ISSN: 2096-3246
Volume 50, Issue 01, Jan, 2018

Safeguarding the Internet of Things: Tackling Security and Privacy Hurdles

[1] Jyoti [2] Sumathi B. H. [3] Shylaja S N
[1] Senior Scale Lecturer.Department of Electronics and CommunicationS.J. Government Polytechnic Bangalore.
[2] Senior scale lecturerDepartment of Electronics and CommunicationS.J. Government polytechnic Bangalore.
[3] Lecturer Department Of Electronics and Communication.Government Polytechnic for Women, Hassan
[1] jyotimurag@gmail.com
[2] sumathibh@gmail.com
[3] shylasn@gmail.com

Keywords

Safeguarding , Internet of Things (IoT) , Security, Privacy

Abstract

The smooth exchange and sharing of data across networked physical and virtual objects is made possible by the Internet of Things (IoT), a fast expanding and inventive field. It does away with the necessity for human intervention and provides cutting-edge services for many real-world uses. IoT envisions a world in which computing is pervasive and offers improved connection for a variety of applications around the globe.The 3-layered and 4-layered IoT designs that are now in use, however, have limits when it comes to fulfilling certain specifications for real-world applications. To solve this problem, we offer a 5-layered IoT architecture that emphasises useful and intelligent applications while properly interpreting IoT features. The development, definition, five-layered structure, technology, and applications of IoT are all covered in this architecture overview.In addition to its advantages, IoT is vulnerable to security vulnerabilities that jeopardise data sharing and exchange. To provide a secure environment, it is essential to solve these security challenges. The main privacy and security issues that each layer of the IoT architecture presents are highlighted in this study. We can create IoT solutions that prioritise data security and privacy by taking these issues into account.

Introduction

The Internet of Things (IoT) industry has seen substantial technological advancement and market expansion throughout time. The IoT is poised to become the next profound change in how we perceive and share information, much like historical revolutions like the industrial revolution in the 19th century and the information age revolution triggered by computer development in the 1960s. The Internet of Things (IoT) is a dynamic global network architecture that connects real-world and virtual objects using technologies like ZigBee, RFID, GPS, and sensors. Big data processing, satellite communication, cloud computing, mobile communication, and database management are just a few of the technologies that make up the Internet of Things, which enables ubiquitous computing and offers cutting-edge services for enterprises. By 2020, more than

ISSN: 2096-3246
Volume 50, Issue 01, Jan, 2018

24 billion smart gadgets are anticipated to exist. Our daily lives are changing as more commonplace items are integrated into information systems and end-user applications. This creates a connected universe where machines and people interact to improve safety, sustainability, and well-being in our society. The World Wide Web's (www) launch in the early 1990s served as the impetus for the development of the Internet of Things. Initially, the internet allowed for the sharing of information via email and websites, which is known as the "Internet of Content." Dynamic web sites, which offer improved services and practical platforms for e-commerce and are successfully used by businesses like Amazon, Flipkart, and Alibaba, developed with the development of the World Wide Web. The Internet of Services could be used to describe this phase. The development of personal smart gadgets like tablets and smartphones is another factor. led to the emergence of well-known websites like Facebook, Instagram, LinkedIn, Hike, and YouTube, which turned the internet into a social networking platform. The Internet of People could be used to characterise this stage. We are currently witnessing the beginning of the next internet revolution, often known as the Internet of Things (IoT), which is enabled by machine-to-machine (M2M) connections [1].

