R. Thirukkumaran and P. Muthu Kannan

4 Security issues and trust management schemes in Internet of things

Abstract: Internet of things (IoT) is an emerging research field in the network domain and is applied to almost all the applications that can change the people's lives as smart. Moreover, in some cases, large volumes of sensitive data could be generated. The number of security threats related to infrastructure, platform and application of IoT has been increased over the last few years. Hence, it is necessary to apply proper security solutions that ensure privacy and confidentiality of data. To address the secure and reliable communication, various trust-based solutions were introduced. Most of the nodes in IoT system are heterogeneous and have limited storage space. Many of the existing trust-based solutions could not be able to achieve this requirement. This chapter provides a detailed review of the security challenges and trust management techniques adopted for IoT to secure data in a cloud environment.

Keywords: Internet of things, M2M communication, threat analysis, IoT protocols, attacks

4.1 Introduction

The term Internet of things (IoT) is very popular in current research and industrial development [1]. In IoT, all the “things” also called as objects will be connected cooperatively to provide seamless communication and smart services. This enables “things” that can be accessed from anywhere at any time. In the beginning, M2M (machine-to-machine) communication protocols were focused by many researchers in the field of IoT, which are entirely different from the general communication of network in the aspect of deployment environment and the characteristics [2]. Along with the basic principles of authorization, integrity, authentication, availability and confidentiality, the network and security and privacy of the information should be equipped. IoT would be a significant part of the economy in the world rather than the Internet.

IoT is a technological revolution that has recently become more important to the real world as there are more than billion devices that connect to the Internet due to the growth of smart devices, embedded and ubiquitous communication technologies. The main components of IoT are the sensor, actuator, network, platform, services and users. IoT devices are combined with the cyber world to provide many smart services for different application domains like agriculture, energy, health care, retail market, logistics and industrial process [3]. They generate large volumes

of data that are valuable but not protected due to the nature of device constraints. The wireless sensor network (WSN) is one of the most important parts of IoT to collect data from end devices.

IoT and big data analytics are the promising technologies that address next-generation intelligence for various applications [4]. IoT applications promise to bring immense values into our lives. With newer wireless networks, superior sensors and revolutionary computing capabilities, the IoT could be the next frontier in the race for its share of the wallet [5]. A growing portion of IoT devices will be created in future, which includes connected vehicles, home automation, wearable technology, connected health, health-care analytics, industrial automation, smart agriculture, environmental monitoring and appliances with remote monitoring capabilities [6–8].

The communication between the IoT devices, cloud platform and users should consider proper security solutions to protect data because the sensor devices have limited capacity of power, computation and memory. IoT-enabled services are particularly creating and facing new challenges in security and privacy concerns. All the devices in the IoT are still subject to traditional security issues such as data confidentiality, integrity, availability and privacy. Intruders or attackers can target the data violation, bandwidth consuming and utilizing processing capacity of devices in the IoT-enabled network. The designing of security measures in IoT is quite challenging and should address the secure communication between sensor to sensor, the sensor to a gateway, gateway to server and server to the user.

4.2 IoT network components

IoT is an emerging and fast developing technology that connects billions or trillions of heterogeneous devices. The transformation process of interfacing, objects and smart devices to the network in order to function proficiently and remotely is the main objective of IoT. IoT is visualized as a completely connected world that makes it possible to represent the real world in a digital manner. The network interconnected devices implanted in the physical environment to improve the existing process [9]. Figure 4.1 illustrates various components of IoT network. IoT application covers most of the real-world business market like smart cities, industries, smart health and smart logistics.

4.2.1 IoT device

A sensor or an actuator along with the communication component constitutes an IoT device [10]. The principal component of IoT is sensor, which transmits the information gathered from the surrounding environment to the cloud server. There are

Figure 4.1: IoT network components.

numerous sensors available for various applications. Some of the usually utilized sensors are pressure sensor, sound sensor, temperature sensor, moisture sensor, light sensor, humidity sensor and others, in current and future applications. Sensors such as accelerometers are used for patient monitoring, biosensors for food testing, image sensor in surveillance, motion detectors in games and simulations.

IoT devices can make decisions locally, after aggregation and filtration of the collected information whenever central or global control is not required, reducing the processing and data transmission. By nature, IoT devices are heterogeneous, which vary in terms of communication protocols, computational and storage capabilities.

4.2.2 Connectivity

Connectivity represents the medium through which the gathered information from the IoT device is sent to the cloud infrastructure. The communication protocols such as Wi-Fi, ZigBee, radiofrequency identification, near-field communication, cellular networks, Bluetooth, wide area networks and satellite networks can be used to transport the collected data from the sensor to the cloud infrastructure [11]. Low-power wireless technologies such as Bluetooth, Wi-Fi, LoRaWAN and Z-Wave connect the smart devices and the sensors. Connectivity has its own advantages and disadvantages in terms of data transfer rate, efficiency and power.

4.2.3 Gateways

The data traffic between protocols and various networks are managed by the IoT gateway in a bidirectional manner. Gateway ensures the interoperability of the associated devices and sensors, also the translation of various network protocols. Configuration of the gateway includes the local preprocessing of the information gathered from a huge number of sensors before transmitting to the subsequent stages. In certain situations, it would be important due to the compatibility of the protocols such as Transmission Control Protocol (TCP) and Internet Protocol (IP). The information is transmitted through the IoT gateway ensuring network security with higher encryption standards. In order to protect the network from unauthorized access and malicious intruders, IoT gateway acts as a middle layer between the cloud and the devices.

4.2.4 Cloud

IoT generates large volume data from devices, applications, and users which must be managed in an efficient way. IoT cloud offers many service tools to collect, process, manage and store huge amount of data in real time [12]. It also provides a predictive analytics-based solution to enhance processes and products. To manage billions of devices and data traffic, IoT cloud is provisioned with high-performance server and storage. The application server, storage server, authentication and authorization server, message broker and IoT platform are the main components in the IoT cloud.

