A Model on IoT Security Method and Protocols for IoT Security Layers

Chandra Prakash and Rakesh Kumar Saini

Abstract Internet of things (IoT) digitalized the worldwide system containing individuals, connected things, smart devices, data, and information. It is a well-known fact that as an ever-increasing number of devices interface with the Internet, the difficulties of making sure about the information that transmitted and interchanges that they start are getting progressively significant. Throughout the years, we have seen a flood in IoT devices, comprehensively in two parts: homes and manufacturing. Since these are autonomous and secure fields, the duties of making sure about the devices rest with the platform providers. In this paper, we have discussed the various application areas where IoT is applied to get an effective and reliable outcome, and majorly, we have focused on security aspects related to IoT. For that purpose, we have proposed a security model to protect the IoT network or system from unwanted threats and attacks. The proposed model is providing a choice of a suitable security method and protocols for IoT Security layers. This model is used to improve the performance of IoT system by opting the appropriate security methods for IoT layers to reduce the power and time consumption.

Keywords IoT applications · IoT security challenges · IoT communication protocols · IoT in manufacturing · IoT in healthcare

1 Introduction

IoT can be defined as a systematic setup of interrelated computing devices, individuals, connected things, advanced machines, data, and information that are given through unique identification and capable to send information over a system without direct interfering of human. A thing in the word IoT can be an individual with

C. Prakash (✉) · R. K. Saini
School of Computing, DIT University, Dehradun, Uttarakhand, India
e-mail: chandra.thukral.19@gmail.com

R. K. Saini
e-mail: rakeshcool2008@gmail.com

N. Marriwala et al. (eds.), *Mobile Radio Communications and 5G Networks*,
Lecture Notes in Networks and Systems 140,
https://doi.org/10.1007/978-981-15-7130-5_63

implantable cardiac monitor, a car that has in-built sensors to caution the driver when pressure of tire is low or some other regular or man-made article that can be allotted an IP address and can move information over a system. IoT is a thought that could drastically modify our relationship with innovation. The market is as of now concentrating on the vertical spaces of IoT since it is in moderately early periods of advancement, but IoT cannot be treated as a solitary thing, or single device, or even a solitary innovation. So as to accomplish the normal quick development from IoT deals, more concentration should be put on interfaces, versatile applications, and normal/predominant guidelines [1, 2].

Web-enabled remote study classrooms will be an achievement for creating nations, making profound infiltration in regions where setting up a customary institution foundation is beyond the realm of imagination. Web-enabled industries and manufacturing units are giving separating outcomes, making them more secure and increasingly proficient through robotized process controls. Finance-related administrations are as of now utilizing the web for a large number of their administrations [3, 4]. While the potential outcomes of these new advancements are amazing, they have additionally uncovered unadorned IoT security challenges. During most recent couple of years, we have seen an increment in the number and the refinement of attacks focusing on IoT devices. The interconnectivity of individuals, objects, and groups in the present digitalized world opens up an entirely different playing field of susceptibilities passageways where the cybercriminals can get in. On the other hand, IoT technology devises a number of problems as well. Like, complexity is one of the most substantial drawbacks as IoT operations are difficult, and there is not at all flexible incorporation between nodes. There are various devices with diverse design, implementation and deployment, so any drawback in software and hardware will have severe difficulties. IoT network undergoes from validation and access control problems because smart things have diverse devices that are based on various platforms. Moreover, all devices are essential to interact with another device via different network. Therefore, security problems have the key challenge because all devices are unprotected to all kinds of attacks and threats. There are many kinds of attacks and threats that might cause severe tragedies in the network. Furthermore, all private data of users are unprotected to the most hazardous attacks. In the proposed model, that is used to create security control system for the IoT network to offer appropriate security tools for the IoT security layers. It can assist designer to reduce the time and power consumption. This paper also gives a review of the present province of IoT security challenges [5].

2 Security Challenges in IoT

There are some security challenges in Internet of things that are shown in Fig. 1.

