IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

*ISSN: 2664-9519 (Online); Vol. 1, Issue 2, November 2019*

# A Comprehensive Security Model for Internet of Things

**Ali Syed, Sajjad Hussain Shah**

Department of Computer Science, Bahria University Islamabad

* Corresponding Author: Ali Syed; Aliisb1987@gmail.com

*Received; 25 September, Revised; 27 October Accepted; 15 November*

**Abstract:** Internet of Things **(**IoT) is a network where various devices are interconnected for data communication. Various IoT applications facilitate the users by more convenience, affordable, fast and user friendly services. Due to complex and heterogeneous networks, IoT has suffered with number of security concerns. Researchers have been discussed the security attacks and their solutions without discussing the comprehensive model. This paper presented a comprehensive model for IoT security to address the attacks and their preventions. This paper specifically targeted the security and privacy issues at each layer of IoT. This review is very comprehensive in nature where we focus on to the point contents related to security in IoT. The proposed model provides more clear and understandable situation in IoT networks and best for authentication, intrusion detection and risk assessment.

## 1. Introduction

The term IoT (internet of things) is introduced by Radio Frequency Identification Development (RFID) member in 1999 [1]. The IoT comprises of humans, machines, computers, electronics, and many other devices. The IoT is defined as a network of physical devices [2]. The term IoT also refers to the interconnection of a large number of devices and objects which exchange information to provide various services [3, 4]. IoT has many applications such as transportation, agriculture, healthcare, defense, energy, and manufacturing. This means that the fully operational devices around us collect the data and transfer it to other devices where some automated and smart decisions are made. This leads to changing the devices from passive to smart systems. The main goal of IoT is to upgrading human living by enabling the devices to perform routine tasks. The number of IoT devices is going to reach 50 billion by the year 2020 worldwide [5]. his is not only being a great achievement but an inevitable sign of the rapid growth of IoT. However, the large network of interconnected devices also brings with it new security and privacy issues. IoT involves continuous data collection and transmission where security and privacy issues raise a lot of questions. To provide a statistical overview, authors in [6] stated that 70% of devices in IoT do not encrypt the data and 80% of devices function without requiring complex passwords and 60% are vulnerable firmware and user interfaces.

It is now apparent that security of IoT is one of prime concern which is not addressed properly and impede its development [7]. IoT can only be adopted on a worldwide scale if it is able to answer all the questions related to its security. Secondly, if IoT is not fully secure' a very large number of users which largely consists of the general population are affected and taken advantage of it. For example, even seemingly normal data like temperature, pressure and water level readings need to be protected in order to prevent the attacks [8, 9]. IoT devices can also easily be accessed by the third party thus there is a need to secure the user data and provide security and privacy to the users [10, 11]. It is worthwhile noted that conventional security schemes are not sufficient for IoT due to their difference in architecture from traditional networks. This paper will analyze all the security risks present across all the layers of IoT and will also provide possible solutions to these threats.

This paper is organized as follows. Section 2 explains the general architecture of IoT. Section 3 describes the security objectives of the IoT. Section 4 then presents the various security threats present on each layer. Section 5 then gives the security model for IoT and section 6 concludes this research paper.

## 2. Literature Review

The research in the field of IoT and its security related literature has been carried out and is still going on. Research highlighting that the various studied have discussed the security issues of IoT but do no cover the entire range of IoT issues. For instance in [12], authors described security issues at all the layers of IoT and provides all the theoretical security solutions without giving a proper security model. On the other hand, the authors in [13] discussed the various DoS (Denial of Service) attacks for WSN (Wireless Sensor Networks) and a few security attacks in the RFID technology like tag duplication and tag flooding. However, this paper does not give any practical examples of how vulnerabilities are exploited for these two technologies which are used in IoT at sensing layer and what security mechanisms can use against the referred attacks [14]. The authors provide various IoT security risks including lack of standardization by referring to existing security frameworks such as COBIT, ISO/IEC 27001:2013, much of the suggested security solutions are focused on hardware and protocol level security with an emphasis to develop IoT specific security standards.

Researchers in [3] covered a broad spectrum of security issues in IoT with a focus on internal and external attacks, like DoS attacks, physical attacks and attacks on privacy. Authors also discussed the user confidentiality, integrity, authentication, trust management, and access control [15]. The focus of this paper is only on the IoT communication protocol including 6loWPAN and described the possible manipulation of the datagram. Authors in [16], suggested the use of an SDN (Software-Defined Network) based network security scheme to provide monitoring and network control on IoT devices.