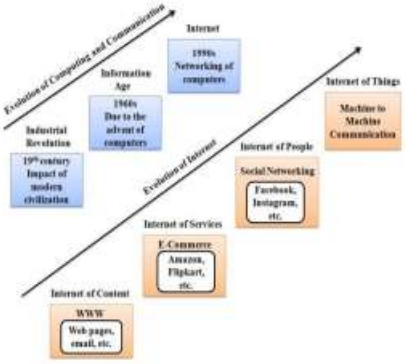

Figure 1 .Evolution of IoT

A big incident involving the Dyn Network, a key US DNS service provider, occurred in 2016. This service provider was subjected to an unrelenting data flood that reached 1 terabyte per second and caused a serious distributed denial of service (DDoS) attack. The hack had a significant effect, taking down popular websites including Reddit and Airbnb. This attack was notable because it was the first significant example of one that involved Internet of Things (IoT) devices. Smart cameras and home routers were among the over 150,000 IoT devices that were hijacked and used to attack a single DNS service provider. This event underscores how crucial privacy and security are in the IoT space.IoT security and privacy must be ensured at all times, but especially while creating IoT protocols, systems, and devices. Addressing numerous security and privacy concerns is crucial. These concerns include user and service privacy, authentication, undeniability, data integrity, confidentiality, and user secrecy. A wide range of devices and apps are deployed in several scenarios as a result of the IoT's integration in the real world, which increases the importance of effective security and privacy safeguards.

Architectures

Considering the challenges posed by IoT requirements, the characteristics of IoT itself, and the need to connect billions of heterogeneous devices through the Internet, it is crucial to adopt a dynamic architecture.We can investigate various IoT architectures suggested in the literature in order to satisfy particular IoT requirements. The 3-layered architecture and the 5-layered architecture are two distinguished architectural designs. The perception layer, network layer, and application layer are the three layers of the architecture. The sensing layer, network layer, processing layer, application layer, and business layer are all parts of the 5-layered architecture in contrast [2]. We give a brief summary of each layer in the five-layered architecture in the paragraphs that follow.A. Perception Layer: The Perception Layer acts as the IoT's fundamental layer by linking the informational and physical worlds. It includes both real-world things like GPS and QR codes as well as virtual ones like sensors, RFID tags, actuators, and Wireless Sensor Networks (WSN). This layer's main function is to use RFID reader-writers, two-dimensional code labels, and code reader-writers to translate detected object information into digital data (such as wind speed, pH level, position, vibration, and humidity). The network layer [3][4] receives the digitised data after it has been transferred.B. Network Layer: The Network Layer is essential for tying together servers, network devices, and the numerous smart objects or "things" in the Internet of Things. Depending on the exact sensor devices used, it makes use of technologies including 3G, 4G-LTE, Wi-Fi, and ZigBee to provide safe sensor data transmission. Establishing connectivity and facilitating communication amongst IoT devices is the layer's main duty. This calls for the use of a variety

of communication channels, network interfaces, and protocols as well as the upkeep and administration of information and networks. Data is moved from the processing layer to the perception layer in this layer [5].

