International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Mitigating the Security Risks of IoT Devices using IPv6

Praveen Misra[1], Dr. Rajeev Yadav[2]

Senior Scientist, Education and Research Network
Ph.D. Scholar from the department of Computer Science and Application of Sri Krishna University, Chhatarpur, MP, India
Email: *dr.misrap[at]gmail.com*

Professor, Department of Computer Science and Application, Sri Krishna University, Chhatarpur, MP India
Email: *rajeevtpo[at]gmail.com*

Abstract: ***Numerous IoT devices are now present in many areas of our living environment as a result of the development of the Internet of Things (IoT) technology, which has many positive effects on our lives. The vast majority of IoT devices, however, were widely deployed without adding security by design at the time of development in order to respond to the IoT market's quick changes. As a result, IoT devices have been the target of hostile attackers who have also compromised IoT devices without security safeguards, leading to several security incidents. In particular, a hacker can take control of an IoT device with insufficient security protections, like the Mirai Botnet. Consequently, in order to increase the security of the IoT service environment, this study suggests a plan to reduce security threats and vulnerabilities in IoT devices. The addressless IoT server concept, which is proposed in this paper, enables users to leverage a significant portion of the IPv6 address space to safeguard IoT server security. An IPv6 prefix rather than an address is assigned to the server. The authorised client creates a unique destination address under the prefix using an encryption method when it commences communication. When a packet is received, the server checks the destination address and discards it if the check is unsuccessful. By doing so, the model can keep up with the current Internet while preventing attackers from identifying the server and performing scans or attacks. In this study, the prototype is put into use, and numerous experiments are carried out. The outcomes show that the model can enhance server security.***

Keywords: IoT, Smart Devices, Internet of Things, IPv6, IoT Security

1. Introduction

There are billions of communicative devices connected to the Internet through the IoT, a next- generation network. According to a research published in 2017 by Howell, there will be 125 billion linked Internet of Things devices worldwide by 2030. The technology and software required for data transmission and processing are present in the communication devices, enabling them to work together. These billions of gadgets might include Computers, cellphones, sensor systems, controllers,

household appliances, intelligent electric appliances, automobiles, individual components of things, smart webcams, smart textiles, and so forth. Additionally, the usage of these devices through the internet to create apps generates a vast quantity of data for the benefit of the consumers. Fixed Internet, cellular, Wi-Fi, Bluetooth, ZigBee, 802.15.4, PLC, and other techniques are employed to link devices to the Internet. These gadgets are known as IoT nodes in the IoT paradigm, and they might be asset or unfettered nodes. [1]

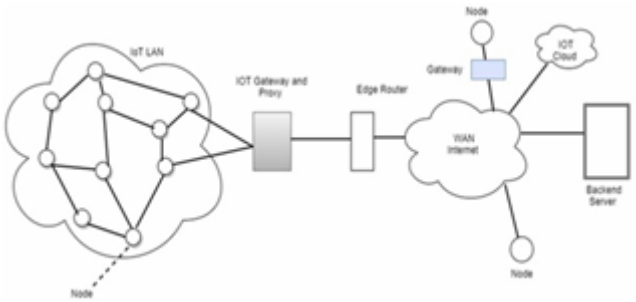

Figure 1: IoT's general architecture [1]

Fig. 1 illustrates an IoT local area network (LAN) or wide area network (WAN) that connects objects to the Internet either directly or indirectly. Due to the insufficient allocation of resources, these nodes ought to be able to configure themselves. Relay nodes, sensor/actuator, powering devices, connecting devices, and other IoT nodes may all be categorised into different classes according to their properties. With the help of technology in the future, machines and living beings will be able to communicate.