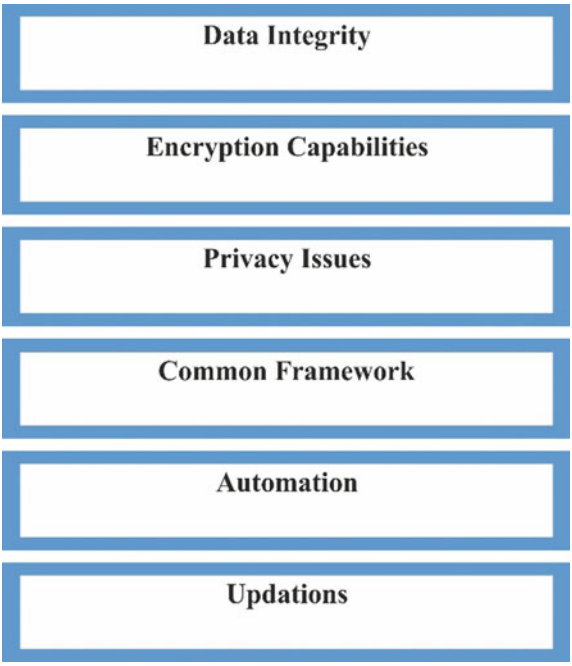

Fig. 1 Security challenges in IoT

2.1 Data Integrity

Data integrity is the correctness, consistency, and completeness of data. Additionally, data integrity can be defined as data security with respect to administrative consistence. It is kept up by an assortment of procedures, guidelines, and standards actualized during the structure stage. At the point when the data integrity is secure, the data will keep complete, correct, and consist in the database, regardless of what extent its put away or how regularly it is accessed. The integrity of data guarantees that your information is sheltered from any outside forces [6].

2.2 Encryption and Decryption Capabilities

IoT carries another set of security parameters. In contrast of VPN encryption, which protect network by an encryption and unspecified channel, IoT devices bring with their own built-in robust security and encryption protocols. VPN distributes a separated space on the system. However, any participant inside the VPN can access the devices of the network. IoT device with a VPN can have many options to create a secure network.

2.3 Privacy Issues

IoT is about the transferring of information among different devices, individuals, and platforms. IoT devices assemble information for various reasons, such as improving proficiency and experience, decision-making, offering better assistance, and so forth; in this manner, the end purpose of information will be totally made sure about and defended [7].

2.4 Common Framework

There is a nonappearance of a typical structure; thus, all the manufacturers need to deal with the security and hold the protection all alone. When a typical normalized structure is implemented, the individual endeavors will then together be used in an expandable way; thus, the usability of code can be accomplished.

2.5 Automation

In the end, industries should manage increasingly more number of IoT devices. This tremendous measure of client information can be hard to oversee. The reality cannot be denied that it requires a solitary mistake or trespassing a solitary calculation to cut down the whole foundation of the information.

2.6 Updations

Dealing with the update of a huge number of devices should be practiced individually. Sometimes, it is required to update the IoT devices manually because they did not have the support of auto-update. One should monitor the accessible updates and apply the equivalent to all the various devices. This procedure becomes tedious and convoluted and if any error occurs in the process than this will prompt escape clauses in the security later. IoT includes the utilization of a large number of information focuses and each point ought to be made sure about. For sure, the need is for the multilayer security (security at every single level). From endpoint devices, cloud, embedded applications to web and versatile, applications that influence IoT, each layer ought to be security unblemished [8].

3 Literature Review

IoT technology is a framework, which makes devices of routine work smarter and everyday conversation develops educational. Many researchers are working on IoT. In this paper, we describe some existing work proposed by many researchers that are:

Atzori et al. [9] extraordinary visions of this IoT paradigm are reported and permitting technology reviewed. What emerges is that still essential troubles shall be faced by means of the studies community.

Lee et al. [10] proposed an encryption technique based on XOR manipulation, in place of complicated encryption along with the use of the hash characteristic, for anti-counterfeiting and privacy protection. The enhancement of the safety is defined, and hardware layout method is also established.