We discussed the literature only focused the security implementation and its functionality within the devices including improving the security features of protocols that IoT uses. For example, the authors in [17], suggested that optimizing the DTLS (Datagram Transport Layer Security) communication protocol for reliable data exchange in IoT. Authors in [18] Identified Sybil, node replication attack, Eavesdropping & flooding attack on link layers of the sensor network protocol stack & advises. The adoption of IEEE 802.15.4 complaints link-layer security features. In another notable work in [19], the authors presented light encryption and decryption scheme for Identity authentication between the sensor nodes.

The paper [20], authors described the detail on IoT standards and security issues. However, suitable counter-strategies are missing in this work. Another paper by the same authors [21], discussed only a few countermeasures to the IoT threats. However, global policies for ensuring security in IoT are missing. The authors in [22], discussed the threats present at the perception layer but the only solution given for these threats is encryption at the perception layer. A very comprehensive survey for IoT, WoT (Web of Things) and SWOT (Social Web of Things) is presented in [23], in which security issues their suitable countermeasures are discussed. However, the authors restricted their focus on securing IoT by using the latest network protocols such as IPv6 and 5G. WIPr (Wireless Internet service Provider Roaming) and RADIUS are the possible solutions to solve the user authentication problem for IoT [24].

As a result, there is a need to present the practical threats in IoT present at every layer and provide the users with practical solutions to counter these threats. At the same time, these countermeasures should be compatible with the variety of IoT standards in use and give an end-to-end security. Table 1 presents the security threats and countermeasures for IoT.

**Table 1:** Security Threats and Countermeasures for IoT

| S# | Ref# | Security threats in IoT | Countermeasure |
|---|---|---|---|
| 1 | [7] | Discusses some security threats present across the IoT layers namely man in the middle, Eavesdropping, Sniffing attack, Injection attacks, storage attacks & environmental related attacks. | No discussion on any practically implementable countermeasure. |
| 2 | [8] | The authors provide an in-depth analysis how DoS & DDoS attacks are possible on WSN and Tag flooding and Tag duplication attacks in RFID thus posing a threat to end user privacy. | The paper does not provide any strategy or steps to counter DoS attacks at sensing layer. |
| 3 | [9] | The authors highlight the lack of standardization in IoT as major gap by referring to the current information security standards such as COBIT, ISO/IEC 27001:2013 as insufficient for IoT security. | The authors urge the need of development for IoT specific security standards and policy however none are given in the paper. |

| | | | |
|---|---|---|---|
| 4 | [10] | Researchers in this paper only focus on IoT communication protocol i.e. 6loWPAN and describe the possible manipulation of the 5datagram with respect to confidentiality, i6ntegrity and authentication. | No suitable countermeasures have been provided. |
| 5 | [11] | The authors discuss the security and privacy issues present in IoT based devices such as usage of HTTP which lacks encryption. Some devices exchange data which in plaintext on Wi-Fi which can easily be captured. Using MD5 based digest which can be easily recreated. | Suggests the use of SDN to provide monitoring and network control on IoT devices.SDN can be used to block and quarantine device based on their network activity, time of day, usage or occupancy level. |
| 6 | [12] | No discussion on threats | The paper focuses on optimizing the DTLS (datagram transport layer security) communication protocol for reliable data exchange in IoT |
| 7 | [13] | The paper identifies Sybil, node replication attack, Eavesdropping & flooding attack on link layers of the sensor Network protocol stack. | suggests adoption of IEEE 802.15.4 compliant link layer security features |
| 8 | [14] | No discussion on IoT threats | Provides a light encryption and decryption scheme for identity authentication between sensor nodes. It proposes dynamic variable cipher security certificate. |
| 9 | [15] | Mention the IoT standards and security issues associated with them. | Countermeasures are missing. |
| 10 | [16] | Published by the same authors as in [15] | Countermeasures have been suggested. |
| 11 | [17] | The authors discuss the threats present at perception layer namely node capture, DoS, Timing attack, routing attacks and replay attack. | Advices to use and encryption scheme at perception layer namely IPsec. |
| 12 | [18] | Discusses the security threats present in for IoT, WoT (Web of things) and SWOT (Social Web of things) | authors restrict their focus on securing IoT by using latest network protocols such as IPv6 and 5G |
| 13 | [19] | Identifies user authentication as major threat. | Suggests WIPr (wireless internet service provider roaming and RADIUS are the possible solutions to solve the user authentication problem in IoT |

## 3. General Architecture

IoT has generally four main layers including perception, network, middleware and application layer. The layers are shown in the Figure 1.

