IoT-based Application of Information Security Triad

https://doi.org/10.3991/ijim.v15i24.27333

Mana Saleh Al Reshan(✉)
College of Computer Science and Information Systems,
Najran University, Najran, Saudi Arabia
msalreshan@nu.edu.sa

Abstract—Information Security is the foremost concern for IoT (Internet of things) devices and applications. Since the advent of IoT, its applications and devices have experienced an exponential increase in numerous applications which are utilized. Nowadays we people are becoming smart because we started using smart devices like a smartwatch, smart TV, smart home appliances. These devices are part of the IoT devices. The IoT device differs widely in capacity storage, size, computational power, and supply of energy. With the rapid increase of IoT devices in different IoT fields, information security, and privacy are not addressed well. Most IoT devices having constraints in computational and operational capabilities are a threat to security and privacy, also prone to cyber-attacks. This study presents a CIA triad-based information security implementation for the four-layer architecture of the IoT devices. An overview of layer-wise threats to the IoT devices and finally suggest CIA triad-based security techniques for securing the IoT devices.

Keywords—IoT application, security of IoT, information security, security triad

1 Introduction

Some application domains well define the IoT (Internet of Things) comprising health, agriculture, home, supply chain and manufacturing, city and transportation utilities. In these domains, physical devices are connected via Internet [1].

Further, the home device comprising appliances, thermostats, smart door locks, smart homes, wearable, smart vehicles. The health devices for monitoring and recording the patients' data namely heartbeat monitoring system, pacemakers, and glucose monitoring system. Manufacturing or industrial supply chain Radio Frequency Identification (RFID) tags and sensor networks. Whereas, agricultural IoT devices include green-house sensor systems, monitoring fields, and irrigation controllers. The streetlights water distribution systems are applications for city IoT domains [2–7].

It is the IoT that equally benefits organizations, individuals, and municipalities. Home-life has become more economical and convenient with the help of IoT devices and inexpensive remote sensor networks. The sensor networks monitor those areas which are inaccessible and hard to monitor [3–6]. IoT technology of smart cities allows to monitor and track energy usage and the environment. While health care

IoT technologies provide the error-free and most precise results of health conditions for elderly or remote patients. All application domains in IoT attracted the interest of academia, business, and investors [8–10].

With these enormous benefits, the IoT brings a lot of challenges to privacy and security. IoT constraints in power supply comparing to traditional IT devices namely smartphones, laptops, and desktops [11]. So, the IoT lacks memory and processing capabilities ranging from tens of kilobyte (kB) of Random Access Memory (RAM) at the end sensor. Another limitation is to update the system, where IoT devices may not allow users to update while traditional IoT allows users to update [12].

The uses of Internet of Things (IoT) devices are growing exponentially from the last six years. Estimated connected devices in 2020 will be 30.73 billion and in 2025 estimations are for 75.44 billion as shown in Figure 1. As indicated in a report by Gartner that in 2020–21 the internet-connected things may be more than 8.4bn (Billion) [13]. It is also presumed that this number will grow exponentially up to 42.62bn (billion) by the year 2022 connected via IoT technology as shown in Figure 1. Therefore, as the size of the IoT network exponentially increases the security and privacy issues of IoT applications come to light [13]. These consist of wireless sensors, RFID tags, and many more smart devices. These devices share a large amount of information either it's our health information or our day-to-day cash transaction information, this massive quantity of information is shared between many different devices over the common platform i.e., IoT. As the IoT network expands we need some architecture for better work of IoT devices.

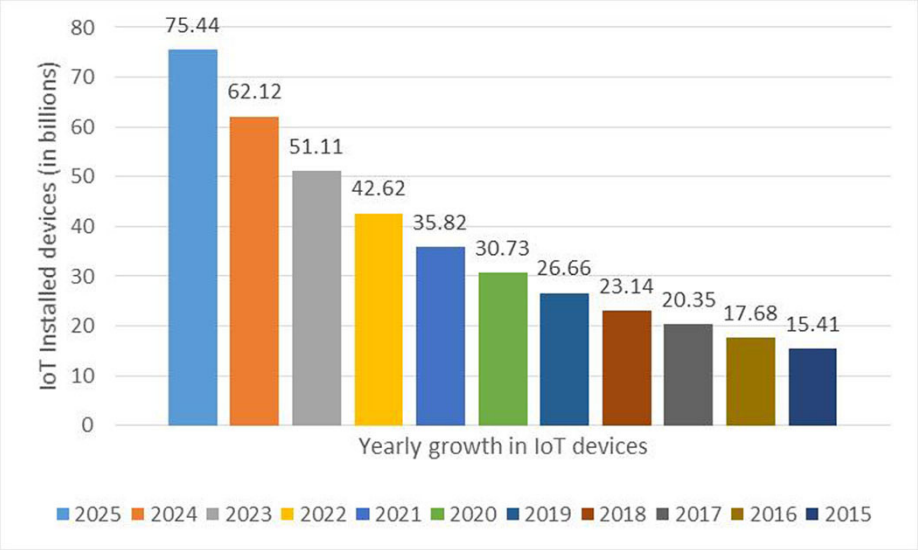

Fig. 1. Global scale of installed IoT devices [13]