a) Full stack of IoT protocol

Fig. 2 shows an overall protocol stack for Internet of Things devices that divides protocols into five different layers [1]: (1) Data, (2) Application, (3) Transport, (4) Network, and (5) Link Layer. The technical specifications and criteria for each layer are presented in the following section. Link Layer: Data transmission through the network's physical media is handled by the link layer. 802.15.4 low rate wireless personal area networks (LR-WPANs), 802.3 Ethernet, 802.11 WI-FI, 802.16- WiMAX, and 2G/3G/LTE/4G/5G cellular connections, among others, can be used as link layer protocols in an IoT setting. Network Layer: Giving each IoT node a distinct address is a fundamental need for Internet of Things (IoT) node routing. IANA just stated that IPv4 addresses have run out. IPv4 is mostly used by Internet hosts to assign unique addresses. Numerous gadgets in the Internet of Things (IoT) expected and needed a unique address. Nearly all things in the world may be addressed using

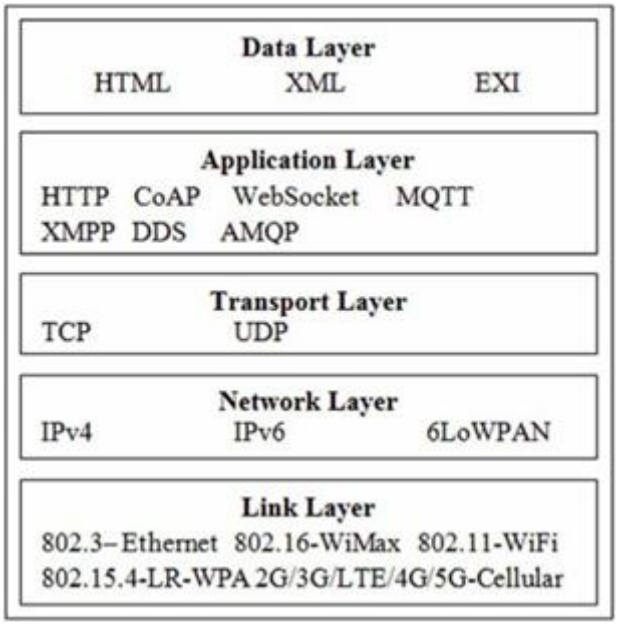

Figure 2: Full stack of IoT protocol [1]

the IPv6 protocol, which was suggested. Given that an IPv6 address is expressed using 128 bits, it can provide billions of IoT nodes a distinctive address. Although IPv6 fixes the addressing issue, its 128-bit long addresses added extra overhead that is unsuitable for constrained IoT nodes. Analysing the service the data link layer offers as a starting point is helpful. The data link layer has several iterations. Some offer a service that relies on connections, while others offer a service that doesn't. As connectionless data link layer services are the most popular, we will concentrate on them in this section. With the aid of various communication protocols, it is primarily responsible for ensuring the connectivity and communication of all the IoT system's devices. Although there isn't a single protocol that is utilised universally for IoT, MQTT 3.1 and the Constrained Application Protocol (CoAP) are the two that are most frequently employed right now. Transport Layer: The transport layer's main duty is to provide end-to-end data delivery without taking the network into account. Data is delivered from one end to the other end via TCP and UDP. Application Layer: To convey data to the Internet, this layer offers an application interface to the transport layer. Application layer data is typically encoded using the HTTP protocol, although constraint nodes do not work well with this protocol. Data transport using Constrained Application Protocol (CoAP), which employs UDP rather than TCP, is useful in constrained environments. Additional application layer protocols are utilised in a particular application, such as WebSocket, Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), and Advanced Message Queuing Protocol (AMQP). It facilitates ways for these devices to communicate outside of the device-oriented system with the use of different kinds of applications depending on the needs of the users [19]; e.g., Smart Home, eHealth, Smart Transportation, Smart Objects etc. Data Layer: As mentioned, the key necessity for the Internet of Things is the interchange of data across nodes. In the Internet of Things, data interchange is accomplished by providing transmitted information in the form of various semantic representation languages, such as the widely used Efficient XML Interchange (EXI) for restricted nodes and eXtensible Markup Language (XML), HTML, and Hyper Text Markup Language (HTML) for unconstrained nodes.