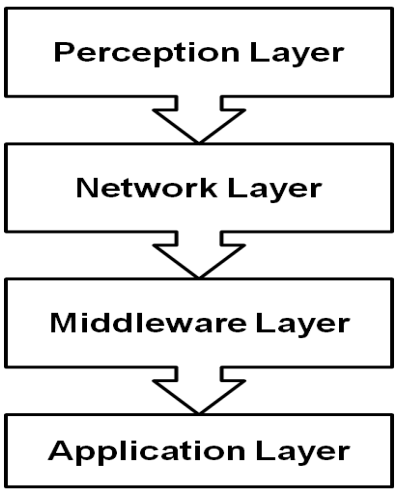


**Figure 1:** IoT Layers

### 3.1 Perception Layer

This layer is comprised of various kinds of sensors such as RFID, barcodes or WSN [14]. The main function of this layer is to accurately collect the data via sensors and forward it to the network layer. This layer is also responsible for performing node collaboration at local and short distance networks [25].

### 3.2 Network Layer

The main function of this layer is to receive the data from the perception layer and to transmit it to any data processing unit using any dependable network as described in [26]. This layer also routes the data over the internet. The prominent technologies used at this layer are Wi-Fi, LTE, Bluetooth, 3G and ZigBee.

### 3.3 Middleware Layer

This layer is made up of information processing systems that are involved in making autonomous decisions based on the data received from the network layer. This layer is the service providing a layer of IoT [27].

### 3.4 Application Layer

The layer runs and supports the IoT based applications according to the requirements of the users such as smart home, automated vehicle and automated building [28].

## 4. Security Goals

The security of IoT is centered on three important goals including confidentiality, integrity and availability. The CIA triad is the most comprehensive security model that does not only assess but also implemented the security controls based on confidentiality, integrity and availability on IoT. The model is shown in Figure 2.

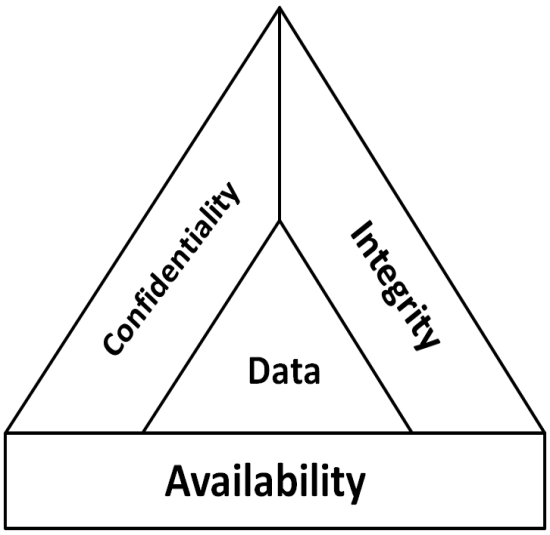


**Figure 2:** Security Model

### 4.1 Data confidentiality

This is all about ensuring the privacy of user data by using procedures to prevent disclosure of information to unauthorized people. The main method to maintain the confidentiality of data is through encryption. Encryption transforms plaintext data into ciphertext and this makes it impossible for people not having the private key or valid authorization to access data. The authorization phase includes two-factor authorization and biometric authentication. IoT encryption ensures that sensor nodes in a sensor network don't disclose data to other nodes and likewise tags don't share data with an unauthorized reader [29].

### 4.2 Data Integrity

This involves preserving the data so that it is not changed either by hackers or due to technical problems such as link failure, server crash or electromagnetic interference. Integrity, therefore, means that the information is not changed while being sent or received [30]. There are some well-known techniques for ensuring the integrity of data such as checksum and CRC (cyclic redundancy check). Other notable techniques include synchronization of data for backups and version control that log the no of file changes in a system to restore it in case it is deleted. These techniques can also be used in IoT.