Abomhara et al. [11] classified risk types also examine, describe IoT devices and offer a model to detect invaders and assault.

Barnaghi et al. [12] present a semantic demonstrating approach for various segments in an IoT system. It is additionally talked about how the model can be incorporated into the IoT system by utilizing mechanized affiliation components with physical elements and how the information can be found utilizing semantic pursuit and thinking instruments.

Gubbi et al. [13] present a cloud-driven vision for overall usage of IoT. The key empowering technologies and applications areas that are probably going to drive IoT to inquire about sooner rather than later are talked about. A cloud usage utilizing Aneka, which depends on interaction of private and open Clouds, is introduced. They finished IoT vision by developing the requirement for convergence of WSN, the Internet and dispersed processing coordinated at innovative research network.

Xiao et al. [14] address the troubles appearing in device finding and interplay. They develop a person interoperable system to allow managers to operate through various devices of various settings by constant semantics and syntax. In the proposed framework, a parting method is used in which a device illustration technique for actual, but not unusual, and digital devices is created. A transformable tool is offered to ensure the right transformation of device semantics and syntax.

Zorzi et al. [15] summarize what in our opinion are the primary wireless—and mobility-related technical demanding situations that lie beforehand, and description a few initial thoughts on how such challenges can be addressed in an effort to facilitate the Internet of things' development and receipt within the next few years. We also pronounce a case study on the Internet of things protocol structure.

Hongsong et al. [16] **s**urvey to protection and consider in M2M gadget is important. Different visions of the M2M security and receive as accurate with standard are specified and studied on this paper. They comprise normal generation educations development and guard creation. All these will contribute to identify safety and outdated advancing in M2M machine.

4 Proposed Model of IoT Security

The layered architecture of IoT network consists of mainly six layers named as coding, perception, network, middleware, application, and business, shown in Fig. 2. Out of these six layers of IoT-layered architecture, three of them, perception, network, and application, are used to design the architecture of IoT security concerns. Every layer of IoT security architecture has its own communication and security protocols, standards, and components. Based on this security architecture of IoT, we have proposed a security model that could help us to protect from unwanted threats and attacks, un-authentication and protect our private information.

The proposed model is consisting of three stages of development that includes concerning of the security layers, security protocols, and database servers. Figure 4 shows the proposed model of IoT security concern.

Most appropriated protocols at different layers of security architecture of the proposed model are given as:

IEEE 802.11 Protocol at Perception layer: IEEE 802.11 defines a group of determinations created by the IEEE for wireless LAN (WLAN). IEEE 802.11 indicates an over-the-air interface between a remote device and a base station or between two remote devices. This standard is utilized related to IEEE 802.2 and is intended to inter-work consistently with Ethernet and is all the time used to convey Internet Protocol traffic.

6LowPAN Protocol at Network layer: The low-power personal area networks over IPv6 (6LoPAN) have characterized embodiment and header-compression systems which permit IPv6 packet to transmit over IEEE802.15.4-based systems.

SMQTT Protocol at Application layer: SMQTT stands for secure message queue telemetry transport protocol. The SMQTT is an extended version of MQTT, which used the lightweight parameter encryption. SMQTT comprises of 4 primary

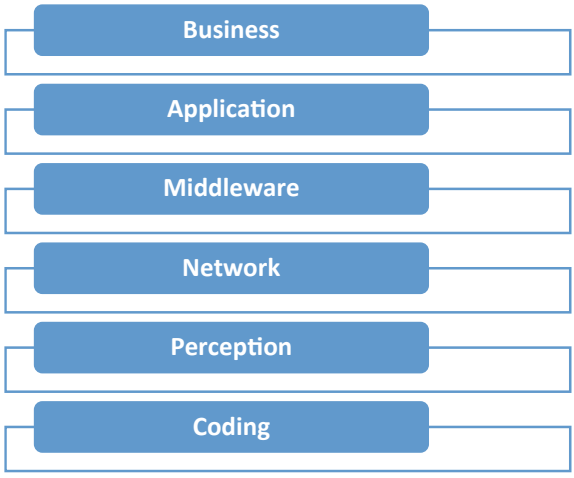

Fig. 2 IoT layered architecture

steps: setup, encryption, publishing, and decryption. In setup stage, subscribers and publishers register themselves to broker and get a master key as per the choose by key generation algorithm (KGA). At the point when the information is published, the data is encrypted and distributed by the broker which sends it to the subscribers, which is at last decrypted at the subscriber end having a similar master key.

