Towards Security Challenges to Internet-of-Things: Big Data, Networks, and Applications

Shurug Alseady, Abdullah Baz, Tahani Alsubait, Louai Alarabi, Hosam Alhakami

College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Summary

The recent era has witnessed a significant orientation towards investment and simulation of the real systems into smart systems that are based on using the Internet-of-Things. Internet-of-Things aims to interconnect distributed smart devices or sensors for simulating a specific domain system. Big data is considered to be a result of this connection. This research aims at discussing the importance of Internet-of-Things and examining the risks of simulating smart systems. Furthermore, the study also examines the architecture of smart Internet-of-Things (IoT) system and a structure layer of IoT risks by depicting a structure of Internet-of-Things challenges. The structure's design is based on four layers that include: authorization, big data, security, and integrity. This paper extracts the risk impact level (from highest to lowest) of various smart applications. The study also shows a comparison between multiple smart applications of Internet-of-Things in various domains and the main challenges that are faced by them. A comparative study of previous research studies, presented in this league, reveals that the attacks and hacks are the highest risks for smart applications. After which, data integrity is the next issue of concern while using the smart applications.

Keywords: *Internet of Things; Security Challenges; Big Data; Networks.*

1. Introduction

In the era of digital technology, the implementation of real smart environment, more essentially, the Internet-of- Things (IoT) devices has become the subject of extensive research. It is very important to use the IoT applications in various domains to automate the controlling process of systems and facilitate decision making remotely. They can save lives, buildings, and other things in several situations. IoT will generate $14.4 trillion in net profit for enterprises over the next two decades. Organizations across all industries have started to develop and implement their own IoT strategies with the aim of seizing the opportunity that this new era presents.

However, the usage of IoT comes with its own set of security challenges. The recent studies done in this domain present several solutions for the challenges in Internet-of-Things (IoT) and suggest means to improve decision making for the real applications [1, 2]. By 2020, the expected communicated sensors through the Internet for smart domain are going to reach thirty billion sensors. According to the latest statistics, the number of sensors will increase to seventy-five billion in 2025 (as shown in figure 1) [3]. It is evident that there has been acceleration in the use of technology and modern methods for securing data and network connection.

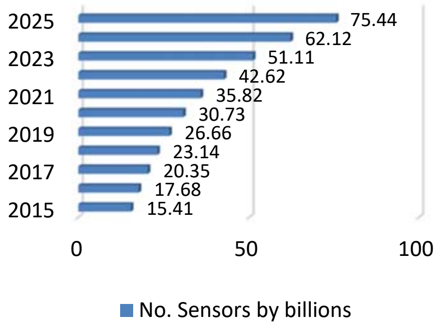


Figure 1: A Recent Statistics of Usage Percentage of IoT Sensors and Devices [3]

More specifically, IoT provides the connection between many devices via Internet [4]. Big data, which is gathered from multiple sources, is a powerful improvement in business investment and systems simulation. The massive volume of extracted sensory data that is obtained from the sensors or IoT devices shows a main obstacle challenge for the applications based on IoT solution. Prior motivations present solutions for Big Data that include analyzing data, classification, clustering, or prediction. *Smart home, smart parking, smart city, smart farming, smart government, smart energy, and smart transportation* are examples of IoT domains [5, 6, 7, 8, 9, 10]. IoT aims to interconnect distributed smart devices or sensors for simulating a specific domain system. Any IoT architecture system needs automation, good connection,

Manuscript received November 5, 2020.
Manuscript revised November 20, 2020.
https://doi.org/10.22937/IJCSNS.2020.20.11.17

huge and qualified servers, and consistent management.

Figure 2: The Main Architecture of IoT for Various Domains [14]

Big data relies on a set of extracted data with various volumes beyond the ability of commonly utilized software applications. The analysis done by big data is based on the concurrent time. Big data has four essential properties; these are known as the 4V: *volume, variety, velocity and veracity* [11]. The 4V can be elucidated as- Big data comes in large amounts, as in the, *volume*. Big data is a mixture of architecture and big information (*variety)*; it arrives at (often real-time) speed (*velocity*), and can be of uncertain provenance (*veracity*). Big data has perceptible advantages. The benefits of big data are real and often far-reaching which is why so many organizations have adopted big data for their own operations.

