International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 11 | November - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Survey on Security issues of IOT

Harshitha Diwakar

Abstract- The Internet of Things (IoT) is a network of uniquely identifiable embedded devices embedded with the software needed to communicate between transients. The purpose of this study is to explore individual IoT security challenges related to IoT standards and protocols currently in use. We presented in this study a detailed review focusing on upcoming IoT security aspects, including identifying risks associated with existing IoT systems, new security protocols, and recently proposed security projects. This work provides an updated IoT architecture review of the protocols and standards provided for next-generation IoT systems. A specific comparative security analysis of protocols, standards, and professional security models is presented according to IoT security requirements. This study shows the need for standardization at the communication and data audit level, which exposes the hardware, software and data to various threats and attacks. Our study shows the need for protocols that are competent enough to address more than one threat vector. In this paper, a detailed review of the security challenges and sources of the Threat in IoT applications is presented. After discussing the various emerging and existing security issues Technologies aimed at achieving a high level of trust in IoT applications are discussed, which will be beneficial in the development of IoT security.

Index Terms- IOT- Internet of Things, Security, Protocol, AI-Artificial Intelligent

1. INTRODUCTION

Recently, the entire network field is undergoing a major technological revolution. Network automation is a hot topic that has been around for quite some time. Adding to it is Internet of Things (IoT) technology, which paves the way for providing that element. The Internet of Things is defined as the interface environment built up by the devices that focus on three important tasks – transmitting data, receiving data, and processing received data. Initially, IoT was considered a network of local physical devices connected to the internet for real-time data analysis. Over time, the scale of it has expanded itself from the local workstation to Industrial IoT frameworks. Research works on it show the proliferation of it in the field of healthcare, industrial setting, business analytics, education, etc. In the future, it is expected that the devices will not only be connected to the Internet and other local devices but also to communicate directly with other devices on the Internet. Apart from the devices or things being connected, the concept of social IoT (SIoT) is also emerging. SIoT will enable various social networking users to be connected to the devices and users can share the devices on the Internet. In any IoT ecosystem or environment, there are four important layers. The first layer includes the use of various sensors and actuators to detect the data or information to perform various functionalities. Based on that, in the second layer, a communication network is used to transmit the collected data. Most emerging IoT applications deploy a third layer, called a middleware layer, to act as a bridge between the network and the application layer. Finally, on the fourth layer, there are various IoT-based end-to-end applications such as smart grids, smart transportation, smart factories, etc. All four of these layers have specific security problems. Apart from these layers, various gateways connect these layers and help in data movement. There are certain security threats specific to these gateways as well.

1.1 Research Challenges

The main objective of this research work is to investigate the latest security solutions in the IoT. Apart from this main goal, the sub-goals include identifying and characterizing the latest security risks in the IoT. Before that, it is important to address the recent research challenges in IoT, such as the issue of Heterogeneity, Interconnectivity, Ubiquitous Nature, the issue of security standards, Technical Areas Trends like Artificial Intelligence like fuzzy logic modules based on Machine Learning, and Networking Enabled Software. Be the emerging field of research to integrate IoT. A significant development in IoT is the ultra-lightweight protocols which are also implemented for performance and security reasons. Research related to the security challenges of IoT covers a wide area, and it is changing every day, with new loopholes being revealed regularly. Today, when we talk about IoT security, the main emphasis is placed on the access control methods, the encryption methodologies used for transient steps, and hardware-specific security solutions, and input-based attack controls SQL. Therefore, our research highlights the ever-changing security perspectives through IoT implementation. Safety problems, correct definitions, classification, and the search for a solution to the present situation against them. Level, which indicates the vulnerabilities at the hardware and software levels. The verifications also demonstrated the need for sufficient protocols to accommodate more than one threat vector. The research findings can help the IoT research community by integrating the safest and most appropriate security features into IoT-based devices.

2. Literature review

Wireless network with embedded networking capability is the current Industrial trend worldwide. IoT is one of the main gainers of this networking domain. It has undergone a significant development by integrating Cloud services, providing SaaS, IaaS, and PaaS. IoT Commercial sectors have seen a major boom in the market during the last few years, as smart system demands grew manifold because of its rich feature and one-click-away services. Smart systems like Smart Home appliances, AI-based smart devices, smart home automation, smart vehicles, smart labs, etc., offer ease of living but too much dependability on them often leads to high risks. It is observed that threat structure is not confined to a particular layer in IoT architecture. Former network practices of integrating network security features in IoT have/had degraded IoT systems' performance. Table 3 comprises a set of recent novel models proposed in the wake of advanced threat reports coming for IoT. We have defined the security parameter concerning which certain research work offers a security model pertaining to conventional security models. The conventional model issue was—Inter-Compatibility among security tools deployed for IoT devices as they differed in Policy and implementation techniques and lack of Low- Powered device algorithms. Recent research has proposed novel solutions using a different plethora of encryption methods and hardware-based methods to overcome conventional security issues. Table 1 discusses some of these significant security models currently in research.