The constraints in the capacity of power and processing lead to the limited ability to run a specific cryptographic protocol. However, an integrated security solution is hard to achieve in the face of heterogeneous protocols and hardware of devices [14]. Though usage of IoT devices at a significant level has risen security and privacy concerns, they also promise convenient and better living by smart devices. Again, the huge number of data and various quantities of new IoT devices create a significant space for information security and privacy concerns. Thus, user security and privacy are under a threat caused by vulnerability to the IoT framework.

This paper is divided into seven sections. Section I starts with the introduction of IoT and information security concerns in IoT. Section II provides the literature review of IoT-based security and privacy. Section III and Section IV discuss CIA Triad and IoT scope and architecture. Information security-related threats are comprised in Section V. Section VI discusses the CIA Triad-based implementation in IoT. Section VII encloses the concluding remarks and future work.

2 Related work

The study of [15] supports the CIA triad-based division of IoT three layers into the Perception layer, Application layer, and Network layer. Where technological challenges have been addressed as wireless network technologies, IoT hardware heterogeneity, security, and scalability containing both end-to-end security and CIA triad. The authors mainly focused on security challenges concerning layers and their counter-measurements namely federated architecture, trust establishment, and authentication. An approach on security for three-layered internet of things architecture has been suggested in [14, 15]. Three layers namely application, transportation, and perception utilized along with physical sensors and sensor actuators. The sensor uses RFID tags to connect with the physical environment or world. Smart functionality for the user is provided by the application layer. While the Network layer fulfills the responsibilities of information transportation via wireless technologies to the other two layers. In [16], scholars debated for an additional layer known as a Processing layer. It sketches an intelligent interface for the Network layer and Application layer. This aims to process information from the Physical layer by data mining, cloud, and parallel computing.

A five-layer security system in IoT with end-user layer represented in [17]. The architecture has been suggested with an Edge Network layer which is responsible for the collection, transmission, and processing of the data from the IoT devices. Where the Core Network layers transport the processed data towards the Storage layer and service layer by edge network. Therefore, further analysis on the received data is carried out by the data servers where some software servers hold data and operating system images. Similarly, the study suggested in [18] discusses an end-to-end scenario with six layers for security architecture. The scholars composed six layers namely the internal communication layer, end device layer, a Gateway Information (GI) layer, Information transmission layer along the cloud layer.

Another study with a comparison of three models is suggested in [19]. These models namely the CISCO Seven layer model, the alternative five-level model, the early 3-layer model used for analysis and comparison. All security measures and countermeasure, security needs for the edge-level attacks have been sorted. The edge level measures include communication among devices, edge nodes dispersed in an area, and Fog computing or edge computing. The study claims that the security cannot be fulfilled and adequately provide desired outcomes with the CIA triad alone. So, IoT security with CIA triad expanded further by the addition of the IAS Octave security paradigm. They claim good outcomes of IAS-Octave in counter the attacks. Therefore, the insecurity increases with the growth of IoT devices exceedingly and privacy implications to such a huge amount of data or information remains to build a suitable design.

3 CIA triad

Confidentiality, Integrity, and Availability (CIA) form a triad that fulfills the basic security needs. For security and privacy of the IoT devices, should satisfy the CIA triad [12] [20–21]. These all three components are important for the better security of the devices as illustrated in Figure 2. So, these security doctrines apply as a whole to the IoT same as they apply on the Internet [22–23].

3.1 Confidentiality

Confidentiality ensures that access must be granted to the authorized user to the information and data reports. The access is subject to the extent of the need for access.

3.2 Integrity

The Integrity is determined and ensured when the data is well secured and protected. The encrypted data only be modified by the authentic user during the process, transmission and storage.

3.3 Availability

Availability of the data play an important role. Information security and authentication are very vital for data security. But, the availability of the data at the required time is a must. It is useless if the data is not available on time or in an emergency or critical situation.