4.2.5 Services

An application consists of single or multiple services. It monitors and collects data from IoT devices and manages to store data. Further, it handles user authentication and access control policies. For example, in the smart city application environment monitoring, smart parking, transport system and water monitoring are the main services [13].

4.2.6 Users

User interface in the cloud environment provides the facility to interact user with the devices through different services [14]. By registering with different services, user can able to get the status of the devices and control it from anywhere. If any changes happened in the devices, the system generates alert and based on that user can react.

4.3 Security in IoT

In day-to-day life, the number of interconnected things drastically increases in various domains like industries, logistics, health and smart cities. More than 50 billions of interconnected devices are expected by 2020 [15]. Moreover, most of the IoT devices are resource-constrained devices due to their limited processing, memory and battery resources. When IoT devices are connected to the Internet, they are more vulnerable to the malicious attackers than PC and smart phones [16]. IoT devices generate a huge amount of valuable data like user location, health details and home security details that are unsecured due to lack of proper security protection.

IoT devices must authenticate themselves for each data communication between the server. When the IoT device or user wants to connect to the network, it should correctly identify their identity and credentials to grant access for authorization [17]. IoT is an emerging and fast developing technology but has no proper reference model and standards. It leads most of the security solutions that are not applicable to the IoT environment. New security solutions should be implemented to enhance the protection level of the IoT devices [18]. The explosion of the number of devices and users generates a large amount of data and it brings a new set of risk and security threats. The important challenges due to various technologies that drive and move forward the IoT into next level are discussed by Tan et al. [19].

Through the study of existing available resources, it has been clearly stated that IoT devices and users are severely affected by various security threats. Major security issues in IoT are the insecure network services, insecure web interface, insecure mobile interface, insecure cloud interface, insufficient authentication, insufficient authorization and lack of security configuration. Hence, it leads to a serious requirement for analyzing different security challenges in the IoT network.

Proactive measures such as cryptography and authentication are implemented as a first-line defense method. These mechanisms effectively protect the attacks from outside the network but fail to detect them from inside the network. The reactive measures are detection mechanism that dynamically monitors and decides whether the events are normal or of an attack. This research focuses on the reactive mechanism.

4.4 Security threats

The number of security threats directly relates to IoT devices that have increased over the last years [20]. The threats and risks are listed in Table 4.1. It shows that attacks take place at different levels in the infrastructures and throughout the process involved in the IoT ecosystem. The major attacks and their impacts are discussed in this section.

Table 4.1: Security threats and impacts.

Threat	IoT device	Platform	Infrastructure	Data	Communication	Decision	Application
Malware	✓	✓	×	×	×	×	×
Exploit kits	✓	×	✓	×	×	×	×
Targeted attacks	×	✓	✓	✓	×	×	×
DDoS	✓	✓	✓	×	×	×	×
Counterfeit	✓	×	✓	×	×	×	×
Attacks on privacy	✓	✓	×	✓	×	×	×
Modification of data	✓	✓	×	✓	×	×	×
Man in the middle	✓	×	×	✓	✓	×	×
Protocol hijacking	✓	×	×	✓	✓	✓	×
Session hijacking	✓	×	×	✓	✓	×	×
Data interception	✓	×	×	✓	✓	×	×
Network reconnaissance	✓	×	✓	✓	✓	×	×
Data gathering	✓	×	×	✓	✓	×	×
Replay of messages	✓	×	×	✓	×	✓	×
Data leakage	✓	✓	×	✓	×	×	×
Software vulnerabilities	✓	✓	✓	×	×	×	✓
Device modification	✓	×	×	×	✓	×	×

✓ represents the impact; × the no impact

4.4.1 IoT attacks

Against IoT device

This type of attackers modifies the configuration of sensors and actuators like generate out-of-range sensor values and changing the threshold value of the sensor to detect the event during installation time. Due to wireless nature, sensor network has led to the vulnerability of attacks either from inside or outside the networks. If one sensor were compromised, it could be identified by using the readings obtained from another sensor [21]. But in IoT, large number of sensors are deployed and attack also targeted to multiple devices at the same time. Packet dropper, data modifier, selfish node, Sybil, node replication, flooding, distributed denial of service (DDoS) and man in the middle are some of the attacks found in sensor networks [22–29].

Against server

This type of attacker comprises different stages to gain the server admin control of an IoT system [30]. It can be easily achieved if a weak authentication method is used. An attack in IoT admin server could affect the communication between devices and disabled the devices.

Against the network link between controller and actuators

The main impact of this type of attack is the leakage of sensitive and operational information. The advanced persistent threat (APT) attacks, eavesdropping and information gathering are the types of attack that identify a weak spot in the network and devices and further it can able to do attack and malicious activities [31].

4.4.2 Method of attacks

Exploits

This type of exploitation is successful. It creates an entry point to the system and may crash the system, making it as the unstable one. These exploits are generated by malware and are used to get access to an unauthorized restricted system. It is worked as part of a larger attack and leads to launch of other malicious contents to the network.

Command inject

This type of attacker launches or injects command into IoT devices and executes malfunction remotely through a console. If one system is getting compromised through that machine, then the attacker is able to attack another system in the same environment. It creates a chain of multiple compromised devices.

Steppingstone attack

This is one of the anonymous attacks used by the intruders by hiding their identities. In the first step, the attacker compromises some nodes in the network. Then by using that compromised node identity, attacker moves a step forward to attack another set of nodes in the network. Further, this process is continued to attack the entire network.

IoT botnet

This type of attack finds the list of vulnerable devices in IoT by sending exploits and enrolling them into botnet after that it launches a DDoS attack, flooding attack, and targets the server with malicious traffic [32].