Xin Zhang and Feng tong Wen propose a new anonymous user WSN authentication for the Internet of Things that builds two algorithmic models UDS (user-server-device) and USD (user-server-device), to ensure valid authentication to prevent the threat solution. This is a versatile method to provide security during the authentication process with lighter storage overheads, efficient communication costs, and faster computational speed.

This work is limited in terms of the amount of security solution provided, except for the light detection devices against visible network layer and attacks based on physical layer. A cluster-based fuzzy logic implementation model has been proposed by Mohammad Dahman Alshehri and Farookh Khadeer Hussain and A secure messaging paradigm between IoT nodes where encrypted communication takes place using hexadecimal values to address port sweep threats and other specific security vulnerabilities for IoT security solutions based on the A.I. This work effectively provides the detection mechanism against the malicious IoT nodes in the network, but risks related to the surface of the data inspection attack are not covered in this model. This study also does not address the performance analysis of the communication and calculation costs that occur during implementation. Regarding Industrial IoT, Munkenyi Mukhandi et al. discusses the new safety solution for robotic communication from an industrial IoT point of view, using MQTT protocols and a robotic operating system. Two main methods - data encryption and authentication have been used to this end, which have shown their efficacy in the security of communication steps. This work provides invaluable insight into the efficiency of cryptographic methods in securing communication channels. In contrast, this study details the difference between performance metrics and cryptographic features. Deep learning and machine learning have made their way into the IoT environment and the main products are Alexa, Echo, which overcomes the text commands and accepts voice commands for action on a real-time basis.

3. Security challenges

Smart Environment: Smart environment includes various IoT applications such as fire detection in forests, snow level monitoring in high altitude regions, landslide prevention, early detection of earthquakes, pollution monitoring, etc. All of these IoT applications are closely linked to the lives of individuals and animals in these areas. Government agencies involved in these areas will also be supported by information from these IoT applications. Security breaches and vulnerabilities in any area related to such IoT applications can have serious consequences. In this context, false negatives and false positives can lead to devastating outcomes for these IoT applications. For example, if the application begins to falsely detect earthquakes, this will result in monetary losses for the government and businesses. On the other hand, if the application is unable to predict the earthquake, then it will result in the loss of both property and life. Therefore, intelligent environmental applications must be very precise, and security breaches and data tampering must be avoided.

Smart Metering and Smart Grids: Smart metering includes various measurement, monitoring and management functions. The most common implementation of smart meters is smart grids, where electricity usage is measured and controlled. Smart metering can also be used to address the problem of electricity theft. Other smart metering applications include monitoring water, oil and gas levels in storage tanks and cisterns. Smart meters are also used to monitor and optimize the performance of solar energy plants by dynamically changing the angle of the solar panels to harvest the most possible solar energy. There are also IoT applications that use intelligent meters to measure water pressure in water transportation systems or to measure the weight of goods. However, smart metering systems are vulnerable to both physical and cyber-attacks compared to analog meters that can only be tampered with through physical attacks. In addition, smart meters or Advanced Metering Infrastructure (AMI) are designed to perform functions other than recording generic energy usage. In a smart home area network (HAN) all electrical equipment in the home is connected to a smart meter and the information collected from this equipment can be used for load and cost management. The consumer or offender may intentionally interfere with these communication systems to alter the information gathered, which may result in monetary loss to service providers or consumers.

Security and Emergencies: Another important domain is security and emergencies where diverse IoT applications are deployed. It includes applications like allowing only authorized people in restricted areas, etc. Another application in this area is the detection of hazardous gas leaks in industrial areas or in areas around chemical factories. Radiation levels can also be measured in the areas around nuclear power reactors or cellular base stations

and alerts can be generated when the radiation level is high. There are various buildings that have sensitive data in their systems or contain sensitive items. Security applications can be deployed to protect sensitive data and goods. IoT applications that sense various liquids can also be used to prevent corrosion and breakdown in such sensitive buildings. Security breaches in such applications can also have various serious consequences. For example, the criminals may try to enter the restricted areas by attacking the vulnerabilities in such applications. In addition, false radiation level alarms can have serious effects both immediately and in the long term. For example, if infants are exposed to high levels of radiation, they can develop serious and potentially fatal diseases in the long run.

Home Automation: Home automation is one of the most widely used and deployed IoT applications. This includes applications such as those associated with the remote control of electrical appliances to save energy, systems deployed on windows and doors for intruders, etc. and detecting resources. Intrusion is detected by comparing the user's activities at key locations in the home with the user's normal behavior in those locations. However, attackers may obtain unauthorized access to IoT devices at home and attempt to harm users. For example, cases of home burglary have increased rapidly following the use of various home automation systems. There have also been various cases in the past where the monitors try to analyze the type and amount of Internet traffic to/from the smart home to assess the behavior and the presence of the residents.

Submitted paper. Selected paper get published (online and printed) in their periodicals and get indexed by number of sources.