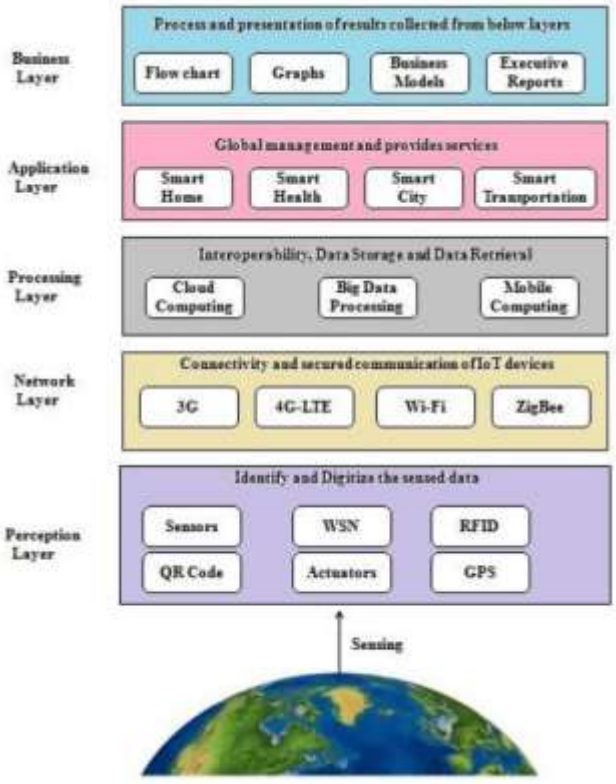

Figure 2.-Layered Architecture of IoT

C. Processing Layer: Also known as the middleware layer, the processing layer is in charge of receiving, examining, and processing the enormous volumes of data that are received from the network layer. For both the upper and bottom layers, this layer manages and provides a wide variety of services. Among its main tasks is the storage and retrieval of data using various database management techniques. Utilising technologies like cloud computing, large data processing modules, and mobile computing, it can accomplish interoperability through pervasive and ubiquitous computing [6].D. Application Layer: Based on the data gathered in the processing layer, the application layer manages applications. It includes a variety of uses for IoT, including smart homes, smart cities, smart health, and smart transportation, among others. Users can access application-specific services through the Application Layer, which also makes it easier to administer applications globally. Intelligent applications between IoT and end users are connected by technologies including virtual reality, augmented reality, multimedia applications, and human-computer interface, enabling the development of intelligent information applications. [7][8][9].E. Business Layer: Based on data processed from the application layer, the business layer manages services and presents a variety of IoT applications. This layer allows the production of flowcharts, useful graphs, business models, and executive reports by utilising exact data acquired from beneath layers.International organisations like ITU-T, IETF, W3C, and others may have refrained from standardising layered IoT architectures in order to foster research on flexible architectures for prospective technological developments [10].III. Key IoT Technologies: The advancement of IoT is being fueled by advancements in device power efficiency, small yet potent device designs, and reasonably priced ubiquitous internet connectivity. As a result, a lot of attention has been paid to IoT technologies as Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), 4G-LTE, ZigBee, Cloud Computing, and Big Data Analytics [11][12].Here, we cover a few of the major IoT technologies.A. RFID Technology: As the foundation of the Internet of Things' architecture, RFID Technology is essential to the development of the IoT. It is a wireless data transmission method that use radio frequency signals to send information for autonomous object tracking and identification. When a query signal is received, RFID tags function as tiny transceivers and communicate their individual IDs to readers. Without having a direct line of sight, RFID readers may retrieve data such as unique IDs and transmit it to the enterprise information system. EPC standards, ISO/IEC standards, and UID standards are examples of international standards that support RFID technology.B. Wireless Sensor Networks (WSN): A WSN is made up of spatially dispersed nodes that can sense their surroundings, compute data, and interact with one another. Each sensor node manages its own decentralised and self-organized operation, preserving optimal connectivity over extended durations, and sending data via many hops to a base station. The use of RFID for object detection and the monitoring of object conditions by WSNs as a supporting technology for multi-hop wireless

communication make RFID and WSNs complementary technologies. These technologies work together to fill the gap between the real and virtual worlds.C. 4G LTE: At the network layer of the Internet of Things, 4G-LTE is a crucial technology for data transmission. Orthogonal frequency division multiplexing is the radio access technology used by Long Term Evolution (LTE), along with cutting-edge antenna technologies. It is built using the same GSM and HSPA technologies as older mobile networks. High-speed data transport is supported by LTE for mobile communications.D. Cloud Computing: By tackling the research problem of utility computing, cloud computing has significantly contributed to the growth of the information technology sector. With the computer infrastructure being referred to as a "Cloud," it enables people and organisations to access programmes whenever they need them from anywhere in the world. Cloud computing's guiding principle is the delivery of computation, storage, and software "as a service."