The main objective of this research is to present a survey for IoT research trends and demonstrate its importance. The study also enumerates several applications, and challenges in this domain. There are two types of IoT challenges- one is related to the data, and the second challenge is related to the connection issues (such as security). This research focuses on the security problems in the connections between sensors in the systems based on IoT. It discusses the architecture of smart IoT system and a structure layer of IoT risks. The structure of challenges is based on four layers: *authorization, big data, security, and integrity*. This paper extracts the risk impact level (*from the highest to the lowest*) on various smart applications.

The rest of this paper has been envisioned as: Section 2 discusses the architecture of IoT, and its' importance. Section 3 discusses the network construction of IoT, Section 4 presents the impact of big data on IoT, Section 5 presents several studies of IoT applications, Section 6 presents the open research challenges and threats to IoT. Section 7 details the discussion, and finally, conclusion and future work in the chosen field has been elaborated upon in Section 8.2. The Architecture of Internet of Things

The main idea of IoT is blending communication between various devices as simulating human actions. The meaning of "Things" is devices that are holding the data and connected with themselves. Thus, big data is generated by extracting data from various devices with different data types to interpret real situations and environments.

A. Architecture

Any smart environment requires a big communication network due to the sensors' big data: loading, processing, and updating that are utilized for supporting fast connection. This process requires a high consistency of systems.

The main architecture of IoT includes four layers that are: *Application, processing, network, and perception layers,* as shown in Fig.3. A brief explanation on all the four layers is enlisted below:

1. *The Perception Layer* is an essential layer of the IoT. It is an interface between the real environments and the information world. The perception layer refers to the connection between sensors through the network to convert the sensed data into the network.
2. *The Network Layer* is responsible for the communication between smart IoT devices. It supports the connectivity with several communication protocols, network interfaces, communication channels, and information maintenance. It is considered to be a link between the perception layer and the processing layer to hold data.
3. *The processing layer* is considered to be a middleware layer that manages and interprets the extracted big data, which drives the inference data interoperability through various IoT sensors.
4. *The application layer* refers to the high-level management for any IoT application. It manages any smart IoT application that is based on different ways as multimedia, augmentation of reality, or the Human-Computer Interaction (HCI).

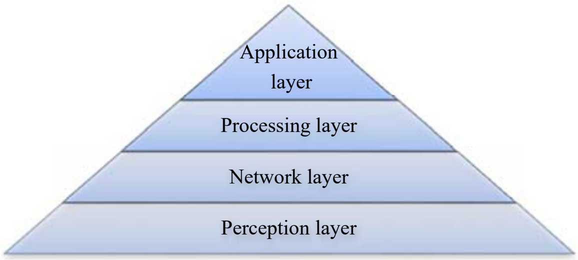


Figure 3: The Main Architecture for any IoT System [13]

B. The Importance of Internet-of-Things

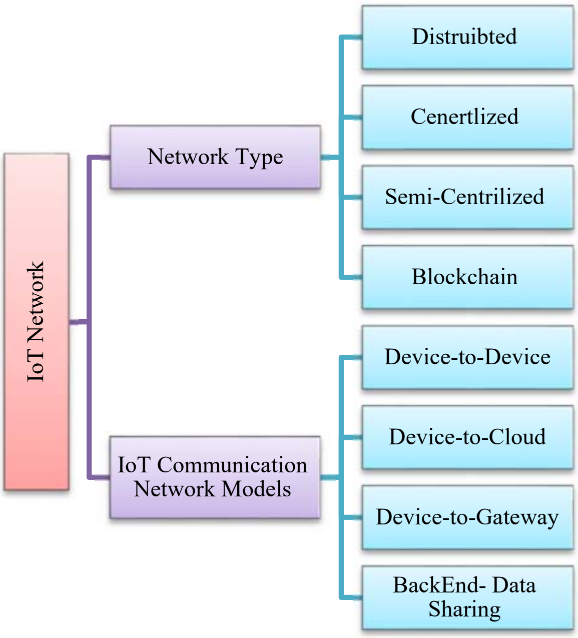
IoT is an innovation revolution in simulation of personal and professional applications. This is one of the most significant features of IoT and the key reason for the extensive use of IoT in the industries. The market for using IoT for managing, monitoring, and operating the fragmented array of IoT networks, sensors opened in 2019. IoT market is likely to generate extra revenue of $344 billion in 2020 due to minimizing costs by $177 billion. By 2022, there will be 28.5 billion networked sensors. Another 127 sensors are communicated to the internet every second. The industry will develop $15 trillion from IoT applications by 2025.The extracted sensory IoT data will be raised based on the automation customer service and sales efforts utilizing customer relationship management (CRM) software. The use of smart devices in IoT is expected to reach the figure.3 of $14 trillion in the global economy by 2030.