### 4.3 Data Availability

Data availability is one of the major objectives of IoT security where the data is available to users when they require it. Authorized users should get access to their data when required no matter what the conditions are. Since data availability is such an important aspect in IoT firewalls which is an essential component to prevent DoS attacks which deny the access of data for the end-users. Redundancy is also another method to ensure data availability in case of any attack or failure of primary systems.

## 5. Security Mechanisms and Issues

There has been comprehensive research in the field of IoT security however there are still some gaps that need to be addressed. In this section threats present at each layer of IoT.

### 5.1 Perception Layer Threats

The perception layer is also sensing layer which utilizes many sensor technologies such as RFID or wireless sensors that involve various kinds of threats which are mentioned below.

**Unauthorized Access to Tags:** Many RFID systems available today do not provide sufficient authentication mechanisms there the tags can be obtained by cyber attackers or unauthorized people. The obtained data can be tampered with or deleted altogether [31].

**Tag Cloning:** Tags data can be modified so the attacker can obtain a tag modify the data to create a copy of the tag so that the reader cannot differentiate between original and modified tag [32].

**Eavesdropping:** Since RFID and wireless sensors used in IoT use wireless media for communication it is very easy for an attacker to obtain data flowing on the wireless communication channel either from the tag to the reader or from the reader to the tag [33].

**Spoofing:** In this type of attack the hacker sends fake data to the RFID devices and ensuring them to assume it to be original and thus the attacker assumes the full control of the system [34].

**RF jamming:** By generating a sufficiently strong noise signal RFID signals can be blocked or hampered in order to disrupt communications [35].

### 5.2 Network Layer Threats

The network layer is primarily made up of WSN (wireless sensor network) which transfers data from source to destination ensuring reliability. The security threats in this layer are mentioned below.

**Sybil Attack:** Sybil Attack: It's the attack in which the hacker changes the logical characteristics of the node so that a single node has multiple identities and this leads to the entire network being hacked based on fake information regarding redundancy [36].

**Sinkhole Attack:** Sinkhole Attack: This attack basically compromised a node and makes it appealing for another node to send data to. As a result, all the nodes transmit data to this compromised node and thus leading to packet drop as the system believes that the other side is receiving the data. This attack can also result in a DoS attack as it leads to higher energy consumption [37].

**Sleep Deprivation Attack:** Sleep Deprivation Attack: Sensor nodes use the battery for energy and one of their key objectives is to conserve energy, they do this by going to sleep mode to save energy. sleep deprivation attack keeps the nodes powered on and the battery is consumed quickly and as a result, nodes shut down [38].

**Denial of Service Attack:** Denial of Service Attack: In the DoS attack fake traffic is generated and loaded on the network resulting in the network being unavailable to intended users [39].

**Malicious Code Injection:** Malicious Code Injection: In this type of attack the attacker injects malicious code in the compromised node which can shut down the network or give full access of the network to the hacker [40].

**Man in the Middle Attack:** This attack is primarily focused on the communication medium in which the attacker can silently monitor and control all communication between the sender and receiver [41].

### 5.3 Middle-ware layer Threats

This layer primarily provides data storage capabilities. The security threats of this layer are listed as follows:

**Unauthorized Access:** As the middleware layer provides storage services it has different interfaces for the applications. In this attack, the attacker manipulates the access rights of these applications to the middleware layer and thus the applications don't get the required services.

**DoS Attack:** If the storage devices are completely shut down then the applications cannot store or retrieve data. This attack is quite similar to the DoS attack discussed on the perception and network layer.

**Malicious Insider:** In this attack, an insider manipulates data for their personal benefits or for the benefit of some party.

### 5.4 Application layer Threats

**Malicious Code Injection:** For this type of attack the attacker needs access to the end-user system from where he/she can launch malicious code into the system and steal the user data.

**DoS Attack:** Denying the end-user of the authorized services and also stealing the personal details by-passing the defensive system of the end-user.

**Spear-Phishing Attack:** This is an email-based attack in which the user is tricked into opening a malicious email through which the attacker gains access to their system and steals sensitive information.

**Sniffing attack:** Attacker gains access to the system via a sniffing program which provides the hacker with network information [42].

## 6. Security at all layers

The security of IoT has been a source of constant debate for the last few years. In this section, we will define security measures that can be taken at each layer to achieve a comprehensive security model for IoT.

### 6.1 Perception Layer countermeasures

The perception layer can be used to provide numerous security services to the hardware. The most common security services that can be achieved using the perception layer are privacy, authentication and risk assessment.