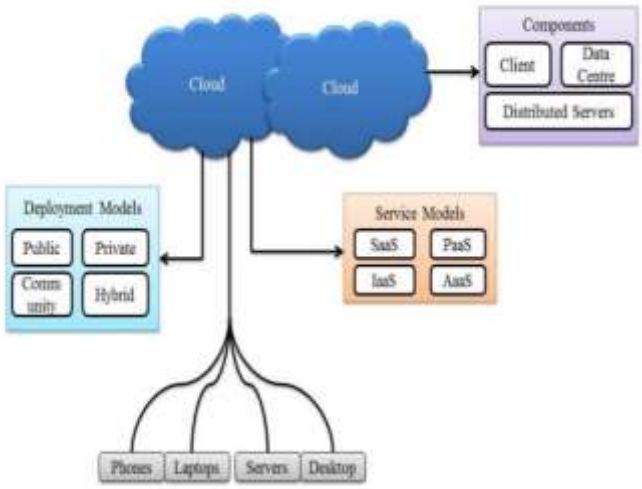

Figure 3.Cloud Computing

E. Big Data Analytics: Traditional database systems find it difficult to handle the enormous amount of data produced by modern internet technologies, such as social networking websites, which create terabytes of data every day. By utilising distributed parallel architecture, Big Data Analytics provides a solution to this problem. Through the use of numerous servers for data dissemination and parallel execution environments, this method accelerates the processing of data. Big Data analytics is a cutting-edge method that makes it possible to quickly store, distribute, visualise, manage, and analyse massive volumes of data. Both structured and unstructured data can be handled by it.Applications of IV. IOT

IoT applications and devices have been incorporated into many facets of daily life, including smart homes, healthcare, and transportation. Our daily routines are improved by these innovations, which make personal and professional chores simpler. The emphasised IoT application domains that have enormous potential for economic growth are listed below.

A. Transportation Domain: IoT integration has advantages for the transportation industry, which includes roads, trains, and waterways. Transportation systems are made smarter and more effective by combining Internet of Things (IoT) technologies, such as RFID tags with embedded intelligence, actuators, sensors, and various gadgets. This makes it possible to track, monitor, and optimise routes in real-time, resulting in more security, less traffic, and better logistics.

B. Manufacturing Sector: Currently, the manufacturing sector is under pressure to achieve strict quality requirements, competitive product pricing, low labour costs, and on-time product delivery. IoT infrastructure is being introduced, including cutting-edge sensor networks, wireless connectivity, cutting-edge hardware, and machine-to-machine communication to address these issues. This evolution of industrial automation techniques offers increased manufacturing productivity and efficiency.

C. Power Management: Despite having surplus power generation, many nations, including India, have power outages in various regions as a result of subpar distribution networks and insufficient power management. The conventional power grid can be upgraded to a "Smart Grid" by adopting IoT-based power analysis and energy optimisation. The smart grid makes use of smart metres, home gateways, smart plugs, and linked products to improve overall power management, save money for consumers, manufacturers, and utility providers, and save resources.

D. Healthcare Domain: IoT finds useful applications in the healthcare industry by gathering patient health parameter data from wearable devices with extremely low power and great energy efficiency, such as blood pressure, body temperature, and heart rate. Healthcare facilities and the appropriate people can receive this information to take additional medical action. Through the use of devices like smart fluid management systems, IoT also helps with the early detection of serious medical diseases including diabetes, prostate cancer, and heart failure.

V. IOT PRIVACY PROBLEMS

The protection of the enormous volume of data created and processed by the IoT depends critically on privacy. Privacy becomes a key element of security principles as more linked devices, services, and users share a single communication network. Network privacy, another name for internet privacy, protects the confidentiality of personal information sent over the internet. To solve the issues of data privacy in the IoT context, effective security features including object naming, identification, service provision, data collecting, and infrastructure administration are required.

The following are some IoT privacy challenges:

A. Data Overload: The enormous amount of data that IoT devices produce can be debilitating. Less than 10,000 households can generate 150 million discrete data points every day, according to a Federal Trade Commission analysis. This plethora of data enhances the vulnerability of private data and gives hackers more entry opportunities.

