT devices and networks from becoming compromised or attacked. The selection of appropriate IoT security solutions will depend on the complexity of an IoT environment, the types of data and devices connected, and the security risks that need to be addressed [28]. The following are examples of some of the most common security solutions available today:

Network Segmentation and Virtualization: Network segmentation helps protect IoT networks, isolating critical components and important data in order to reduce the risk of unauthorized access. Virtualization can further isolate IoT devices, allowing them to be used in a more secure and controlled manner.

- **Encryption and Identity Access Governance:** Encryption algorithms prevent data from being read in an unencrypted form and protect data confidentiality. Identity access governance provides secure authentication and authorization for users to access certain network functions or data.

- **Secure Access Protocols:** Secure access protocols help to ensure that only authenticated users can access the IoT and associated data. Examples of secure access protocols that organizations use to secure their IoT environment are Transport Layer Security (TLS), Secure Socket Layer (SSL) and IPSec.

• **Secure Web Traffic:** When web applications and services are used with an IoT environment, establishing secure web traffic helps protect against malicious actors. This includes encrypting web traffic, using secure web servers, disabling unnecessary services and more.

• **Secure Coding Practices:** Secure coding practices help to ensure that code is developed in a safe and secure manner. Common practices include avoiding security vulnerabilities, testing code before deployment and employing secure code review processes.

• **Secure Patch and Update Management:** Keeping software up to date with security patches and new releases helps to protect IoT devices from the latest threats. This requires a patch and update strategy to ensure systems are kept up to date with the latest security patches and changes.

• **Secure Edge Devices and Firewalls:** Edge devices such as routers and firewalls can help protect IoT networks from malicious external threats. Firewalls are hardware-based solutions that inspect and filter all the incoming and outgoing traffic on a network, helping to block malicious traffic.

• **Secure Monitoring and Logging:** Monitoring and logging IoT networks and devices helps detect and respond to any malicious activities or intrusions. Examples of security monitoring include using Intrusion Detection Systems (IDS) and Behavior Anomaly Detection (BAD) [29].

CONCLUSION

As the need for data security in the IoT environment continues to increase, organizations should look to a wide range of security solutions available to ensure their data, devices and networks are adequately protected. The solutions discussed in this article are just a few of the many options available and should be studied in greater detail to understand which solution best fits individual IoT needs. organizations should consider the following security solutions: Network security solutions: Security solutions that network administrators can use to monitor and protect data, devices and networks from unauthorized access. These include firewalls, antivirus software, and intrusion detection systems. Secure communications protocols: Encryption protocols and authentication methods for data communications, such as Transport Layer Security (TLS), should be implemented to ensure data privacy and integrity. Data and application security solutions: Data should be securely stored and transmitted, and applications should be monitored and patched regularly to reduce risk of attack. Solutions such as database encryption, access control systems and application firewalls can help to secure data and applications. Device security solutions: Security measures should be integrated into the design of the IoT device and could include hardware-based security measures, secure boot systems, secure software update mechanisms, and identity and access control systems. Risk assessments: Risk assessments should be conducted to identify potential threats and vulnerabilities in an organization’s network or IoT system. A periodic risk assessment can help to identify any weaknesses in current security measures and allow organizations to update or implement new security solutions to reduce risk. Organizations should also look to involve experts in the implementation and management of IoT security solutions. Organizations may want to consider hiring a security consultant or security service provider to design and implement an effective security policy and strategy. Additionally, regular security updates and best practices should be implemented on an ongoing basis to keep up with new threats and risks.

REFERENCES

[1]. Rathore, R.S., Sangwan, S., Kaiwartya, O. and Aggarwal, G., 2021. Green communication for next-generation wireless systems: optimization strategies, challenges, solutions, and future aspects. *Wireless Communications and Mobile Computing*, *2021*, pp.1-38.