b) Packet format of IPv6

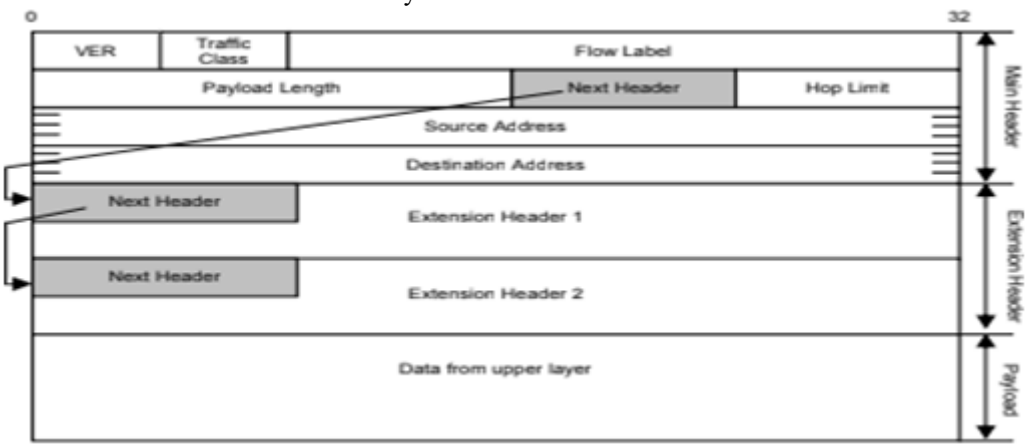

Figure 3: Full stack of IoT protocol [1]

RFC 2460 [3] established the IPv6 packet structure, which includes a fixed main header, an optional extension header, and data from the higher layer. This format is seen in Fig. 3. In contrast to the IPv4 main header's 12 fields, the IPv6 main header is a fixed 40 bytes and has just 8 fields. The less complicated header was designed to lessen the burden on routers, including fragmentation and the absence of a header checksum. The extension header is adaptable, thus it's possible to add other extension headers in the future. A source may choose to carry zero, one, or more extension headers in a packet header. The protocol version is identified by the version field, or VER. The field is 4 bits long and has the value 06. The second element, an 8-bit traffic class field, defines packet priority or its inclusion in a certain traffic class. A router can swiftly decide how to handle each packet in the flow using the information in the next 20 bits, which are called the flow label. In the IPv6 header, this flow label is the only brand-new field. The extension header and packet size information are carried in the 16-bit payload. The maximum length of a packet, 216 or 65,535 bytes, may be determined with 16 bits. Next the IPv6 main header, the following header or data type is defined by

the following 8 bits field. The 8 bits hop limit, which specifies the amount of time before the packet is rejected, is measured in seconds. With each packet forwarding by a router, the value of this field falls by one. In Figure 3, the IPv6 source and destination address fields come before the extension header field as the final two elements. Each field address is 128 bits long, making these fields the longest fields in the IPv6 header. The IPv6 packet's destination address is the address of the recipient, while the source address indicates the IPv6 packet's source address. The version, payload length, next header, source address, and destination address are some of the IPv6 major header elements that are immutable and have fixed values (packet without routing header). Additional fields include traffic class, flow name, and hop limit, which are not fixed or changeable. Internet researchers are concerned with the changeable field, particularly the flow label. IPv6 flow label specifications are already specified, although they are not utilised in actual operations. There are ever more conversations about putting this field into practice. For the IPv6 Flow Label, RFC 6294 [4] provided examples of use cases.

2. Literature Review

The IoT system may experience significant data loss due to a lack of safeguards, and a data breach might involve any sort of data. For this reason, system maintenance is required with regard to a certain time period, and system consideration should be validated using various input and output models (Hassan, 2020). (Obaidat, et al., 2020). [5]

Mentioning the fact that mobile devices now constitute a substantial portion of authoritative IT foundations, with both benefits (such as increased efficiency) and risks (such as security threats). Unauthorised access to company data is the main factor that distinguishes these risks. To develop a safe IoT solution, the right information security techniques must be used, and the password must meet a specified condition that must be maintained via secure interfaces. If the password setup is not done in a way that takes into account the needs for IoT operations, there is a risk of a data breach that will harm end users.