Ransomware

It has many possible targets within the IoT through malware patching into the system. This type of attack blocks the access of data from the victim and also its request to pay for access grant. It can able to hold a power grid, a smart thermostat and a hospital system, and makes the risk for the safety of the people [33].

4.4.3 Security challenges in IoT

Security is a very important aspect as well as a challenge for implementing IoT solutions, rather than considering the benefit of IoT, where inappropriate access and privacy are the main categories of the top list [34]. Moreover, it is necessary to maintain proper authorization because these devices are open networks in which any device can join and communicate with any other devices [35]. With the adoption of new technologies, the IoT environment has become complex, and privacy issues have become more complicated [36]. Furthermore, because of terminal equipment, network structure, scene and other factors of IoT, these concerns are rising,

respectively [37]. Moreover, with a traditional firewall or authentication, protocols or keychain pair might not offer a solution [38].

From the aspect of security and technology, the safety of IoT especially accesses control of miniaturized things that have become the most challenging one. Hence, the access control system (ACS) design will address features such as a solution to eradicate the threats of privacy and security, related with IoT, the solution to protect security [39]. Most of the existing access control methods are based on role-based access control (RBAC), attribute-based access control (ABAC) and access control list (ACL) [40].

ACS allows accessing resources like IoT device, sensor or URL file only for authorized users [41]. Due to lower bandwidth in IoT devices, low power requirements, ad hoc and distributed systems nature, a unique set of access control challenges are increasing. The standard authorization models must be analyzed in depth before applying them to the IoT.

The role of wireless infrastructure in IoT applications is expected to become more prominent with the deployment of mobile nodes and WSNs [42]. If the WSNs are being open to Internet connectivity, it becomes more vulnerable to attackers from anywhere in the world [43]. The important challenges due to various technologies that drive and move forward the IoT into next level are discussed in this section [44].

Availability

To achieve persistent connectivity between end devices, users and their respective services, new technologies have to be designed [45]. The power constraints of lightweight endpoints should be addressed in secure communication. Low-power wide area network should be implemented with the same level of security used in recent mobile communication [46]. During the migration of the IoT endpoints across network boundaries, the same level of security should be supported by the multiple mobile operators [47], which need to address how the network trust can be forwarded from gateway to endpoint communication.

Identity

In an IoT product or service echo system end-point device should be securely identify itself to its peers and services. This is a critical and fundamental aspect to guarantee the data is being delivered to the certified peers and services [48]. In IoT environment services and peers should verify the identity of the end-user and end-point device. Focusing security technology should be capable of securely authenticating peers and services. The identity of a device should be secured from tampering and manipulation.

Privacy

Privacy must be designed to ensure that each action is authorized, device identity is verified, and the data are not exposed to unauthorized users [49]. All the physical world entities are directly affected by digital world actions. It should be considered during the design of the architecture of the endpoint device or service.

Scalability

Scalability is defined as that increase in the number of nodes after the deployment of WSN [50]. The expansion support of the networking protocol is very important in the design of the protocol. The design of the services, protocols and the endpoint devices should ensure that they are scalable under varying load conditions.

Secure routing

Routing and data forwarding is an important service for allowing communication in WSNs and IoT [51]. Existing routing protocols suffer from several security vulnerabilities.

To overcome different security threats in the IoT network, the trust-based mechanism is developed; hence, the next section provides a detailed review of existing trust-based security mechanism adopted in IoT

4.5 Trust management in IoT

This section briefs the existing trust management (TM) schemes and their related application. Further, the challenges in trust-based security solutions and the outcome of this survey are outlined.

4.5.1 Trust management

TM plays a vital role in IoT for enhanced user information security and privacy, for the process of data fusion and data mining and for the qualified data services with intelligence, whereas reputation is a measure to assess the trust level which is put into an entity that is derived from the experiences or knowledge (direct or indirect) on earlier interactions of entities [52].

Trust

The behavior of the node or data is classified as good or bad based on the trust value. A trustor and a trustee are the two entities involved in a trust relationship, and for mutual benefits, they rely on each other. The relationship of trust resides in the context such as the trust environment, the purpose of the trust, and the risk of trust [53].

Direct trust

Direct trust is a technique which is based on experiences or observations, direct interactions between the two entities that are the trustor node and the trustee node [54].

Indirect trust

In indirect trust, there are no past interactions or experiences for the trustor and the trustee. In such a scenario, based on the recommendations and opinion of the other nodes trust is built [55]. Indirect trust can be established if a subject node cannot directly observe the communication behaviors of the object node.

Recommended trust

Recommended trust calculates filtered reliable recommendations. The third-party recommendations are not reliable. Therefore, an effective solution needs to be addressed to detect and filter unreliable recommendations [56].

4.5.2 Trust management model

Most of the existing work calculates the trust value based on node behavior. In the wireless multihop environment, cooperation among neighbor nodes is important. The various applications of trust-based solution for the wireless environment are data aggregation, routing, node selection, localization and malicious attacker detection. Based on the management scheme, trust models can be classified into centralized and distributed. In the distributed approaches, all the participating nodes can be able to calculate their trust values. The base station or any server is used to calculate the trust value for all nodes in the centralized approach. This approach may not be suitable for all applications because this management consumes more energy. In the IoT context, both distributed and centralized approaches can be used

in the different level. The distributed approach is used for device–device communication and centralized approach is used in the user ACS [57].

Several studies developed TM models to enhance security and privacy but based on the architecture modeling of IoT [58]. This research splits IoT into three layers based on the network composition of IoT, namely the application layer, the core layer, and the sensor layer. TM mechanism is deployed in these layers for multiservice, effective routing and malicious detection [59]. The selection of metrics is based on the kind of attacks that we are going to defend. In each layer different metrics are collected for trust calculation. The selection of a computing method is also an important one. Some of the methods are a weighted average method, probability theory, fuzzy logic, game theory and machine learning concepts. The trusted authority or ACS is responsible for taking the final decision based on trust information.