3. The Construction of Internet of Things Network

The IoT network requires two steps that include: Choosing the type of network, and the type of communication model of the constructed network (*as shown in Figure 4*).

A. The IoT Network Type

There are three types of the network of any IoT, *Distributed, Centralized, Decentralized or Blockchain* network (As shown in Figure 2 and 3).



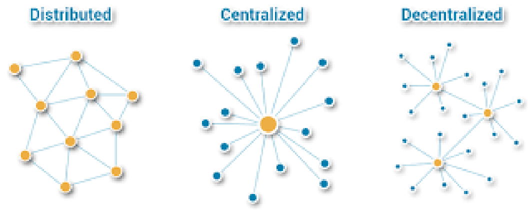


Figure 4: IoT Network Types [4]

Mostly, Distributed Network is the main network type of IoT. Recent researches apply the blockchain mechanism in constructing IoT applications due to the powerful of security data and devices on the blockchain networks as shown in Figure 4, 5. It refers to a series of linked blocks using cryptography wherein each block includes hash function to reach high security.

B. The IoT Network Communication Models

There are four types of communications between IoT devices; these are: (i) Device to Device Communication, (ii) Device to cloud Communication, (iii) Device to Gateway model, (iv) Back-End Data sharing model. Each model requires securing sensors for granting the data and network connection, as indicated in Figure 5 above.

Figure 5: IoT Communication Models [14]

The Device-to-Device network model connects several devices to communicate and exchange messages. The Device-to-Cloud network model communicates data through an Internet connection that is based on transmitting the user viewing data on the cloud network for analysis and enhancing the capabilities of the device. The Device-to-Gateway network model connects the IoT devices to connect the network from the gateway. Finally, the Back-End-Data sharing network model includes analyzing smart object data from various sources including cloud service.

The data is then uploaded onto different applications' service providers. The architecture also helps to collect the data and analyze it through the IoT sensors and the utility systems. This model enables us to access the extracted sensed information and analyze them.

The connectivity between IoT devices is based on automated data exchanging between various devices without any manual or human inference. Mostly, it is based on Wireless Sensor Networks (WSN) for connecting between nodes over limited frequency and bandwidth. This connection includes four main things that are: *Sensors, microcontroller, and memory and radio transceiver*. This mechanism requires determining a suitable communication protocol. Furthermore, it also requires guaranteeing the full power of the battery to save the real readings. The extracted sensed data is fused from multiple sources based on the wireless sensors through participation amongst the various nodes. The transmission process between various nodes on the network requires data and Multi-hop transmissions for taking diverse traffic loads. It needs Radio Frequency Identification (RFID) that includes data tags interacting with each other automatically. RFID tags utilize the extracted waves from radio frequency to interpret and exchange sensed data between many nodes.

4. The Impact of Big Data on Internet of Things

Big data plays a vital role in powerful analysis and fusion data for IoT applications. It relies on the extracted sensed data from smart sensors on IoT network. Big data has several keys and features that include: Volume, Variety, Velocity and Veracity for improving the analysis. The big data is generated from heterogeneous sensors. The analysis of big data is composed of three essential levels of*: Storage, processing,* and *the measurement of accuracy.*

The IoT network connects between various types of smart devices. This connection must be available for 24 hours. The fusion of big data is the main challenge in interpreting data from multiple data sources due to identifying the target. Each smart device has a data type, and a target.