Ecosystems, where the complete Internet of Things (IoT) system is built, can also be weak while, for some devices, the necessity for an API is essential else the data transmission would not be feasible, hence only approved APIs should be utilised. There must be certain mistakes or viruses in APIs, and they might be the main causes of system failure. As the secure interface modelling is necessary to install a secure system, the system failure should be controlled by utilising secured API interfaces so that better controlling and execution can be managed and assured as per control level information and analytics. Every system needs updating and upkeep since every device has a lifespan beyond which it ceases to work and the server's data is compromised.

Only IoT systems will be the best fits for some incredibly complicated processes, but with high-level information security; otherwise, data breaches would be the cause of system failure and organizational failure may be accomplished owing to a significant loss in terms of cost. It could take into account the central system protection for machine-to-machine interaction depending on the privacy level due to the desire for privacy protection from end-users. Since the technical interpretation of information may be used and controlled to establish a significant understanding with the system, appropriate privacy regulations must exist that can be used as a solution for an IoT-based system. The research approaches may alter at the hour of actual use, but this proposal will provide the key context for the study and the methods that will be applied to mitigate risk.

[6] The authors of "Security Threats in Bluetooth Technology" [7] give an introduction of Bluetooth technology, outlining its history and design as well as the many forms of attacks and defence strategies. The authors of "Bluetooth Low Energy Mesh Networks: A Survey" give a comprehensive review of BLE Mesh Networks and touch on security in IoT networks in passing [8]. Information on wireless security and physical layer-based attacks is provided by the authors in "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends" [9].

[10] The implications of the newest features of IoT devices and apps on security and privacy were examined by Zhou et al. [11]. It explores numerous situations, including industrial applications, highlights the burgeoning characteristics of IoT devices, and addresses potential privacy and security concerns. The attack surfaces of such systems are not specifically analysed; rather, it is more of a systematic review of the literature. The properties of the IIoT and consumer IoT were compared by Sisinniet al. [12]. They particularly outlined a three-tier IIoT architecture and talked about potential difficulties and future prospects. When creating safe IIoT infrastructure, they highlighted a number of security factors to take into account, including the adoption of suitable encryption methods and practical identification and authentication techniques.

An industrial robot controller's security was thoroughly analysed by Quarta et al. [13], who also identified potential attack vectors that may be present in general IIoT devices, such as an unprotected network surface, command injection, lax authentication, crude cryptography, and a lack of code signature. They demonstrated a variety of potential weaknesses. After that, they spoke about how to set up a security system in a case study using an industrial robot system. Consumer and IIoT devices, such as a smart metre and a home automation system, were the subject of a thorough security review by Wurm et al. [14]. After that, they talked about security fixes and mitigation strategies. They chose the Itron Centron smart metre as their case study and identified its flaws. Even while certain individual industrial or consumer IoT devices have had their vulnerabilities analysed, a thorough examination of the attack surfaces, attack routes, and defence mechanisms for a typical IIoT device is still lacking.

3. Security Challenges

IoT device attacks are frequently straightforward and simple to carry out, as is covered in more detail in the next sections

of the article. They could be done to violate users' privacy and expose sensitive personal data. The information that is gathered may include everything from straightforward measurements of the humidity and temperature in the space to more practical data like the user's location and daily routines or the heart-rate signal. Compromise of one IoT device and use of that compromised device as a base of operations for fraudulent activity against another network node constitutes another prevalent attack tactic. [15]

Here, we provide a general overview of the IoT security requirements and the associated challenges in order to establish a common ground for the discussion that will take place in the following sections. We first provide a categorization of the security needs for such an IoT system in relation to the various operational levels, specifically at the knowledge, access, and functional levels [16], [17].

1) Information Level: Security should ensure that the following conditions are met at this level:

- Integrity: During the transfer, the data should not have been changed.
- Secrecy: Third parties should not be aware of the identities of the source of data.
- Confidentiality: Data is unreadable by outside parties. For IoT devices to exchange protected information, a trustworthy relationship must be created. Messages that have been duplicated must also be identifiable.
- Confidentiality: No private information about the customer should be shared during the data transfer. Identifiable information must be difficult for listeners to infer.