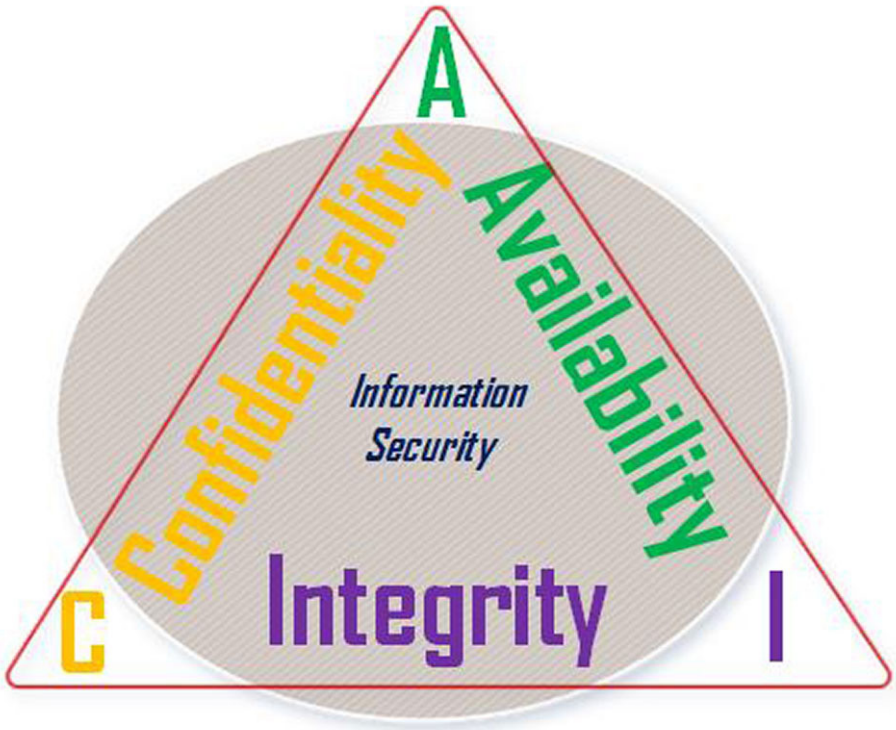

Fig. 2. CIA (Confidentiality, Integrity, and Availability) triad

For security and privacy of the IoT devices, it should satisfy the CIA triad. Components of the CIA triad are confidentiality, integrity, and availability. These all three components are important for the better security of the devices [12]. It poses a significant impact to any individual or institution or organization involved in any CIA triad basic requirements is missed. As a definition for impacts provided by the NIST (the National Institute for Standards and Technology) suggesting High, Moderate, and Low potential impacts due to the loss of CIA triad in FIPS 199 [24, 25]. The loss of availability differs from application to application in an IoT scenario [26]. Confidentiality and integrity are provided by encryption and cryptography for the data on IoT devices and data transportation across the network [27].

4 Over of IoT scope and IoT architecture

The IoT has made our routine activities very convenient and easy. The IoT is not the same as it was in the early days it was born, in late 1960 [28]. In its early days, security was not among the design goals, therefore, security issues were not a major focus. On the other hand, today the security is vital for IoT and its adoption. Almost, none can deny the fact that IoT-based devices and applications have flooded all aspects of life.

The IoT comprising WSNs (Wireless Sensor Networks) WBANs (Wireless Body Area Networks) are playing a very essential role in numerous health-related issues and healthcare atmospheres [3–6], [29–31]. Smart homes, automated and hyper-connected homes, intelligent household systems, and devices including light bulbs, power outlets, thermostats, and other numerous applications are connected through the Internet which allows operating remotely. There are numerous IoT devices and applications are in our surroundings namely smart homes, automatic and smart cars, railway trains, agriculture, transportation, and business. Thus, all spheres of life are surrounded by IoT applications and devices as illustrated in Figure 3.

Fig. 3. IoT applications

The estimation of usage and consumption of IoT devices shows that the current rate of IoT devices will grow and expand exponentially by the year 2025 [32]. It is predicted that IoT connected device approximately reaches around 75bn (Billion) as shown in Figure 4.

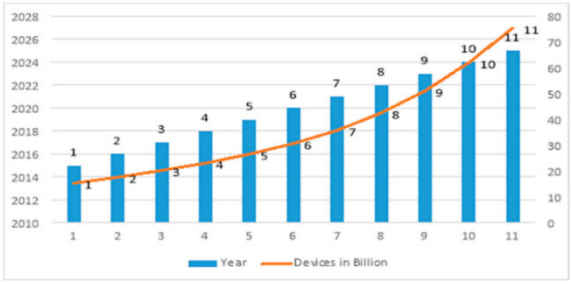

Fig. 4. IoT expected devices by 2025

So there is a Four-Layer architecture being used for IoT devices. Four layers of the architecture are the sensing layer, network layer, middleware layer, and application layer. Access to Information and data, for example, can bring significant security

threats to a network by introducing viruses that might have devastating effects on the operations of an organization. This scenario shows that IoT devices may be used for both good and bad activities, hence, significant research on IoT security threat detection and challenges can help shape the longer term of the IoT domain [33].