4.5.3 Trust-based applications

TM scheme provides solutions for security issues in routing, clustering, target localization, malicious node detection and ACS. In this section, applications of trust model are discussed.

Routing

Routing is generally carried in IoT for the sensor network, which is used for multi-hop communication [60]. From the sensor devices, data should be forwarded through intermediate nodes to the base station or gateway. Presence of malicious nodes in the network causes the routing behavior. This section discusses the implementation of secure routing through TM scheme.

Airehrour et al. [61] introduced a lightweight trust-based routing framework called SecTrust. The trust value is calculated based on the past successful interactions of the IoT device communication. Based on the trustworthiness, routing attackers are isolated from the network.

Khan et al. [62] illustrated a resilient routing mechanism for low power and lossy network using the trust. Each node in the network computes trust value using trust metrics like belief, disbelief and uncertainty.

Cluster

The IoT devices are grouped together to form a cluster. The clustering method provides an efficient way to forward data from devices to base station or gateway. Cluster-based techniques in IoT achieve energy efficient by minimizing the number of

control packets used in network communication. The selection of cluster head (CH) is challenging in terms of selection parameter and selection method. Many techniques were proposed to select CH and cluster member (CM) assignment. The CH selections are broadly classified as centralized and distributed. In IoT context distributed approach gives good performance [63]. CM senses the environment and sends the information to CH. Further, it forwards to base station or gateway in most of the IoT-enabled WSN application scenario. Many trust-based solutions and access control methods are proposed for secured communication [64]. The objective of secure, energy and bandwidth-aware CH selection is not addressed by many of the research work. In general, CH is elected based on node degree, delay, distance and energy.

Rani et al. [65] illustrated a minimum energy consumption chain-based cluster coordinator algorithm (ME-CBCCP) for the energy-efficient IoT. A hierarchical network design was introduced based on different communication levels like local cluster communication, intercluster communication and cluster-to-base station communication. The cluster coordinators balance the load of the CH. The network lifetime and delay performance of the ME-CBCCP were analyzed.

Tsai and Chen [66] presented virtual CH election method for the WSN. By applying virtual ID concept, it avoids nearby CHs and also fully covers all cluster nodes. For energy-efficient CH election highest residual energy parameter is also considered. The performance analysis carried in terms of the number of live nodes, energy consumption and the number of CH elected.

Praveen Kumar Reddy and Rajasekhara Babu [67] demonstrated the CH election method using the combination of gravitational search algorithm and artificial bee colony algorithm for the IoT-enabled WSN. It takes the distance, delay, energy, load and temperature parameters of the sensor devices to select the CH. The performance of this algorithm analyzed in terms of network sustainability and convergence evaluation.

John et al. [68] introduced a dynamic CH election method for IoT applications. The large-scale network area is divided into small clusters with a minimum coverage area by using the Voronoi diagram. The CH is selected at two stages. First one is based on perceived probability and the second one is based on survival time estimation method. The performance analysis shows the improvement in energy savings and network lifetime.

Karthick [69] demonstrated a secure and energy-aware routing protocol for the WSN. At the initial stage, k -means clustering is used later on based on link quality appraisal parameter of nodes' grade points. By using trust and distrust concept, secure path is established. The performance of the proposed system is analyzed in terms of throughput, delay and energy consumption.

Bader et al. [70] presented a CH selection scheme for IoT-enabled sensor network by using trust value. Only the trusted nodes were selected as CH. The trust value is computed based on successful interaction. The forgetting factor is used to assign a different weight value for old entries in the history.

Secure localization

Target localization and tracking is an important application for IoT. To track the exact location of the moving object and to find the event-generated position are challenging one. The location spoofing attacks are the major risk of implementing localization in IoT. The localization method utilizes the reference position information from the neighbor nodes. If the reference node is a malicious node, then the result of the localization will get an error. Several existing methods are proposed to avoid malicious nodes. This section discusses some of the secure localization methods used in IoT environment.

Zhang et al. [71] demonstrated secure localization using a trust evaluation method called trust-based secure localization. Final trust value is computed based on identity and behavior. The identity is evaluated based on an authentication method. If the authentication fails, the parameter is set to zero. The behavior evaluation parameter is calculated by using both self-evaluation and reference evaluation method. It uses transmission radius of the beacon node and distance between the position claimed node and the position estimated node. For the attackers, the final trust value will be low. To find the localization of the node, the reference location information is gathered from trustworthy nodes. This method ensures the secure location information.

Chen et al. [72] presented a detailed survey about security and privacy issues in localization, location information and location-based services. Cryptographic solutions were addressed to secure localization.

Zhang et al. [73] presented the framework of secure location of things for geospatial tagging in the IoT. Further, the impact of spoofing attacks in traditional localization algorithm was analyzed. Based on the reachability of access point the suitability information is scored. This algorithm calculates the maximum likelihood estimator to find the tag location.

Access control system

ACS allows accessing resources like sensors, actuators, medical equipment and data in the server only for authorized users. Due to lower bandwidth between the Internet and IoT devices, low power requirements of IoT devices, network ad hoc, systems distributed nature, a unique set of access control challenges are presented by IoT. The standard authorization models must be analyzed in depth before applying them to the IoT, which includes RBAC, ABAC and ACL.

Mahalle et al. [74] presented trust-based access control using the fuzzy approach based on identity management using the trust level. To address access control in IoT, the fuzzy-based approach for trust calculations deals with the linguistic information of devices. Simulation results demonstrate that the fuzzy approach for trust-based

access control guarantees scalability and it is energy efficient. Finally, the most important works that emphasize access control in an IoT environment are discussed.