2) Access level: It details a few security controls to limit network access. It offers the following capabilities in further detail:

- Access control ensures that only authorised users have access to the devices and network for administrative duties (such distant reconfiguration or monitoring of the IoT devices connected to the network).
- Authorization: This process makes sure that only people and devices with the proper authorization can access network resources or services.

3) Functional level: At this level, the following standards for security are defined:

- Resilience: This is the ability of a network to protect its devices from assaults and other failures while maintaining security for its devices.
- Self organisation: this term refers to an IoT system's capacity to adapt so that it can continue to function even when some of its components fail due to sporadic malfunctions or malicious attacks.

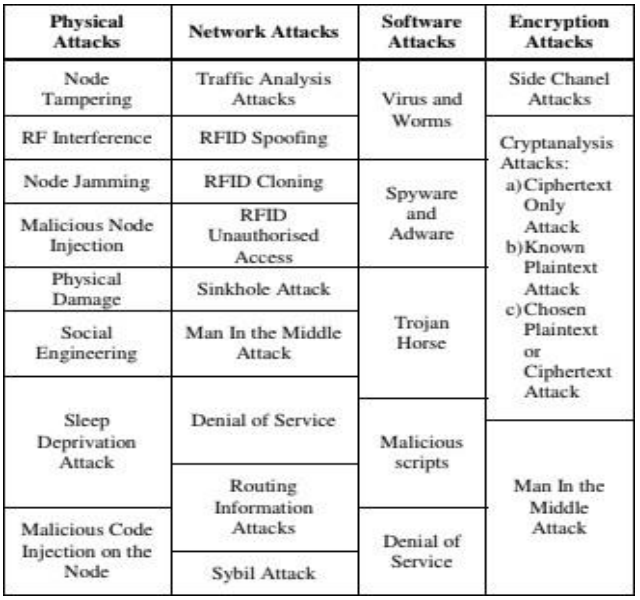

Figure 4: IoT Threat Analysis [18]

A physical attack, an attack from within the network, an attack from the system's applications, and finally, an attack on the encryption algorithms are all ways that an Iot device can be compromised. Internet, RFIDs, wireless sensor networks, and other existing network technologies are used to implement the Internet of Things. In order to design and apply stronger countermeasures for safeguarding it, it is necessary to classify attacks properly so that it encompasses all of the many sorts of threats. Fig. 4 provides an overview of the assaults' taxonomy. Fig. 5 provides the security countermeasures for IoT layers. [18]

4. Proposed Methodology

The development of an incident response system with the ability to recognise a cyberattack that could impair the functionality of IoT systems will be used to complete the research using the qualitative research approach. The following tasks will be possible for the system to complete: The system will

- Detect the type of attack as it enters the system and
- Store the target class and domain as well as the nature of the attack. The system might provide analytical information well about attack so that a mitigation approach can be developed.
- The system will be installed at the main network of an enterprise environment, where the whole implementation and composition of a cyber-attack will be stored.
- The attack will be recognised by an identifier so that the full product level information can be generated and distributed with the incorporation of fundamental level knowledge that can be used