IOT SECURITY USING BLOCKCHAIN: Blockchain and IoT are important technologies that will significantly impact the IT and communications industry. Both technologies are designed to improve overall transparency, visibility, and comfort and user confidence. The IoT devices provide real-time data from sensors and blockchain provides the key to data security using a distributed, decentralized and shared ledger. The basic idea behind blockchain is simple: it is a distributed registry (also referred to as replicated log files). The entries in the block chain are chronological and time-stamped. Each entry in the ledger is tightly coupled with the previous entry using cryptographic hash keys. The miners do not know the identity of the owners of the transactions. Over and above, there are multiple miners working on the same set of transactions, and there is strong competition between them to add the transactions to the blockchain. All these unique features enable the blockchain to be robust.

4. CONCLUSION

In this survey, we presented various security threats at different layers of the IoT application. We have covered the issues related to the sensor layer, network layer, middleware layer, gateways, and application layer. We have also discussed existing and upcoming solutions to IoT security threats including blockchain, fog computing, edge computing, and machine learning. Various open issues and issues arising from the solution itself were also discussed. The state of the art in IoT security was also discussed along with some of the future research directions to improve IoT security levels. This survey is expected to be a valuable resource for improving security for upcoming IoT applications.

REFERENCES

[1] Ashton K (2009) That Internet of Things thing. RFID J 22:97–114

[2] Wan J, Tang S, Shu Z, Li D, Wang S, Imran M, Vasilakos AV (2016) Software-defned industrial internet of things in the context of industry. IEEE Sens J 16(20):7373–7380

[3] Mavrogiorgou A, Kiourtis A, Perakis K, Pitsios S, Kyriazis D (2019) IoT in healthcare: achieving interoperability of high-quality data acquired by IoT medical devices. Sensors 19(9):1978

[4] Lemayian JP, Al-Turjman F (2019) Intelligent IoT communication in smart environments: an overview. In: Artifcial Intelligence in IoT. Springer, Cham, pp 207–221

[5] Mukhandi M, David P, Pereira S, and MS Couceiro (2019) A novel solution for securing robot communications based on the MQTT protocol and ROS. In: IEEE/SICE International Symposium on System Integration (SII), pp 608–613

[6] Rutten E, Marchand N, Simon D (2017) Feedback control as MAPE-K loop in autonomic computing. Software engineering for self-adaptive systems III Assurances. Springer, Cham, pp 349–373

[7] Sinh D, Le LV, Lin BSP, Tung LP (2018) SDN/NFV—a new approach of deploying network infrastructure for IoT. In: Wireless and optical communication conference (WOCC), IEEE, 27th, pp 1–5

[8] Safkhani M, Bagheri N (2017) Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. J Supercomput 73(8):3579–3585.

[9] Coman FL, Malarski KM, Petersen MN, Ruepp S (2019) Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT. In: 2019 Global IoT Summit (GIoTS), IEEE, pp 1–6

[10] Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH (2019) Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access 7:7273–7285

[11] Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M (2020) Internet of Things (IoT) enabling technologies, requirements, and security challenges. Advances in data and information sciences. Springer, Singapore, pp 119–126

[12] Wang Li, Dinghao Wu (2019) Bridging the gap between security tools and SDN controllers. ICST Trans Secur Saf 5(17):156242

[13] Urla PA, Mohan G, Tyagi S, Pai SN (2019) A novel approach for security of data in IoT environment. In: Computing and network sustainability. Springer, Singaporem, pp 251–259

[14] Abdul-Ghani Hezam A, Konstantas D, Mahyoub M (2018) A comprehensive IoT attacks survey based on a building-blocked reference model. Int J Adv Comput Sci Appl 9:355–373

[15] D. F. Rajesh Kandaswamy, "Blockchain-based transformation," https://www.gartner.com/en/doc/3869696-blockchain-basedtransformation-a-gartner-trend-insight-report/, online; accessed June. 5, 2018.

[16] Gsma, "Safety, privacy and security," https://www.gsma.com/ publicpolicy/resources/safetyprivacy-security-across-mobileecosystem/, online; accessed 29 January 2019.

[17] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," IEEE Access, vol. 6, pp. 32 979– 33 001, 2018.

[18] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: present and future challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, 2018.

[19] Flashpoint, "Mirai Botnet Linked to Dyn DNS DDoS Attacks," https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linkeddyn-dns-ddos-attacks/, online; December. 18 ,2018.

[20] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, "Iot-based remote pain monitoring system: From device to

cloud platform," IEEE journal of biomedical and health informatics, vol. 22, no. 6, pp. 1711–1719, 2018.

[21] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, 2017.

[22] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," IEEE access, vol. 6, pp. 6900–6919, 2018.

[23] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[24] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, Oct 2017.

[25] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future iot: A survey," IEEE Access, vol. 5, pp. 8956–8977, Mar 2017.

[26] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "Iot middleware: A survey on issues and enabling technologies," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1–20, Feb 2017.