4.1 Implementation of Proposed Model

Step 1: The first step of the proposed model consists of maintaining the security requirements of IoT security layer, like Access control, Privacy, Confidentiality, Integrity, Availability, Authorization, and Authentication, by using algorithms like Hash Algo, End-to-End authentication, Cryptography Algo, Access Control, Key Management, Intrusion Prevention System Encryption Protocol, Data privacy and integrity ACLs, Antivirus, Firewalls, and Risk Assessment from attacks like Node Capture, Fake Node, Denial of Service, Replay Attack, Node Jamming, Routing Threats, RFID Tag Spoofing and Cloning, Session Hijacking, Sybil, Flooding Attacks, Data access permission, Managing mass information and programming vulnerabilities (Fig. 3).

Step 2: In the subsequent step, i.e. step two, the security protocols or standards and security control mechanism for different layers of IoT security architecture have been described. The most appropriate communication protocols in perception layer are IEEE 802.11. The most suitable communication protocol for the network layer is 6LowPAN, which encapsulates the IPV6. SMQTT protocol is used for application layer of IoT security architecture.

Step 3: The third stage of the proposed model is database servers which store all data and parameters of security concern for every security layer, clients' profiles, security components errors, log records of the IoT framework, and access control records.

4.2 Flowchart of Proposed Model

Flowchart of the model for overall process is shown in Fig. 4 (On next page). The process is consisting of collecting the data from physical medium like sensor and converted into digital signal for further process. User can also give their instruction via user interface to control the system process. The digital signals are encrypted by using an appropriate key generation algorithm. The encrypted data is aggregated with the user data. With the interface of IoT gateway, the data is transmitted to database via web server, where the encrypted data is decrypted by using of same key and display to user. Meanwhile, the decrypted data is also stored in the database for future reference.