**Authentication:** Authentication can be done using the hashing algorithms which use digital signatures between terminals and this can provide security against attacks such as a side-channel attack, brute force attacks & collision attacks.

**Data Privacy:** Data privacy is ensured by using symmetric and asymmetric encryption techniques such as RSA, DSA, BLOWFISH, and DES. These techniques ensure the privacy of sensor data that has been collected or in transit. Another advantage of using these techniques is that they consume low power so they can be applied to sensor nodes.

**Risk assessment:** This process helps in identifying new threats to IoT security. This helps to reduce security-related attacks by discovering the most efficient security strategies. The recommended technique for this process is the Dynamical Risk assessment method for IoT [43].

### 6.2 Network Layer Countermeasures

Multiple types of attacks are possible on the network layer since it can be both wired and wireless. Wireless medium makes it even easier for attackers to penetrate communications. The network layer security can be achieved through the following techniques.

**Authentication:** Using a good authentication technique and node to node encryption the unauthorized access to sensor nodes can be stopped [44]. This will help to prevent the DoS attacks.

**Routing Security:** Secure routing techniques should be used in order to ensure the security of data travelling over the networks. For this purpose source routing can be used in which data being transmitted is stored and sent to the processing systems only after it has been thoroughly analyzed by intermediated nodes[45].Another technique that can be used is the hop by hop routing in which only the address of destination is known. Routing security can best be achieved by using multiple paths for routing the data which not only improved error detection but lets the system continue performing in case of any error [46].

**Data Privacy:** The monitoring systems are deployed on networks to check for any kind of attacks or intrusion attempts along with integrity check systems to ensure that data being received has not changed.

**Middleware and application layer countermeasures:** Middleware and application layer countermeasures are applied collectively to provide security for these two layers.

**Authentication:** The foremost process at this layer is authentication which restricts access to any illegitimate user. This process is very similar to other layers. In this layer some services also require authentication so users have the liberty to choose what information to share with what services.

Two main technologies are being used at this layer i.e. virtualization and cloud computing. Cloud computing is highly vulnerable to insider threat and virtualization is vulnerable to DoS attacks. Research needs to conducted to secure these.

**Intrusion Detection:** Anomaly detection, intrusion detection and data mining approaches can be used for this purpose [47].

**Risk Assessment:** Continuous risk assessment is necessary for identification of new threats and vulnerabilities.

**Data Security:** Data security is ensured by using light weight encryption techniques. In addition to encryption Anti-DoS firewalls can also be used to ensure data security.

## 7. Conclusion

IoT is the future that will not only make communication easier but will also have applications in every walk of life. However, the security concerns of IoT must be addressed. There has been plenty of research on IoT security however a comprehensive model is missing. This paper presented a comprehensive model for IoT security. The model is open for future research and further enhancements. This paper specifically targeted the security and privacy issues at each layer of IoT. In future further work can be conducted on authentication, intrusion detection and risk assessment. Legal frameworks are another field that should be considered for improving IoT security.

# References

[1] M. F. Muhammad, W. Anjum, and K. S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications,* vol. 111, no. 7, 2015.

[2] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science computing,* vol. 6, no. 5, 2016.

[3] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *2014 international conference on privacy and security in mobile systems (PRISMS)*, 2014, pp. 1-8: IEEE.

[4] K. M. Awan *et al.*, "A priority-based congestion-avoidance routing protocol using IoT-based heterogeneous medical sensors for energy efficiency in healthcare wireless body area networks," *International Journal of Distributed Sensor Networks,* vol. 15, no. 6, p. 1550147719853980, 2019.

[5] S. Shukla, M. F. Hassan, L. T. Jung, and A. Awang, "Architecture for Latency Reduction in Healthcare Internet-of-Things Using Reinforcement Learning and Fuzzy Based Fog Computing," in *International Conference of Reliable Information and Communication Technology*, 2018, pp. 372-383: Springer.

[6] E. Bertino, "Data Security and Privacy in the IoT," in *EDBT*, 2016, vol. 2016, pp. 1-3.

[7] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481-2501, 2014.

[8] M. Irshad, "A systematic review of information security frameworks in the internet of things (iot)," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2016, pp. 1270-1275: IEEE.

[9] S. Iqbal, A. H. Abdullah, K. N. Qureshi, and J. Lloret, "Soft-GORA: Soft constrained globally optimal resource allocation for critical links in IoT backhaul communication," *IEEE Access*, vol. 6, pp. 614-624, 2017.