IoT devices are connected to the internet, machine to machine, and also a machine to humans. At the very start of IoT, there were only a few devices that could connect to the internet but as time goes the devices get increased which can connect to the internet. So there is a need to be a certain architecture at which a device can work properly. There are two IoT architectures: three layers and four layers [34]. There are three fundamental layers in the IoT. These layers are 1). Sensing Layer 2). Network Layer 3). Application layer. Due to security reasons, a new layer was introduced to IoT architecture and this layer is the Middleware layer. Figure 5 shows the four-layer architecture with characteristics [17], [34, 35].

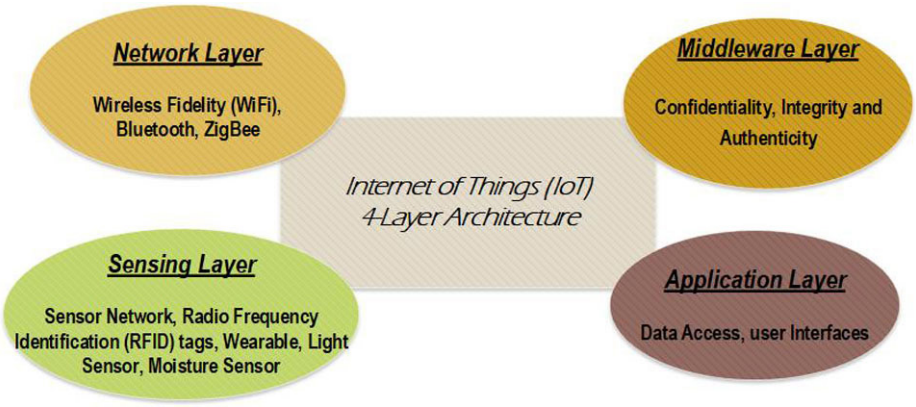

Fig. 5. Inter of things (IoT) 4-layer architecture

4.1 Sensing layer

The Sensing layer is the bottom layer of IoT architecture. The sensing layer consists of a network of different kinds of data sensors that collects data and information from the environment and transmits it to the network. So this layer is the very important layer of architecture [2] [18].

4.2 Network layer

The network layer is the collection of different communication technologies whose function is data routing and information transmission to different IoT hubs and devices. At this layer different platforms like cloud computing, internet gateways, and routing devices are using different internet technologies like 3G/4G, LTE, Wi-Fi, Bluetooth, and ZigBee, etc. to transmit data through the internet [10].

4.3 Middleware layer

The middleware layer is a software layer between the network layer and the application layer. It is a security span between the network layer and the application layer. This layer is focused on the data exchanged. It provides Confidentiality, Integrity, and Authenticity to the data exchanged. This layer is associated with the conversation of data stored at different data storing platforms [26].

4.4 Application layer

The Application layer is the topmost layer of IoT architecture. This layer provides a user-friendly environment to the user where users can access data sensed by different sensors. This helps users to identify current trends and decision making [14], [36].

5 Information security threats in IoT

The field of IoT is expanding exponentially over the last five to seven years. So the threats are also emerging at the same rate as IoT expanding. As the IoT devices have resource limitations there are many threats to the IoT System. Though at this level we cannot secure all the threats to the System we can secure big threats to the system. We can classify the threats in the four-layer architecture:

5.1 Sensing layer threats

As sensors are the least secure devices in the whole architecture, threats based on the sensing layer are most important. Because sensors can be the easiest entrance to enter the entire IoT architecture and launch an attack [8]. Attackers can use sensors to inject malicious code and activate it to capture sensitive data exchanged between different IoT devices. If sensors are located in open locations so that attackers can do side-channel attacks which are based on electromagnetic field monetization, power consumption monetization or timing monetization to attack different encryption mechanisms or they can inject noise to the signals [22] [35]. An attacker can also data manipulate at sensors, can do boot attacks, can capture a Node [18].

5.2 Network layer threats

Everything is embedded in an IoT network, so attackers are attracted to attack in the network layer. A Man-in-the-Middle (MiTM) attack weakens the network layer and the attacker introduces a malicious node among genuine nodes. In MiTM, the attacker can eavesdrop, modify and monitor the overall communication which takes place over the IoT communication system [37].

Sybil attack in which attacker steals information and breaks the integrity by showing a single node at multiple locations within the IoT network. The attacker compromises an IoT device that can pretend to have many genuine identities in the IoT system and

imitate them [38]. Having different identities, the compromised device (Sybil device) sends fabricated information to its neighboring devices.

In addition, routes that include the Sybil device as a forwarding node could be deceived that many routes are available when there is only one route available where all traffic transmitted will go. This can lead to different attacks, such as a DoS or jamming attack [21]. In the Sybil attack, nodes are used with fake IDs which results from the outnumbers in real nodes in a network, [38]. The attacker can perform Distributed denial of service attack. In a DDoS attack, the attacker captures a node from the network, which has an assigned IP and can make requests to a server, either public or private depending on the nature and complexity of the attack. After capturing the node server is flooded by the request and the server gets overloaded. So the user is no longer able to access the Server [10] [11] [17].