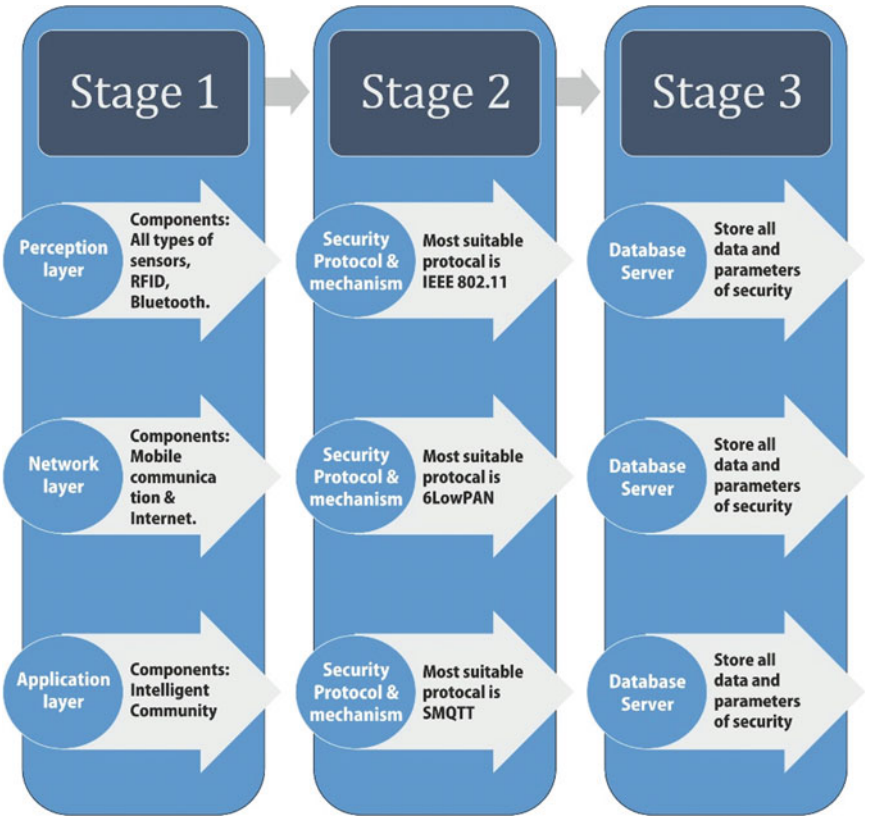

Fig. 3 Proposed Model of IoT Security Concern

5 Conclusion

The IoT framework is helpless against attacks at each layer. Subsequently, there are numerous security risks and prerequisites that should be dispatched. Current situation of research in IoT security is fundamentally focused on verification and access control conventions. However, with the quick development of innovation it is basic to merge new systems administration conventions like IPv6 and 5G to accomplish the dynamic blend of IoT technologies. The primary emphasis of this paper was to feature significant security issues of IoT. Especially, centering the security attacks and their countermeasures. The proposed model is capable enough to handle these attacks and threads to protect the sensitive data and private information. The main goal of the proposed security model is to choose and apply the appropriate security protocol and algorithm. By using these protocols and security algorithm, the system is capable enough to detect the problem and apply the suitable algorithm to protect the system from unavoidable unwanted situations. As we are aware that a lot of IoT