5. Internet of Things Applications

Any smart system requires a huge network communication system, powerful servers, and high-quality computers.

Researchers in [15] built a smart medical system for monitoring the patients remotely. The system achieved an accuracy of 95% in warning about the ailments and detection of the ailing cases. Although the system showed good results, a challenge was found in identifying the hidden layers. Researchers in [16] introduced a smart health system for after surgeries observations that recorded an accuracy of 95%. However, it still faced a shortage of unification scheme for various surgeries. Researchers in [17] presented a graphical smart system to visualize the patients' cases in the real-time. The system released alerts for doctors about sudden cases. But it required the use of additional feature or dimension reduction to improve the system. Researchers in [18] proposed a mobile application system for the smart education system in classrooms. This system had a limitation of high implementation cost with variant sensors. Researchers in [19] provided smart parking for reserving the available parking places automatically. However, it still required motivation to ensure the available places for the parking automated systems. Researchers in [20] presented a smart home that guaranteed reliability. Nevertheless, it required enhanced security. Researchers in [21] introduced a smart home system for home automation and safety alarms system. But it took a long time to implement and required high cost for the IoT devices. Researchers in [12] provide a smart system for saving Researchers in [22] introduce a small simulation system in Masdar Dhabi. However, it faces a challenge of users' management. Researchers in [23] simulate a smart city system for managing energy remotely. On the other hand, it has a lack of security system. Researchers in [24] provide a smart system for saving energy and electricity in Amsterdam city but has a problem with the consistency of the network.

6. Open Challenges and Threats

There are several challenges that demand workable solutions in the context of IoT applications. These challenges could be related to the network, or associated with the extracted data [25,26].The main challenges are authentication, integrity, multiple users, and attacks or hacks as shown in Figure 6.

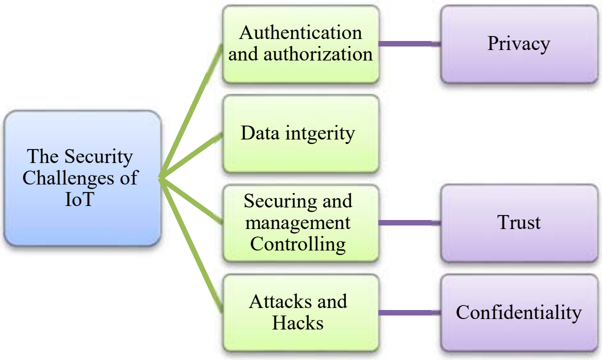

The Security Challenges of IoT
Authentication and authorization
Data intgerity
Securing and management Controlling
Attacks and Hacks
Privacy
Trust
Confidentiality

Figure 6: The Security Challenges of IoT

A) Authentication

Protecting user's information is crucial in IoT domain [27,28,29]. Each user must choose a password that should be strong to avoid compromising the system by a brute force attack. An authentication approach means guarantee user's accounts and accessing profiles with right usernames and passwords. Therefore, it is important to ensure the quality of user's authentication based on a password that is not redundant, or verification questions. Recently, researchers have examined many types of attacks, the types that threaten the user's accounts. They classify the authentication into static and dynamic. Privacy is a very important challenge during data transmission.

After analyzing the previous researches, the authors conclude that the open challenges are in how to reach the most powerful and secure authentication [30, 31, 32, 33, 34, 35]. The authors recommend a combination of several types of authentication as a password, and image password or pin code. Recent researches provided the facial, fingerprint or iris print to improve the security level and save the user's accounts.

B) Data Integrity

Integrity refers to protecting data for any IoT system [36]. The main objective of data integrity is preventing data corruption and avoiding the errors of data. There are two types of data: the *Common or normal data* and the *Sensitive or important data.* The encryption process is used to save sensitive information. Data integrity is the most important issue in cloud networks. It requires guaranteeing data on the server for real-time access. The main types of data integrity are physical and logical. Physical integrity faces challenges in the correct storing and fetching of data. Logical Integrity may be affected by data faults or errors such as ultimate temperatures, or sudden high pressures. Previous researches presented the types of data integrity and concluded that the problems in data integrity may be happen due to the failure in hardware, problems in data fusion and interpretation. The integrity can be evaluated by the correctness and reliability measurements [37, 38, 39, 40].