5.3 Middleware layer threats

At this layer, an internal attacker deliberately modifying and extracting data or information within the network. An underlying attack is a platform-as-a-service (Paas)-based attack as shown in Figure 6. Third-party relationship attacks are caused by third-party components such as mashup, which increase the security of the data and network on Paas. In an SQL injection attack, an attacker injects a malicious SQL query into a program to make it malicious. In Cloud Malware Injection the attacker obtains control to inject malicious code or virtual machine to the cloud and the attacker pretends to be a valid service [13].

5.4 Application layer threats

At the application layer data is provided to the final user to their smart devices. So the shared malicious data enters the smart devices of the final user. The attacker enters a malicious object like malware, Trojan horses, and spyware into the system and gets full access to the system [3], [16].

In contrast to the RFID (Radio Frequency Identification) tags, the DoS attacks are vulnerable, and the tag reader is unable to interpret the tag. RF channel is being jammed and difficult to read, therefore, DoS causes unavailability of tags [39]. Apart from channel jamming, a node jamming attack is a vulnerability type where the attacker attacks by transmitting a noise signal over the channel. This interference in the communication channel helps to occupy IoT data and cause signal jamming. The attacker introduces new nodes which creates the increments of fake nodes. The fake nodes create collisions with real nodes and unnecessary retransmit the signal. All real once attacked with unnecessary retransmissions by fake nodes results in depletion of the energy. Thus, nodes get depleted and die down quickly before the estimated time. However, the quick energy consumption due to the jamming of signals disables the communication between devices and nodes. Ultimately, the signal jamming resulting in the DoS of the nodes prevents communication for the IoT nodes or whole network [13, 35, 40–43].

IoT Layers	Information Security Threats
Sensing Layers	*Data Manipulation* *Boot Attack* *Side Channel Attack* *Node Capturing*
Middleware Layers	*PaaS Attack* *SQL injection* *Cloud malware injection*
Network Layers	*MITM Attack* *DDOS Attack* *Sybil Attack*
Application Layers	*Data Leakage* *DoS Attack* *Malicious Code injection*

Fig. 6. IS threats in IoT layers

6 Implementation of CIA triad in IoT

Information security and privacy in IoT fields demand IoT consideration and concerns. Undoubtedly, the biggest issue in the field of IoT is information security. Without addressing the security concerns which come along with IoT, the application or device is worthless. To counter these issues we have the CIA triad. We implement the standard triad of Confidentiality, Integrity, and Availability (CIA) for information security. For ensuring the security of data IoT architecture should provide confidentiality, integrity, and availability of data to the system [12], [35].

All IoT-based fields require a specific information security implementation. The security-based on CIA triad ensures that unauthorized use is no longer to access the data. CIA triad-based techniques provide desired results when the security meets the layers-based authorization, trust, and privacy criterion as given in Table 1. At the sensing layer level, it is very important to develop some encryption techniques to secure information and information access to authorized users only. Encryption methods may include the cryptographic hash algorithms and digital signatures as described in Table 1. Figure 7 shows the IoT information security.

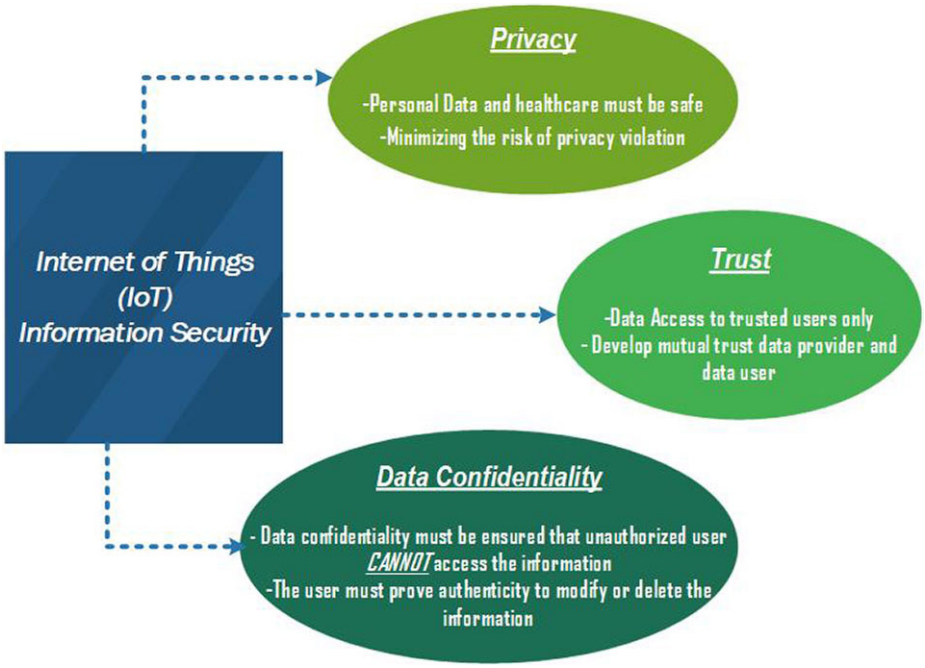

Fig. 7. Inter of things (IoT) information security

For data privacy, user authentication plays a very important role. Where user authorization and mutual trust between the data provider and user ensure that the information is being used is safe and no harm to secured information as depicted in Table 1. Apart from this, authentication at the network layer level needs to be full-filed by point-to-point encryption and cryptographic hash algorithms. The routing of data throughout the network demands much more consideration and focus.