[10] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2017, pp. 492-496: IEEE.

[11] K. N. Qureshi, M. M. Idrees, J. Lloret, and I. Bosch, "Self-Assessment Based Clustering Data Dissemination for Sparse and Dense Traffic Conditions for Internet of Vehicles," *IEEE Access*, vol. 8, pp. 10363-10372, 2020.

[12] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5772-5781: IEEE.

[13] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:.02211*, 2015.

[14] M. Ahlmeyer and A. M. Chircu, "Securing the Internet of Things: A review," *Issues in information Systems*, vol. 17, no. 4, 2016.

[15] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015.

[16] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)*, 2015, pp. 163-167: IEEE.

[17] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, 2012, vol. 3, pp. 648-651: IEEE.

[18] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello, and M. Rossi, "Low power link layer security for IoT: Implementation and performance analysis," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013, pp. 919-925: IEEE.

[19] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, 2012, vol. 3, pp. 1062-1066: IEEE.

[20] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, no. 9, pp. 51-58, 2011.

[21] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266-2279, 2013.

[22] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth international conference on computational intelligence and security*, 2013, pp. 663-667: IEEE.

[23] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," *Ad Hoc Networks*, vol. 28, pp. 68-90, 2015.

[24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer networks*, vol. 76, pp. 146-164, 2015.

[25] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer networks*, vol. 56, no. 16, pp. 3594-3608, 2012.

[26] X. Yang, Z. Li, Z. Geng, and H. Zhang, "A multi-layer security model for internet of things," in *Internet of things*: Springer, 2012, pp. 388-393.

[27] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *2012 10th international conference on frontiers of information technology*, 2012, pp. 257-260: IEEE.

[28] Y. R. Shi and T. Hou, "Internet of Things key technologies and architectures research in information processing," in *Applied Mechanics and Materials*, 2013, vol. 347, pp. 2511-2515: Trans Tech Publ.

[29] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad hoc networks*, vol. 10, no. 7, pp. 1497-1516, 2012.
[30] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787-2805, 2010.
[31] R. Uttarkar and R. Kulkarni, "Internet of things: architecture and security," *International Journal of Computer Applications*, vol. 3, no. 4, pp. 12-19, 2014.
[32] M. Burmester and B. De Medeiros, "RFID security: attacks, countermeasures and challenges," in *The 5th RFID academic convocation, the RFID journal conference*, 2007.
[33] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 709-712: IEEE.
[34] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491-505, 2010.
[35] L. Li, "Study on security architecture in the Internet of Things," in *Proceedings of 2012 International Conference on Measurement, Information and Control*, 2012, vol. 1, pp. 374-377: IEEE.
[36] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, 2002, pp. 251-260: Springer.
[37] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," *ACM SIGMOBILE Mobile Computing Communications Review*, vol. 9, no. 2, pp. 4-18, 2005.
[38] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network," *arXiv preprint arXiv:.06249*, 2012.
[39] D. G. Padmavathi and M. J. a. p. a. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," 2009.
[40] P. S. Fulare and N. Chavhan, "False data detection in wireless sensor network with secure communication," *International Journal of Smart Sensors AdHoc Networks*, vol. 1, no. 1, pp. 66-71, 2011.
[41] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," *International Journal of Computer Science Information Technology Security*, vol. 1, no. 2, pp. 136-146, 2011.
[42] B. S. Thakur and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey," *International Journal of Advanced Computer Research*, vol. 3, no. 2, p. 7, 2013.
[43] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R. Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology," in *2012 8th International Conference on Natural Computation*, 2012, pp. 874-878: IEEE.
[44] Y. Maleh and A. Ezzati, "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," *arXiv preprint arXiv:.02211*, 2014.
[45] S. Agrawal and D. Vieira, "A survey on Internet of Things," *Abakós*, vol. 1, no. 2, pp. 78-95, 2013.
[46] C. Qiang, G.-r. Quan, B. Yu, and L. Yang, "Research on security issues of the internet of things," *International Journal of Future Generation Communication Networking*, vol. 6, no. 6, pp. 1-10, 2013.
[47] J. Gubbi, R. Buyya, S. Marusic, and M. J. F. g. c. s. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," vol. 29, no. 7, pp. 1645-1660, 2013.