B. Eavesdropping: Manufacturers or hackers may use connected gadgets to violate a person's privacy when they are at home. For instance, researchers in Germany were able to identify the television show being viewed at a certain time by intercepting unencrypted data from a smart metre device.

C. Consumer Confidence: Every issue relating to privacy has the potential to reduce consumer confidence and have an effect on the uptake of connected items. The Internet of Things can't realise its full potential because of this lack of confidence.

VI. IOT SECURITY PROBLEMS

In order to prevent unauthorised access to devices, data, and networks and to guarantee data integrity, security is of the utmost significance. IoT system intrusions are monitored and prevented by policies and technologies. IoT security deals with the dangers brought on by the vast majority of unprotected devices connected to the internet.IoT security concerns safeguarding connected systems and networks inside the IoT. Numerous unsecure devices connecting to the internet are the potential concern. The security issues unique to each layer of the IoT architecture are described in this section.A. Perception Layer: The main job of the perception layer is to sense and digitise data. The manipulation of data gathered from real-world and virtual objects is a major security problem for IoT at the perception layer. Significant concerns come from attacks like malicious code injection and node capture. Effective monitoring and fake node detection are essential defences against node capture threats. Effective code authentication techniques are also necessary for preventing malicious code injection.At the perception layer, eavesdropping and interference are additional security concerns. Unauthorised individuals may intercept the information being transmitted by IoT devices when they communicate wirelessly. By filtering out noise data and restoring the underlying information, secure noise filtering systems can assure accurate and fast data transmission.B. Network Layer: Transmitting sensed data is the network layer's main duty. This layer's security issues mostly relate to wireless communication and the accessibility of network resources. Attacks that cause a denial of service (DoS) to the system represent a serious threat by making such services unavailable. Network protocol attacks including Ping of Death, TearDrop, UDP flood, SYN flood, and Land Attack deplete IoT resources. IoT security depends on researching and creating defences against DoS threats.Attacks Using spoofing techniques, like as IP spoofing or RFID spoofing, adversaries can gain unauthorised access to an IoT system and transfer malicious data into the network. In RFID spoofing, the attacker creates a fake RFID tag, records the information from it, and then uses that tag to send harmful data to the IoT network.Sinkhole Attacks: During a sinkhole attack, an infected device or node makes fictitious claims about having superior processing, communication, and power in order to persuade other nodes to choose it as the source node for data routing. Numerous secure routing protocols and strategies must be developed and put into use to defend against this attack.Routing information attacks target IoT systems' routing protocols, giving attackers the ability to change routing information and introduce route loops in network data transfer. By establishing secure connections between IoT devices, trust management and secure

routing protocols are used to minimise this threat and stop the leakage of IP addresses and identifying information to adversaries.Sinkhole Attacks: During a sinkhole attack, an infected device or node makes fictitious claims about having superior processing, communication, and power in order to persuade other nodes to choose it as the source node for data routing. Numerous secure routing protocols and strategies must be developed and put into use to defend against this attack.Routing information attacks target IoT systems' routing protocols, giving attackers the ability to change routing information and introduce route loops in network data transfer. By establishing secure connections between IoT devices, trust management and secure routing protocols are used to minimise this threat and stop the leakage of IP addresses and identifying information to adversaries.Identity theft: Unauthorised users have the ability to obtain authentication data, such as EPC codes or passwords, jeopardising private data and sensitive information.Routing assaults: In routing assaults, attackers can take control of an IoT device's routing information, increasing security risks.