Table 1. Information security triad implementation inter of things

IoT Layers	**Security Technique**	***Implementation***
Sensing Layer	Authenticity	The authenticity can be ensured through encryption and digital signature along with cryptographic hash algorithms.
	Data Privacy	Privacy cannot be ignored at any level. So, lightweight cryptographic algorithms and encryption algorithms are crucial for the privacy of information to prevent unauthorized access to information assets.
Network Layer	Authenticity	At this layer, authentication can be provided by point-to-point encryption algorithms to block unauthorized access.
	Routing Security	Information routing is very sensitive to errors. To make sure of error-free routing some robust routing mechanisms either with multiple routing paths or only recognized routing path selections, can be adopted.
	Data Privacy	Data is to be ensured for its safe and sound utilization. The data privacy techniques are useful to detect intrusion attacks and verification authorized users. The integrity helps to the correctness of data.

(Continued)

Table 1. Information security triad implementation inter of things *(Continued)*

IoT Layers	Security Technique	*Implementation*
Middleware Layer	Confidentiality	At this layer level, a better lightweight cryptographic algorithm with cryptographic keys and cryptographic hash method helps in data confidentiality. Confidentiality must be checked during the data exchange process.
	Data Storage	Good data storage with encryption of stored data can provide efficient data protection to data storage. For this, instead of using a centralized cloud service, we can use a decentralized Blockchain for reliable and secure data protection.
Application Layer	Authenticity	User authentication is crucial at this point. Different authorization and authentication methods help to prove user authorization and identity.
	Intrusion Detection	At this layer intrusion detection gives a lot of advantages. The data can be kept safe if the intruder is timely identified. The intrusion detection mechanisms can be applied to constantly monitor the user activities and send the acknowledgment to the system if any suspicious activity is monitored over the system. It may use a data mining approach to detect intrusion.
	Data Security	At the application layer level, firewalls can be a good choice to protect data and also prevent information stealing or tempering in information.

However, the routing security is required to ensure that the data transmission or reception is only from the trusted user and from the recognized path as described in Table 1. At the Network layer level, data privacy is only to ensure the authorized and trusted user is sending or receiving the information as described in Table 1.

At the middleware layer level, confidentiality plays a vital role. CIA triad provides complete security in terms of data confidentiality, user and information provider integrity, and availability of request information to the authorized user as described in Table 1. Data or information availability requires good guaranteed and secured data storage. So, data protection is essential to secure using encryption and cryptographic algorithms. Also, decentralized BlockChain services can be utilized instead of centralized cloud services for secured data storage and information usage as described in Table 1. The data can be kept safe if the intruder is timely identified. The intrusion detection mechanisms can be applied to constantly monitor the user activities and send the acknowledgment to the system if any suspicious activity is monitored over the system. It may use a data mining approach to detect intrusion.

7 Conclusions

Information Security is the major concern for IoT devices and applications. Since the advent of IoT, its applications and devices have experienced an exponential increase in numerous applications which are utilized. The IoT device differs widely in capacity storage, size, computational power, and supply of energy. With the rapid increase of IoT devices in different IoT fields, information security and privacy are not addressed well. Most IoT devices having constraints in computational and operational capabilities are

a threat to security and privacy, also prone to cyber-attacks. This study presents a CIA triad-based information security implementation for the four-layer architecture of the IoT devices. The data can be kept safe if the intruder is timely identified. The intrusion detection mechanisms can be applied to constantly monitor the user activities and send the acknowledgment to the system if any suspicious activity is monitored over the system. firewalls can be a good choice to protect data and also prevent information stealing or tempering in information. It may use a data mining approach to detect intrusion. Confidentiality plays a vital role. CIA triad provides complete security in terms of data confidentiality, user and information provider integrity, and availability of request information to the authorized user. The CIA triad-based technique for the enhanced information security and further research for fully adoption of application-specific IoT mitigation and countermeasures of the information security concerns is the future challenge.