Yeh et al. [75] developed a technique of cloud-based fine-grained in health care for access control using lightweight IoT devices with attribute revocation functions and data dynamics auditing. This proposed scheme handles the problem of cloud reciprocity, wherein cloud service providers reduce the amount of data loss that occurs in the network system. Experimental analysis of the results shows that the proposed approach exhibits significant security analysis and performance comparisons, which makes it an excellent design for cloud-based PHI system.

Authorized users of each resource are stored by the ACL, that is, the matrix of access control that stores in a row-wise order. This is a major challenge for IoT because it is hard to update the user list in a distributed system due to low processing power in devices [76].

A widely used protocol is an RBAC system that designs and builds access control. It provides security for the system regarding authorization, but the ACS and authentication provide critical functionalities even in the Internet resource access. Further, there are three perspectives of role-based access model such as the end user, access control and administrator [77].

A different approach to authorization is provided by ABAC as it provides access based on specific attributes of the user [78]. By combining both attributes and other data such as Mac address, the location and IP address, this method provides a better ACS. It combines various attributes to make a context-aware decision instead of using an authorized user role for a sensor at runtime [79].

4.5.4 Challenges in trust-based security solutions

Trust and reputation system face some of the challenges such as heterogeneity, scalability, infrastructure, identity, integrity, and network resources.

Trust and reputation systems must consider the heterogeneity as the first challenge. Because the future Internet will exhibit high heterogeneity levels like web-enabled, digital virtual and cyber-physical [80]. The second challenge is scalability. To stay fully functional, the trust and reputation system must scale with the growth in the number of devices [81]. Trust and reputation systems must consider infrastructure as the third challenge. Because it collects information from the public area. Most of the entities need others to interact with them and also they must be able to find them within the network [82]. Both challenges and the opportunity to improve security are offered by identity management in IoT [83]. The underlying mechanism and identity of things are not the same, and it is the most important aspect of this challenge [84].

The prevention of unauthorized modification to hardware and software is ensured by the concept of integrity. Authorized or unauthorized personnel does not

do an unauthorized modification of data, and that data should be internally and externally consistent [85]. The last challenge is exhibited from connections of various things and different network capabilities [86]. This means that bandwidth, availability and the latency difference must be considered especially if certain aspects of the interactions are critical in a time.

4.5.5 The outcome of the survey

To design efficient trust-based security solution, the following set of points needed to be considered:

Trust model should be lightweight and easy to implement. Trustworthiness of the nodes should be continuously updated. If the numbers of interactions between the nodes are increased, the trust value can be able to achieve a good level of accuracy. For the recommendation approaches, we need to select proper filtering and aggregation models to remove unwanted recommendation. Trust model should consider different attacks. Need more flexibility to integrate data trust, device trust and user trust based on the application use-case.

4.6 Conclusion

To protect the data in an IoT network, TM scheme has been widely used and hence this review examines the TM scheme for securing data in the IoT in different aspects. The chapter reveals that even though the TM scheme provides a significant advantage for various threats, yet it requires some effective modification.

References

- [1] Da Xu, Li., Wu, He. and Shancang, Li. Internet of Things in industries: A survey, IEEE Transactions on Industrial Informatics, 10(4), 2013, pp. 2233–2243.
- [2] Sathish Kumar, J. and Patel, Dhiren R.. A. survey on Internet of Things: Security and privacy issues, International Journal of Computer Applications, 90(11), 2014, pp. 20–26.
- [3] Sarowar, M G., Kamal, M S. and Dey, N. Internet of Things and its impacts in computing intelligence: A comprehensive review–IoT application for big data, In Big Data Analytics for Smart and Connected Cities (pp. 103-136). Hershey, PA: IGI Global, doi:10.4018/978-1-5225-6207-8.ch005.
- [4] Elhayatmy, G., Dey, N. and Ashour, A S. (Eds.)Internet of Things based wireless body area network in healthcare, In Internet of things and big data analytics toward next-generation intelligence, Cham : Springer, 2018, pp. 3–20.
- [5] Dey N., Hassanien, A. E., Bhatt, C., Ashour, A. and Satapathy, S C. (Eds.). Internet of things and big data analytics toward next-generation intelligence, Berlin : Springer, 2018.