[2]. J. H. Ruan, H. Jiang, C. S. Zhu, X. P. Hu, Y. Shi, T. J. Liu, W. Z. Rao, and F. T. S. Chan, “Agriculture IoT: Emerging trends, cooperation networks, and outlook,” *IEEE Wirel. Commun.*, vol. 26, no. 6, pp. 56–63, Dec. 2019. doi: 10.1109/MWC.001.1900096

[3]. Rathore, R.S., Sangwan, S. and Kaiwartya, O., 2021. Towards Trusted Green Computing for Wireless Sensor Networks: Multi Metric Optimization Approach. *Adhoc & Sensor Wireless Networks*, *49*.

[4]. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, “Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges,” *IEEE Access*, vol. 8, pp. 32031–32053, Feb. 2020. doi: 10.1109/ACCESS.2020.2973178

[5]. Rathore, R.S., Sangwan, S., Adhikari, K. and Kharel, R., 2020. Modified echo state network enabled dynamic duty cycle for optimal opportunistic routing in EH-WSNs. *Electronics*, *9*(1), p.98.

[6]. G. Fortino, W. Russo, C. Savaglio, W. M. Shen, and M. C. Zhou, “Agent-oriented cooperative smart objects: From IoT system design to implementation,” *IEEE Trans. Syst. Man Cybernet.:Syst.*, vol. 48, no. 11, pp. 1939–1956, Nov. 2018. doi: 10.1109/TSMC.2017.2780618

[7]. Rathore, R.S., Sangwan, S., Mazumdar, S., Kaiwartya, O., Adhikari, K., Kharel, R. and Song, H., 2020. W-GUN: Whale optimization for energy and delay-centric green underwater networks. *Sensors*, *20*(5), p.1377.

[8]. M. H. Ghahramani, M. C. Zhou, and C. T. Hon, “Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services,” *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 6–18, Jan. 2017. doi: 10.1109/JAS.2017.7510313

[9]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. *International Journal of Computer Applications*, *61*(19).

[10]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. *J. Comput. Eng. Intel. Syst*, *3*(7), pp.32-41.

[11]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. *IUP Journal of Computer Sciences*, *4*(3).

[12]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. *International Journal on Computer Science and Engineering*, *2*(3).

[13]. Rathore, R.S., Sangwan, S., Prakash, S., Adhikari, K., Kharel, R. and Cao, Y., 2020. Hybrid WGWO: whale grey wolf optimization-based novel energy-efficient clustering for EH-WSNs. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), pp.1-28.

[14]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. *IJCST*, *6*, pp.93-95.

[15]. Kumar, V. and Rathore, R.S., 2018, October. Security issues with virtualization in cloud computing. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 487-491). IEEE.

[16]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. *International Journal of Computer Applications*, *119*(2).

[17]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, August. Information Technology Architectures for Grid Computing and Applications. In *2009 Fourth International Multi-Conference on Computing in the Global Information Technology* (pp. 52-56). IEEE.

[18]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. *International Journal of Computer Applications*, *1*(13), pp.26-31.

[19]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In *2009 Second International Conference on Emerging Trends in Engineering & Technology* (pp. 1143-1150). IEEE.

[20]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. *International Journal of Computer Applications*, *116*(19).

[21]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. *International Journal of Computer Applications*, *138*(8).

[22]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. *International Advanced Research Journal in Science, Engineering and Technology*, *3*(4), pp.83-86.

[23]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.

[24]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. *Recent Developments in Computing and Its Applications*, p.155.

[25]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. *International Research Journal of Engineering and Technology (IRJET)*, *4*(5), pp.153-155.

[26]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. *International Journal on Computer Science and Engineering*, *2*(5), pp.1439-1444.

[27]. Bali, V., Rathore, R.S. and Sirohi, A.,2010. Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11). *International Journal of Computer Science & Communication*, *1*(1), pp.25-28.

[28]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. *International Journal Of Engineering Development And Research*.

[29]. Bhatnagar, D. and Rathore, R.S.,2015. CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES. *International Journal of Advance Research in Science And Engineering*, *4*(01), pp.683-690.