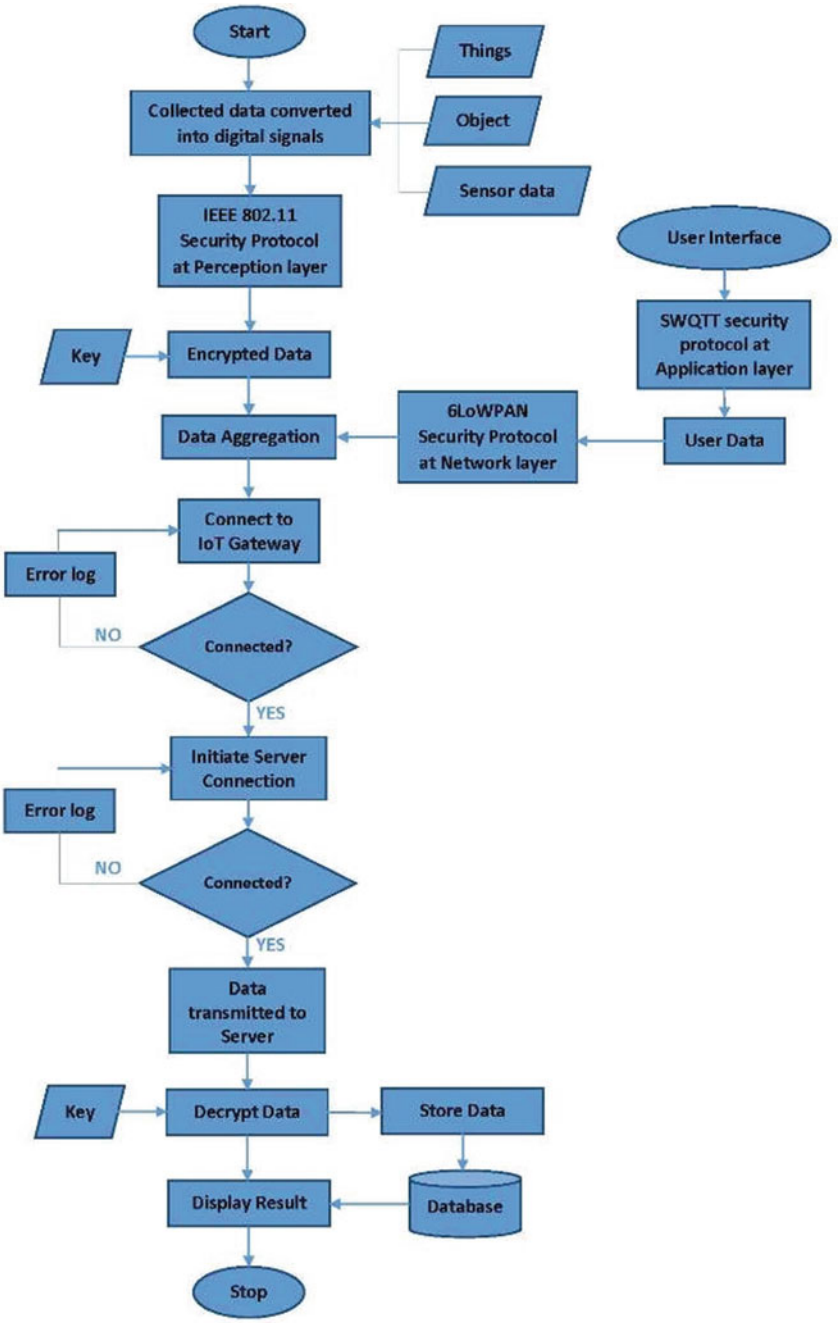

Fig. 4 Flowchart of the IoT security model

devices are come to be easy target. Indeed, even this isn't in the casualty's information on being contaminated. In this paper, the security prerequisites are additionally conferred for authentication, secrecy, integrity, and so on. In this paper, we study the existing work in this area. We have faith that this paper will be valuable for researchers in the field of security for IoT by assisting the significant issues in IoT security and giving better comprehension of the threats and their elements starting from different interlopers like intelligence agencies and organizations.

References

1. Koblitz N (1987) Elliptic curve cryptosystems. Mathematics of computation 48:203–209
2. Vignesh R, Samydurai A. 1 Student, 2 Associate professor security on internet of things (IOT) with challenges and countermeasures in 2017. IJEDR 5(1) ISSN: 2321-9939
3. Xie Y, Wang D (2014) An item-level access control framework for inter-system security in the internet of things. Appl Mech Mater 1430–1432
4. Anggorojati B, Mahalle PN, Prasad NR, Prasad R (2012) Capability-based access control delegation model on the federated IoT network. In: Int'l symposium on wireless personal multimedia communications (WPMC). 604–608
5. Castrucci M, Neri A, Caldeira F, Aubert J, Khadraoui D, Aubigny M et al (2012) Design and implementation of a mediation system enabling secure communication among critical infrastructures. Int'l J Crit Infrastruct Prot 5:86–97
6. Da Xu L, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Inf 10(4):2233–2243
7. Tarouco LMR, Bertholdo LM, Granville LZ, Arbiza LMR, Carbone F, Marotta M, de Santanna JJC (2012) Internet of things in healthcare: Interoperability and security issues. In: IEEE international conference on Communications (ICC) 2012. IEEE. pp 6121–6125
8. Mohan A (2014) Cyber security for personal medical devices internet of things. In: 2014 IEEE international conference on distributed computing in sensor systems (DCOSS). IEEE. pp 372–374
9. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805
10. Lee JY, Lin WC, Huang YH (2014) A lightweight authentication protocol for internet of things. In: Int'l symposium on next-generation electronics (ISNE). 1–2
11. Abomhara M, Køien GM Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks
12. De S, Barnaghi P, Bauer M, Meissner S (2011) Service modelling for the internet of things. In 2011 Federated conference on computer science and information systems (FedCSIS). IEEE. pp 949–955
13. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (iot): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660
14. Xiao G, Guo J, Xu L, Gong Z (2014) User interoperability with heterogeneous iot devices through transformation
15. Zorzi M, Gluhak A, Lange S, Bassi A (2010) From today's intranet of things to a future internet of things: a wireless-and mobility-related view. Wireless Commun IEEE 17(6):44–51
16. Hongsong C, Zhongchuan F, Dongyan Z (2011) Security and trust research in m2m system. In: 2011 IEEE international conference on vehicular electronics and safety (ICVES). IEEE. pp 286–290