8 References

[1] Da Xu, L., He, W., and Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10: 2233–2243. https://doi.org/10.1109/TII.2014.2300753

[2] Khatua, P. K., Ramachandaramurthy, V. K., Kasinathan, P., Yong, J. Y., Pasupuleti, J., and Rajagopalan, A. (2020). Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. Sustainable Cities and Society, 53: 101957. https://doi.org/10.1016/j.scs.2019.101957

[3] Dehghantanha, A., Internet of Things Security and Forensics: Challenges and Opportunities. Future Generation Computer Systems, 78: 544–546, 2018. https://doi.org/10.1016/j.future.2017.07.060

[4] Abozeid, A., AlHabshy, A. A., and ElDahshan, K. (2021). A Software Security Optimization Architecture (SoSOA) and Its Adaptation for Mobile Applications. International Journal of Interactive Mobile Technologies, 15(11). https://doi.org/10.3991/ijim.v15i11.20133

[5] Alghamdi, M. I. (2020). Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. International Journal of Interactive Mobile Technologies, 14(16). https://doi.org/10.3991/ijim.v14i16.16953

[6] Narayandas, V., Archana, M., and Raman, D. (2021). The Role of MANET in Collaborating IoT End Devices: A New Era of Smart Communication. International Journal of Interactive Mobile Technologies, 15(13). https://doi.org/10.3991/ijim.v15i13.23045

[7] Shaikh, A., Ali, S., Memon, N., and Karampelas, P. (2010). SOA security aspects in web-based architectural design. In From Sociology to Computing in Social Networks (pp. 415–430). Springer, Vienna. https://doi.org/10.1007/978-3-7091-0294-7_22

[8] Shah, A. A., Solangi, S. A., and Shah, A. A., Cloud Computing for Bio-Iinformatics: A Pakistani Perspective," in Third National Conference On Emerging Trends In Bioinformatics & Biosciences, October 2019.

[9] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7: 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

[10] Ali, I., Sabir, S., and Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309.

[11] Nagarkar, S., and Prasad, V. (2019). Evaluating Privacy and Security Threats in IoT-based Smart Home Environment. International Journal of Applied Engineering Research, 14.

[12] Frustaci, M., Pace, P., Aloi, G., and Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal, 5: 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291

[13] Global scale of installed IoT devices, Available online: https://www.informationmatters.net/internet-of-things-statistics/ (accessed on 10 August 2021).

[14] Panchiwala, S., and Shah, M. (2020). A comprehensive study on critical security issues and challenges of the IoT world. Journal of Data, Information and Management, 2: 257–278. https://doi.org/10.1007/s42488-020-00030-2

[15] Miraz, M. H., Ali, M., Excell, P. S., and Picking, R. (2015). A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). In 2015 Internet Technologies and Applications (ITA) IEEE, pp. 219–224. https://doi.org/10.1109/ITechA.2015.7317398

[16] Liu, S., Yue, K., Zhang, Y., Yang, H., Liu, L., and Duan, X. The Research on IOT Security Architecture and Its Key Technologies. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), October 2018, IEEE, pp. 1277–1280. https://doi.org/10.1109/IAEAC.2018.8577778

[17] Guo, H., Ren, J., Zhang, D., Zhang, Y., and Hu, J. (2018). A scalable and manageable IoT architecture based on transparent computing. Journal of Parallel and Distributed Computing, 118: 5–13. https://doi.org/10.1016/j.jpdc.2017.07.003

[18] Obaidat, M., Khodiaeva, M., Obeidat, S., Salane, D., and Holst, J., Security Architecture Framework for Internet of Things (IoT)," In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), USA, October. 2019. https://doi.org/10.1109/UEMCON47517.2019.8993096

[19] Mosenia, A., and Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5: 586–602. https://doi.org/10.1109/TETC.2016.2606384

[20] Sadique, K. M., Rahmani, R., and Johannesson, P., (2018). Towards security on internet of things: applications and challenges in technology. Procedia Computer Science, 141: 199–206. https://doi.org/10.1016/j.procs.2018.10.168

[21] Dhanvijay, M. M., and Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks, 153: 113–131. https://doi.org/10.1016/j.comnet.2019.03.006

[22] Ahanger, T. A., and Aljumah, A. (2018). Internet of things: a comprehensive study of security issues and defense mechanisms. IEEE Access, 7: 11020–11028. https://doi.org/10.1109/ACCESS.2018.2876939

[23] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., and Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20: 3453–3495. https://doi.org/10.1109/COMST.2018.2855563

[24] Nat'l Inst. of Standards and Technology, NIST Cloud Computing Forensic Science Challenges, NIST draft NISTIR 8006, 2014.

[25] NIST Computer Security Division. F. I. P. S. Standards for Security Categorization of Federal Information and Information Systems; NIST FIPS 199; NIST: Gaithersburg, MD, USA, 2004.