IoT Layer	Counter Attacks for the Specific Layers	Counter Attacks for All Layers
Physical Layer	1) Secure Booting for all IoT devices a) Low power Cryptographic Hash Functions 2) Device Authentication using Low Power Techniques a) Data Integrity b) CRC – Cyclic Reduntancy Check c) Checsum d) Parity Bit e) WH Cryptographic Hash Function 3) Data Confidentiality a) Encryption Algorithms like Blowfish and RSA 4) Data Anonimity a) K- Anonimity	1) Risk Assessment b) Finding New Threats c) Applying Updates d) Applying Patches e) Providing Improvements f) Upgrading Systems 2) Intrusion Detection Mechanisms specific to IoT Systems 3) Securing the IoT Premises a) Physical Barriers b) Intrusion Detection Alarms c) Monitoring Devices d) Access Control Devices e) Security Personel 4) Trust Management a) Trust relation between layers b) Trust of Security and Privacy at each layer c) Trust betweeen IoT and User
Network Layer	1) Secure Communication between the devices a) Network Authentication – challenge-response mechanisms b) Point-to-Point Encryption for the confidentiality of the transmited Data c) Cryptographic Hash Functions for the Inegrity of the transmited Data 2) Implementation of Routing Security a) Use of Multiple Paths b) Encrypting Routing Tables c) Hashing Routing Tables 3) Secure User Data on the Devices a) Data Authentication b) Data Confidentiality; Encryption Schemes of encrypting the data c) Data Integrity; Cryptographic hash functions	
Application Layer	1) Data Security a) Authentication; biometrics, passwords, etc. b) Confidentiality; Strong Encryption Schemes (AES) c) Integrity; Cyrptographic Hash Functions 2) Access Control Lists (ACLs) 3) Firewalls 4) Protective Software a) Anti-virus b) Anti-adware	

Figure 5: Countermeasures for security

In accordance with the right position of attack data collection.

- The network department will receive an immediate report from the system, allowing them to provide network security directives to safeguard the entire IoT system.
- As a result of this study's analysis of IoT security incidents [19],
- It is simple to collect data on IoT devices that are linked to the Internet due to the absence of available for quick reaction to the IoT service market
- The goal of this project was to provide security technologies for IoT devices already in use without including safety by design at the time of creation and sale.

Additionally, IoT devices only function in relation to the applications provided in the system and do not engage directly with consumers unless abnormal circumstances arise [20]. This study used technologies, such as network hardening and security monitoring, to prevent or identify behaviours other than normal operation in light of these kinds of features of IoT devices.

All prominent stateless IPv6 addressing schemes for IoT networks are compared in Fig. 6 for your viewing pleasure. The non-spatial and spatial categories of these addressing methods are separated. While the majority of non-spatial addressing strategies produce IPv6 addresses with integrated spatial information, they do not always ensure uniqueness. Even though the efficiency of such IPv6 addressing strategies is encouraging, further optimised schemes will be needed to address problems such Quality of service (QoS) awareness IPv6 addressing scheme to satisfy the QoS parameters of IoT ecosystem, information security, portability, and adaptation of harsh environments.

Addressing Scheme	Type	Uniqueness	Address reuse	Energy Consumption	Communication Overhead	Location Information
EUI-64	Non-Spatial	Guaranteed	No	Low	No	No
Privacy Address	Non-Spatial	Guaranteed	Yes	Low	Low	No
Cryptographically Generated Addresses	Non-Spatial	Guaranteed	No	High	High	No
SIPA	Spatial	No	Yes	High	High	Yes
SLIPA	Spatial	No	Yes	High	High	Yes
SLIPA-Q	Spatial	No	Yes	High	High	Yes
DSIPA	Spatial	Guaranteed	Yes	Low	Low	Yes
MPIPA	Spatial	Guaranteed	Yes	Low	Low	Yes
(Hyojeong et al., 2009	Spatial	Guaranteed	Yes	High	High	Yes
(Chakraborty et al.,2015)	Non-Spatial	No	No	Low	Low	No
(Kassem et al., 2015)	Spatial	Guaranteed	No	Low	Low	No

Figure 6: IoT IPv6 addressing strategy comparison [1]

5. Conclusion

This paper introduces the addressless server, a new type of IoT server. By allocating an IPv6 prefix rather than an IPv6 address to each server, the approach employs the prefix delegation technique. All addresses inside the prefix are open to the server. The server checks the data flow using the address of the destination and only verified clients are able to generate valid destination addresses using encryption. The huge IPv6 address space is used by the model to

conceal the actual addresses. No longer does the server have a fixed IPv6 address. In this approach, the one-to-one relationship between the host and the IP address is removed, making it more challenging for an attacker to identify the precise address from which to launch attacks, protecting the server from scanning and attacks. The security of the server is ensured by these characteristics.