- [6] Hassanien, A. E., Dey, N., and Borra, S. (Eds.). *Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications*, CRC Press, 2018.
- [7] Bhatt, C., Dey, N., and Ashour, A. S. (Eds.). *Internet of things and big data technologies for next generation healthcare*, 23, New York : Springer, 2017.
- [8] Dey, N. Ashour, A. S. and Bhatt C. (Eds.) *Internet of things driven connected healthcare*, In *Internet of things and big data technologies for next generation healthcare*, Cham : Springer, 2017, pp. 3–12.
- [9] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. Internet of Things (IoT): A vision, architectural elements and future directions, *Future Generation Computer Systems*, 29(7), 2013, pp. 1645–1660.
- [10] Jovovic, I., Forenbacher, I. and Perisa M. Massive machine-type communications: An overview and perspectives towards 5G, 3rd International Virtual Research Conference in Technical Disciplines, DOI: 10.18638/rcitd.2015.3.1.73 2015.
- [11] Atzori, L., Iera, A. and Morabito, G. The Internet of Things: A survey, *Computer Networks*, 54 (15), 2010, pp. 2787–2805.
- [12] Kantarci, Burak and Mouftah, Hussein T. Trustworthy sensing for public safety in cloud-centric Internet of Things, *IEEE Internet of Things Journal*, 1(4), 2014, pp. 360–368.
- [13] Mohammed, Farah Hussein. and Esmail, Roslan. Survey on IoT services: Classifications and applications, *International Journal of Science and Research, IJSR*, 4(1), 2015, pp. 2124–2127.
- [14] Shelby, Zach. Embedded web services, *IEEE Wireless Communication*, 17(6), 2010, pp. 52–57.
- [15] Asghar, MH., Negi, A. and Mohammadzadeh, N. Principle application and vision in Internet of Things (IoT), *International Conference on Computing, Communication & Automation, IEEE*, 2015, pp: 427–431.
- [16] Padmavathi, G., Shanmugapriya, D. A survey of attacks, security mechanisms and challenges in wireless sensor networks, *International Journal of Computer Science and Information Security, IJCSIS*, 4(1 & 2), 2009, pp. 1–9.
- [17] Kim, Hokeun., Wasicek, Armin., Mehne, Benjamin and Lee, Edward A. A secure network architecture for the Internet of Things based on local authorization entities, *IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud*, 1, 2016, pp. 114–122.
- [18] Waz, Ibrahim R., Sobh, Mohamed Ali and Ayman, M Bahaa-Eldin. Internet of Things (IoT) security platforms, 12th International Conference on Computer Engineering and Systems, ICCES, 2017, pp. 500–507.
- [19] Tan, L. and Wang, N. Future internet: The Internet of Things, 3rd International Conference On Advanced Computer Theory and Engineering, ICACTE, 2010, pp. 376–380.
- [20] Gautam, G. and Sen, B. Survey on different types of security threats on wireless sensor networks, *International Journal of Computer Science and Information Technologies*, 6(1), 2015, pp. 770–774.
- [21] Cai, Jiwen., Ping Yi, Jialin Chen, Zhiyang Wang and Ning Liu. An adaptive approach to detecting black and gray hole attacks in ad hoc network, *IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 775–780
- [22] Wang, Chuang, Feng, Taiming, Kim, Jinsook, Guiling, Wang and Zhang, Wensheng. Catching packet droppers and modifiers in wireless sensor networks, *IEEE Transactions on Parallel and Distributed Systems*, 23(5) 2012, pp. 835–843.
- [23] Prathap U., Shenoy, P. D. and Venugopal, K. R. CPMTS: Catching packet modifiers with trust support in wireless sensor networks, *IEEE International WIE Conference on Electrical and Computer Engineering, WIECON-ECE*, 2015, pp. 255–258.
- [24] Sowmyadevi, D. and Karthikeyan, K. Merkle-Hellman knapsack-side channel monitoring based secure scheme for detecting provenance forgery and selfish nodes in wireless sensor

- networks, 2017 Second International Conference on Electrical, Computer and Communication Technologies, ICECCT, 2017.
- [25] Zhang, K., Liang, X., Lu, R., and Shen, X. Sybil attacks and their defenses in the Internet of Things, *IEEE Internet of Things Journal*, 1(5) 2014, pp. 372–383.
 - [26] Chia-Mu, Yu., Tsou, Yao-Tung, Chun-Shien Lu. and Kuo, Sy-Yen. Localized algorithms for detection of node replication attacks in mobile sensor networks, *IEEE Transactions on Information Forensics and Security*, 8(5), 2013, pp. 754–768.
 - [27] Kamaldeep, Malik M., and Dutta, M. Contiki-based mitigation of UDP flooding attacks in the Internet of things, 2017 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2017, pp. 1296–1300.
 - [28] Yan, Q., Yu, F. R., Gong, Q. and Li, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges, *IEEE Communications Surveys & Tutorials*, 18(1), 2016, pp. 602–622.
 - [29] Xu, Y., and Liu, F. Hybrid key management scheme for preventing man-in-middle attack in heterogeneous sensor networks, 2017 3rd IEEE International Conference on Computer and Communications, ICC3, 2017, pp. 1421–1425.
 - [30] Shikha Singh, Binay Kumar Pandey, Ratnesh Srivastava, Neharawat, Poonamrawat and Awantika. Cloud computing attacks: A discussion with solutions, *Open Journal of Mobile Computing and Cloud Computing*, 1(1), 2014, pp. 1–7.
 - [31] Liao, CH., Shuai, HH. and Wang, LC. Eavesdropping prevention for heterogeneous Internet of Things systems, 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018.
 - [32] Hachinyan, O., Khorina, A. and Zapechnikov, S. A game-theoretic technique for securing IoT devices against Mirai botnet, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 2018, pp. 1500–1503.
 - [33] Sajjan, R. S. and Ghorpade, V. R. Ransomware attacks: Radical menace for cloud computing, International Conference on Wireless Communications, Signal Processing and Networking WiSPNET, 2017, pp. 1640–1646.
 - [34] Jin-cui, Yang and Bin-xing, Fang. Security model and key technologies for the Internet of things, *The Journal of China Universities of Posts and Telecommunications*, 18(2), 2011, pp. 109–112.
 - [35] Godha, R., Prateek, S. and Kataria, N. Home automation: Access control for IoT devices, *International Journal of Scientific and Research Publications*, 4(10), 2014, pp. 1–4.
 - [36] Pereira, Pablo Punal, Eliasson, Jens and Delsing, Jerker. An authentication and access control framework for CoAP-based Internet of Things, 40th Annual Conference of the IEEE Industrial Electronics Society ECON, IEEE, 2014, pp. 5293–5299.
 - [37] Fielding, R. T. and Taylor, R. N. Principle and design of the modern web architecture, *ACM Transaction Internet Technol*, 2(2), 2002, pp. 115–150.
 - [38] Song, Y. Security in Internet of Things, THES, school of information and communication technology (ICT), KTH, <http://kth.diva-portal.org/smash/get/diva2:702223/FULLTEXT01.pdf>, 2013.
 - [39] Liu, Jing, Xiao, Yang and Philip Chen, C.L. Internet of Things' authentication and access control, *International Journal of Security and Networks*, 7(4), 2012, pp. 228–241.
 - [40] Cruz-Piris, L., Rivera, D., Marsa-Maestre I., De La Hoz, E. and Velasco, J.R. Access control mechanism for IoT environments based on modelling communication procedures as resources, *Sensors (Switzerland)* 18(3), 2018, pp. 917.
 - [41] Ouaddah, Aafaf, Bouij-Pasquier, Imane, Abou Elkalam, Anas and Ait Ouahman, Abdellah. Security analysis and proposal of new access control model in the Internet of Thing, International Conference on Electrical and Information Technologies, ICEIT, IEEE, DOI: 10.1109/EITech.2015.7162936.2015