[26] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., and Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirica Look on Internet-Scale IoT Exploitations IEEE Common. Surv. Tutor, 21: 2702–2733. https://doi.org/10.1109/COMST.2019.2910750

[27] Ghadeer, H. Cybersecurity Issues in Internet of Things and Countermeasures. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII),, USA, October 2018. https://doi.org/10.1109/ICII.2018.00037
[28] Said, O., and Masud, M. (2013). Towards internet of things: Survey and future vision. International Journal of Computer Networks, 5: 1–17.
[29] Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., and Hayajneh, T. (2018). Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet of Things Journal, 6: 410–420. https://doi.org/10.1109/JIOT.2018.2854714
[30] Al Hayajneh, A., Bhuiyan, M. Z. A., and McAndrew, I. (2020). A novel security protocol for wireless sensor networks with cooperative communication. Computers, 9: 4. https://doi.org/10.3390/computers9010004
[31] Hayajneh, T., Griggs, K., Imran, M., and Mohd, B. J. (2019). Secure and efficient data delivery for fog-assisted wireless body area networks. Peer-to-Peer Networking and Applications, 12: 1289–1307. https://doi.org/10.1007/s12083-018-0705-6
[32] Alam, T. (2018). A Reliable Communication Framework and Its Use in Internet of Things (IoT). IJSRCSEIT, 3: 450–456. https://doi.org/10.31219/osf.io/cmza5
[33] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., and Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21: 1636–1675. https://doi.org/10.1109/COMST.2018.2874978
[34] Jaswal, K., Choudhury, T., Chhokar, R. L., and Singh, S. R., Securing the Internet of Things: A proposed framework, In Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, May. 2017. https://doi.org/10.1109/CCAA.2017.8230015
[35] Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., and Brown, J. (2020). A Comprehensive and Systematic Survey on the Internet of Things : Security and Privacy Challenges, Security Frameworks , Enabling Technologies , Threats , Vulnerabilities and Countermeasures. Comput. Artic., 9: 1–43. https://doi.org/10.3390/computers9020044
[36] Ojo, M. O., Giordano, S., Procissi, G., and Seitanidis, I. N. (2018). A review of low-end, middle-end, and high-end IoT devices. IEEE Access, 6: 70528–70554. https://doi.org/10.1109/ACCESS.2018.2879615
[37] Urien, P. An innovative security architecture for low cost low power IoT devices based on secure elements: A four quarters security architecture. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, January 2018, pp. 1–2. https://doi.org/10.1109/CCNC.2018.8319309
[38] Newsome, J., Shi, E., Song, D., and Perrig, A., The Sybil attack in sensor networks: Analysis & defenses. In Proceedings of the Third International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, April 2004, pp. 259–268. https://doi.org/10.1145/984622.984660
[39] Andrea, I., Chrysostomos, C., and George, H. Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC), Larnaca, Cyprus, 2015, IEEE, pp. 180–187. https://doi.org/10.1109/ISCC.2015.7405513
[40] Puthal, D., Nepal, S., Ranjan, R., and Chen, J., (2016) Threats to Networking Cloud and Edge Datacenters in the Internet of Things, IEEE Cloud Comput., 3: no. 3, 64–71. https://doi.org/10.1109/MCC.2016.63
[41] Alelyani, T., Shaikh, A., Sulaiman, A. A., Asiri, Y., Alshahrani, H., and Almakdi, S. (2021). Research Challenges and Opportunities Towards a Holistic View of Telemedicine Systems: A Systematic Review. Enhanced Telemedicine and e-Health: Advanced IoT Enabled Soft Computing Framework, 3–26. https://doi.org/10.1007/978-3-030-70111-6_1

[42] Imran, K., Anjum, N., Alghamdi, A., Shaikh, A., Hamdi, M., and Mahfooz, S. (2022). A Secure and Efficient Cluster-Based Authentication Scheme for Internet of Things (IoTs). CMC-Computers Materials & Continua, 70(1), 1033–1052. https://doi.org/10.32604/cmc.2022.018589

[43] Shaikh, A., and Alghamdi, A. (2020). IoT, smart environments and interdisciplinary applications for technology management and sustainable development. International Journal of technology management & sustainable development, 19: 257–261. https://doi.org/10.1386/tmsd_00025_2

9 Author

Dr. Mana Al Reshan received the B.S. degree in information systems from King Khalid University, Abha, Saudi Arabia, in 2007, the M.S. degree (Hons.) in computer, information, and network security from DePaul University, Chicago, USA, in 2011, and the Ph.D. degree in computer science from The Catholic University of America (CUA), Washington, DC, USA, in 2019. He was a Teaching Assistant with the College of Computer Science and Information System, Najran University,Saudi Arabia, from 2007 to 2009. He was a Lecturer with the College of Computer Science and Information System, Najran University, in 2012, where he is currently an Assistant Professor and head of network engineering department. His current research interests include computer network and security, system security, wireless and mobile security, body area networks, and cloud security.

Article submitted 2021-09-03. Resubmitted 2021-10-13. Final acceptance 2021-10-13. Final version published as submitted by the authors.