Acknowledgement
This research was supported by our departmental staff members. We thank our colleagues from our institution who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations of this paper.

References

[1] Kumar, Gyanendra and Tomar, Parul. (2018). A Survey of IPv6 Addressing Schemes for Internet of Things. International Journal of Hyperconnectivity and the Internet of Things. 2. 43-57. 10.4018/IJHIoT.2018070104.
[2] Praptodiyono, Supriyanto. (2012). Review on IPv6 Security Vulnerability Issues and Mitigation Methods. International Journal of Network Security and Its Applications. 4. 173-185. 10.5121/ijnsa.2012.4613.
[3] Request for Comments: 2460, Internet Protocol Version 6 (IPv6) Specification, December 1998: Internet Engineering Task Force. http://www.ietf.org/rfc/rfc2460.txt.
[4] Request for Comments: 6294, Survey of Proposed Use Cases for the IPv6 Flow Label, 2011, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc6294.txt.
[5] Butun, Ismail and Österberg, Patrik and Song, Houbing. (2019). Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. IEEE Communications Surveys and Tutorials. 22. 616-644. 10.1109 / COMST.2019.2953364.
[6] Lonzetta, Angela and Cope, Peter and Campbell, Joseph and Mohd, Bassam and Hayajneh, Thaier. (2018). Security Vulnerabilities in Bluetooth Technology as Used in IoT. Journal of Sensor and Actuator Networks. 7. 28. 10.3390/jsan7030028.
[7] Hassan, S.S.; Bibon, S.D.; Hossain, M.S.; Atiquzzzaman, M. Security Threats in Bluetooth Technology.Comput. Secur. 2017, 74, 308–322. [CrossRef]
[8] Darroudi, S.M.; Gomez, C. Bluetooth low energy mesh networks: A survey. Sensors 2017, 17, 1467. [CrossRef][PubMed]
[9] Zou, Y.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. arXiv 2015, arxiv:1505.07919.
[10] Jiang, Xingbin and Lora, Michele and Chattopadhyay, Sudipta. (2020). An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. ACM Transactions on Internet Technology. 20. 1-24. 10.1145/3379542.
[11] Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2):1606–1616, 2018.
[12] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 14(11):4724–4734, 2018.
[13] Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. An Experimental Security Analysis of an Industrial Robot Controller. In Proc. of 2017 IEEE Symposium on Security and Privacy (SP), pages 268–286. IEEE, 2017.
[14] Jacob Wurm, Khoa Hoang, Orlando Arias, Ahmad-Reza Sadeghi, and Yier Jin. Security analysis on consumer and industrial IoT devices. In Proc. of 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pages 519–524, IEEE, 2016.
[15] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, DOI: 10.1109/JIOT.2019.2935189.
[16] P. Fremantle and P. Scott, “A survey of secure middleware for the Internet of Things,” PeerJ Computer Science, vol. 3, p. e114, May 2017.
[17] R. H. Weber, “Internet of Things – new security and privacy challenges,” Computer Law and Security Review, vol. 26, no. 1, pp. 23–30, Jan. 2010.
[18] Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.
[19] Choi, S.-K and Yang, C.-H and Kwak, Jin. (2018). System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Se- curity Vulnerabilities and Threats. KSII Transactions on Internet and Information Systems. 12. 906-918. 10.3837/tiis.2018.02.022.
[20] Ryan Williams, Emma McMahon, Sagar Samtani, Mark Patton and Hsinchun Chen, “Identifying Vulnerabilities of Consumer Internet of Things (IoT) Devices: A Scalable Approach,” in Proc. of Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on, July 2017 Article (CrossRef Link)

Author Profile

Praveen Misra, Senior Scientist is working in Education and Research Network, a scientific institution of the Government of India. He is pursuing Ph.D. from the department of Computer Science and Application of Sri Krishna university, Chhatarpur, MP, India.

Dr. Rajeev Yadav is a Professor in the Department of Computer Science and Application, Sri Krishna University, Chhatarpur, MP India