- [42] Duan, J., Gao, D., Yang, D., Foh, C.H., and Chen, H-H. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications, *IEEE Internet of Things Journal*, 1(1), 2014, pp. 58–69.
- [43] Fagen, Li. and Xiong, Pan. Practical secure communication for integrating wireless sensor networks into the Internet of Things, *IEEE Sensors Journal*, 13(10), 2013, pp. 3677–3684.
- [44] Said, Omar and Masud, Mehedi. Towards Internet of Things: survey and future vision, *International Journal of Computer Networks IJCN2013*, 5(1), 2013, pp. 1–17.
- [45] Proano, Alejandro and Lazos, Loukas. Packet-hiding methods for preventing selective jamming attacks, *IEEE Transactions On Dependable And Secure Computing*, 9(1), 2012, pp. 101–114.
- [46] Petajajarvi, Juha, Mikhaylov, Konstantin, Pettissalo, Marko, Janhunen, Janne and Jarilinatti. Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage, *International Journal of Distributed Sensor Networks*, 13(3), 2017, pp. 1–16.
- [47] Khan, R., Khan, S. U., Zaheer, R. and Khan, S. Future internet: The internet of things architecture, possible applications and key challenges, *10th International Conference On Frontiers of Information Technology (FIT)*, 2012, pp. 257–260.
- [48] Keoh, Sye Loong, Kumar, Sandeep S and Tschofenig, Hannes. Securing the Internet of Things: A standardization perspective, *IEEE Internet Of Things Journal*, 1(3), 2014, pp. 265–275.
- [49] Tabane, Elias and Zuva, Tranos. Is there a room for security and privacy in IoT?, *International Conference on Advances in Computing and Communication Engineering, ICACCE*, 2016, pp. 260–264.
- [50] Compton, M., Barnaghi, P., Bermudez, L., Garca-Castro, R., Corcho, O., Cox, S., Graybeal, J., Hauswirth, M., Henson, C., Herzog, A., Huang, V., Janowicz, K., Kelsey, W. D., Phuoc, D. L., Lefort, L., Leggieri, M., Neuhaus, H., Nikolov, A., Page, K., Passant, A., Sheth, A., and Taylor, K. The SSN ontology of the W3C semantic sensor network incubator group, *Journal of Web Semantics*, 17, 2012, pp. 25–32.
- [51] Teng, Liping and Zhang, Yongping. SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks, *2nd International Conference on Computer Modeling and Simulation*, 2010, pp. 79–82.
- [52] Chen, I.R., Guo, J. and Bao, F. Trust management for service composition in SOA-based IoT systems, *IEEE Wireless Communications and Networking Conference, WCNC*, 2014, pp. 3444–3449.
- [53] Yan, Z., Zhang, P. and Vasilakos A.V. A survey on trust management for Internet of Things, *Journal of Network and Computer Applications*, 42, 2014, pp. 120–134.
- [54] Eder, T., Nachtmann, D. and Schreckling, D. Trust and REPUTATION in the Internet of Things, conference seminar ss2013 – real life security (5827HS), https://web.sec.uni-passau.de/projects/compose/papers/Eder_Nachtmann_Trust_and_Reputation_in_the_Internet_of_Things.pdf, 2013.
- [55] Raha, A., Naskar, M. K., Chakraborty, A., Alfandi, O. and Hogrefe, D. A novel indirect trust based link state routing scheme using a robust route trust method for wireless sensor networks, *5th International Conference on New Technologies, Mobility and Security, NTMS*, 2012.
- [56] Govindan, K., and Mohapatra, P. Trust computations and trust dynamics in mobile ad hoc networks: A survey, *IEEE Communications Surveys & Tutorials*, 14(2), 2012, pp. 279–298.
- [57] Boswarthick, D., Elloumi, O., and Hersent, O. (2012). *M2M Communications: A systems approach*. Hoboken, NJ: ETSI. 2012.
- [58] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. Internet of Things (IoT): A vision, architectural elements and future directions, *Future Generation Computer Systems*, 29(7), 2013, pp. 1645–1660.