D. User-requested services are provided by the application layer, making it a difficult target for software attacks.

Phishing assaults: In phishing assaults, the attacker pretends to be a reliable entity in order to obtain users' private information, such as usernames and passwords, using tainted emails or phishing websites. While online, users should exercise caution because IoT devices are not intelligent enough to efficiently detect these dangers.Malicious Virus/Worm Attacks: To access sensitive data, adversaries use unauthorised self-propagating attacks to corrupt IoT apps. Methods like virus identification and defence systems should be used to stop these attacks.Attacks Using Malicious Scripts: In order to interfere with the operation of IoT systems, malicious scripts are inserted, modified, or removed from software. All IoT applications are connected to the internet, making it simple for attackers to deceive users into running malicious programmes. To lessen this hazard, efficient script detection approaches should be used, such as static code analysis.E. Business Layer: It can be difficult to deploy remote signing device configuration and operational information securely because IoT devices frequently connect to the network on their own after deployment. Managing security data, such as IoT machine logs, emerges as a new issue that may jeopardise the trustworthiness of the connection between the network and service platform, raising more security issues.

Conclusion

IoT has become a reality thanks to the quick development and advancement of technology, changing and improving our lives. The frontiers of networks and the internet have been enlarged, going beyond the realm of what is possible in the future. IoT makes computing ubiquitous by enabling interaction and communication with everything, anywhere, and at any time, which promotes self-sufficient data sharing and exchange. In this article, we give an overview of the development of the Internet of Things (IoT), define it, and suggest a 5-layered architecture that combines enabling technology and intelligent applications. In order to ensure safe communication, our main focus is on addressing the substantial privacy and security challenges connected to each layer of the IoT architecture.

References

[1] S. Kraijak and P. Tuwanut, “A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends,” Int. Conf. Commun. Technol. Proceedings, ICCT, vol. 2016– Febru, pp. 26–31, 2016.

[2] L. Patra, U. P. Rao, L. Patra, and U. P. Rao, “Internet of Things - Architecture, applications, security and other major challenges,” 2016 3rd Int. Conf. Comput. Sustain. Glob. Dev., pp. 1201–1206, 2016.

[3] N. Papakostas, J. O’Connor, and G. Byrne, “Internet of things technologies in manufacturing: Application areas, challenges and outlook,” Int. Conf. Inf. Soc. i-Society 2016, pp. 126–131, 2017.

[4] Y. C. Pranaya, M. N. Himarish, M. N. Baig, and M. R. Ahmed, “Cognitive Architecture based Smart Grids for Smart Cities,” pp. 44–49, 2017.

[5] X. Xu, “Study on security problems and key technologies of the internet of things,” Proc. - 2013 Int. Conf. Comput. Inf. Sci. ICCIS 2013, pp. 407–410, 2013.

[6] M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” 2015 IEEE World Congr. Serv., pp. 21–28, 2015.

[7] A. Shifa, M. N. Asghar, and M. Fleury, “Multimedia security perspectives in IoT,” 2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016, pp. 550–555, 2017.

[8] P. A. H. Williams and V. McCauley, “Always connected: The security challenges of the healthcare Internet of Things,” 2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016, pp. 30–35, 2017.

[9] 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 Things J., vol. 4, no. 5, pp. 1125–1142, 2017.

[10] C. Le Zhong, Z. Zhu, and R. G. Huang, “Study on the IOT architecture and gateway technology,” Proc. - 14th Int. Symp. Distrib. Comput. Appl. Business, Eng. Sci. DCABES 2015, pp. 196–199, 2016.

[11] M. Khari, M. Kumar, S. Vij, P. Pandey, and Vaishali, “Internet of Things: Proposed security aspects for digitizing the world,” Proc. 10th INDIACom; 2016 3rd Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2016, pp. 2165– 2170, 2016.

[12] M. R. Kounte and B. K. Sujatha, “Identification of Visual Attention Regions in Machine Vision Using Saliency Map,” pp. 639–643, 2015.

[13] C. Yang, W. Shen, and X. Wang, “Applications of Internet of Things in manufacturing,” Proc. 2016 IEEE 20th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2016, pp. 670–675, 2016.

[14] A. Riahi, E. Natalizio, Y. hallal, N. Mitton, and A. Iera, “A systemic and cognitive approach for IoT security,” 2014 Int. Conf. Comput. Netw. Commun. ICNC 2014, pp. 183– 188, 2014.

[15] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012.