- [59] Lize, G., Jingpei, W. and Bin, S. Trust management mechanism for Internet of Things, *China Communications*, 11(2), 2014, pp. 148–156.
- [60] Zhu, Jianping, Tao, Zhengsu and Chunfeng Lv. Performance improvement for IEEE 802.15.4 CSMA/CA scheme in large-scale wireless multi-hop sensor networks, *IET Wireless Sensor Systems*, 3(2), 2013, pp. 93–103.
- [61] Airehrour, David, Gutierrez, Jairo and Ray, Sayan Kumar. A Lightweight Trust Design for IoT Routing, *IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, Auckland, New Zealand, IEEE, pp. 552–557, 2016
- [62] Khan, Zeeshan Ali, Ullrich, Johanna, Voyiatzis, Artemios G and Herrmann, Peter A. Trust-based resilient routing mechanism for the Internet of Things, *12th International Conference on Availability, Reliability and Security, ARES*, 2017.
- [63] Hamzeloei, Fahimeh, Dermany, Mohammad Khalily. A TOPSIS based cluster head selection for wireless sensor network, *Procedia Computer Science*, 98, 2016, pp. 8–15
- [64] Al-Hamadi, Hamid and Chen, Ing-Ray. Trust-based decision making for health IoT systems, *IEEE Internet of Things Journal*, 4(5), 2017, pp. 1408–1419.
- [65] Rani, Shalli, Talwar, Rajneesh, Malhotra, Jyoteesh, Ahmed, Syed Hassan, Sarkar, Mahasweta and Song, Houbing. A novel scheme for an energy efficient internet of things based on wireless sensor network, *Sensors*, 15(11), 2015, pp. 28603–28626.
- [66] Tsai, Ming-Yu and Chen, Yaw-Chung. A virtual cluster head election scheme for energy-efficient routing in wireless sensor networks, *3rd International Conference on Future Internet of Things and Cloud*, 2015, pp. 341–348.
- [67] Praveen Kumar Reddy M. and Rajasekhara Babu M. Energy efficient cluster head selection for Internet of Things, *New Review of Information Networking*, 22(1), 2017, pp. 54–70.
- [68] John, Aniji, Rajput, Anagha, Babu, Vinoth. Dynamic cluster head selection in wireless sensor network for internet of things applications, *IEEE International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology, ICIEEIMT*, (2017), pp 45–48.
- [69] Karthick, Suyambu. TDP: A novel secure and energy aware routing protocol for wireless sensor networks, *International Journal of Intelligent Engineering and Systems*, 11(2), 2018, pp. 76–84.
- [70] Bader A., Ali Hanady M., Abdulsalam and Alghemlas, Aseel. Trust based scheme for IoT enabled wireless sensor networks, *Wireless Personal Communications*, 99(2), 2018, pp. 1061–1080.
- [71] Zhang, Ting, Jingsha He and Zhang, Yang. Trust based secure localization in wireless sensor networks, *International Symposium on Intelligence Information Processing and Trusted Computing*, 2011, pp:55–58.
- [72] Chen, Liang, Thombre, Sarang, Jarvinen, Kimmo, Lohan, Elena Simona, Al'en-Savikko, Anette, Leppakoski, Helena, Zahidul, M., Bhuiyan, H., Bu-Pasha, Shakila, Ferrara, Giorgia Nunzia, Honkala, Salomon, Lindqvist, Jenna, Ruotsalainen, Laura, Paivi Korpisaari and Kuusniemi, Heidi. Robustness, security and privacy in location-based services for future IoT: A survey, *IEEE Access*, 5, 2017, pp. 8956–8977.
- [73] Zhang, Pengfei, Nagarajan, Sai Ganesh, and IdoNevat. Secure Location of Things (SLOT): Mitigating localization spoofing attacks in the Internet of Things, *IEEE Internet of Things Journal*, 4(6), 2017, pp. 2199–2206.
- [74] Mahalle, Parikshit N., Thakre, Pravin A., Prasad, Neeli Rashmi and Prasad, Ramjee. A fuzzy approach to trust based access control in Internet of Things, *Wireless VITAE*, IEEE, 2013, pp. 1–5.

- [75] L. Yeh, P. Chiang, Y. Tsai and J. Huang, "Cloud-Based Fine-Grained Health Information Access Control Framework for LightweightIoT Devices with Dynamic Auditing andAttribute Revocation," in IEEE Transactions on Cloud Computing, 6(2) 2015, pp. 1–13.
- [76] Suominen, Ilpo. Access control for Internet of Things – Intopalo. [Online], <https://www.intopalo.com/blog/2015-05-25-access-control-for-internet-of-things/>, 2015.
- [77] Habib, Muhammad Asif, Ahmad, Mudassar, Mahmood, Nasir and Ashraf, Rehan. An evaluation of role based access control towards easier management compared to tight security, International Conference on Future Networks and Distributed Systems – ICFNDS '17, New York, New York, USA : ACM Press, 2017, pp. 1–6.
- [78] Wang, Junshe, Wang, Han, Zhang, Hongbin and Cao, Ning. Trust and attribute-based dynamic access control model for Internet of Things, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, IEEE, 2017, pp. 342–345.
- [79] Monir, S. A lightweight attribute-based access control system for IoT, University of Saskatchewan, <https://ecommons.usask.ca/bitstream/handle/10388/7556/MONIR-THESIS-2016.pdf?sequence=1>, 2017.
- [80] Sundmaeker, Harald, Guillemin, Patrick, Friess, Peter and Woelfflé, Sylvie. Vision and challenges for realizing the Internet of Things,[online], http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf, 2010.
- [81] Evans, D. The Internet of Things – how the next evolution of the internet is changing everything, CISCO white paper, 1, 2011, pp. 1–11.
- [82] Cho, J.H., Swami, A. and Chen, I.R. A survey on trust management for mobile ad hoc networks, IEEE Communications Surveys & Tutorials, <http://ieeexplore.ieee.org/document/5604602/>, 13 (4), 2011, pp. 562–583.
- [83] Mahalle, P., Babar, S., Prasad, N. R., and Prasad, R. (July). Identity management framework towards internet of things (IoT): Roadmap and key challenges, In International Conference on Network Security and Applications Berlin, Heidelberg : Springer, 2010, pp. 430–439.
- [84] Roman, Rodrigo, Alcaraz, Cristina, Lopez, Javier and Sklavos, Nicolas Key management systems for sensor networks in the context of the Internet of Things, International conference on Computers and Electrical Engineering 37, 2011, pp. 147–159
- [85] Hintzbergen, Jule, Hintzbergen, Kees, Smulders, André and Baars, Hans. Foundations of information security based on ISO27001 And ISO27002 (Best Practice), Van Haren Publishing, Zaltbommel, https://www.vanharen.net/shop/amfilerating/file/download/file_id/328/, 2015.
- [86] Mahalle, P. N., Anggorojati, B., Prasad, N. R., and Prasad, R. Identity authentication and capability based access control (iacac) for the internet of things. Journal of Cyber Security and Mobility, 1(4), 2013, pp. 309–348.