C) Securing and Management Controlling from Various Users

Smart IoT systems and applications have many users which may cause inference of orders and conflicting decisions [41]. Therefore, the IoT system requires to be completely secured to avoid risks of users' accounts or controls. This can be achieved by creating trust between users while transmitting data. But this aspect is a new trend of research, and it does not get enough attention because most automation techniques aim to control remotely only, but the recent trend aims to control and enable decision making by multiple users [42,43]. Each user has a control panel that may be different from others such as a smart IoT health environment that can simulate the hospitals and healthcare remotely. The users are physician, nurse, and hospital recipient employees. Each user has some authority, available decisions and different results. However, in the other smart IoT environment such as Smart Home, all the users can manage all the devices (for example: *opening the light, opening the conductors, closing the TV*, etc.) and show all reports of the house (*such as the temperature of the house*). The current trend of this challenge is entitled *Social IoT* that interprets how to manage users' decisions and activities remotely [44, 45]. Table 1 shows a comparison between several researchers' proposed techniques, strengths and weakness in IoT security challenges.

Table 1: A Comparison between Several Implemented Systems of Smart IoT Environment

Paper No.	Domain	Features	Strengths	Weaknesses
[41]	Smart Medical	Monitoring patients remotely	It improves decision making with 95% of useful warning detection.	The difficulty of choosing the optimal number of hidden units
[42]	Smart Medical	It is based on creating surgical prediction multi-model for patients	It enhances the rate of accuracy of 95%. Minimum redundancy (mRMR)	The shortage of unification scheme for multimodal surgical data
[43]	Smart health	It presents a new tool based on graphical visualization issues for monitoring patients.	It relies on implementation of machine learning techniques for generating patients' model and creating alerts to be sent to doctors	It requires summarizing data that may be needed to use dimension reduction or feature reduction
[44]	Smart Education	It uses mobile application system	It demonstrates the future Classrooms that holds several machines or devices connected needs	Requires good network and requires huge systems to records all actions.
[45]	Smart Parking	It executes by utilizing the sensor circuitry and cloud server	Provides the reservation parking process from mobile application simultaneously.	Requires several sensors and it is hard to ensure that the same people park in the reservation places
[46]	Smart home	It works in real time stream, remotely management, and safety system	Guarantee reliability	Requires more privacy characteristics to improve the security system
[47]	Smart home	It is based on the specific application for managing the home. It does not connect to Internet continually.	It provides home automation and safety alarms system.	It takes long time of using this implementation. It needs enhancing the management of several user management to secure their accounts and decisions.
[48]	Smart City	Masdar city -Abu Dhabi	It introduces a small simulation system for experiment and implementation 2030	It takes long time for using this implementation. It requires to enhance the management of several user management to secure their accounts and decisions.
[49]	Smart City	Amsterdam city	It supports saving energy and management control	It requires training the same in several application and cities. Requires more security systems.
[50]	Smart Energy	Amsterdam city	It provides smart energy network.	It needs to have network consistency.

D) Attacks and Hacks

There are two types of attacks: *Passive* and *Active* (as shown in Figure 7). An active attack is defined by the trials of editing the resources or making an impact on the processes of these resources. A passive attack is defined by the benefits of users' information through the system but that does not make any impact on the resources of the system. The most popular attack in smart IoT network is Denial-of-Service (DoS) that targets cutting off the connection in between the resources in the system.

The construction of any smart IoT system relies on several layers to save data and network (as shown in Figure 3).

The first layer is known as the perception layer. It is divided into IoT devices such as sensors, and Bluetooth. These sensors are threatened by cyber-attacks and physical attacks for example:

1) Physical attack on a node in the network.
2) Creating a fake node in the network, stealing user's information through attacking the side channel of the user.
3) Physical damage as Daniel-of-Service (DoS) attacks.
4) Eavesdropping attack

The second layer is known as the network layer. It includes checking the security measurements to guarantee data integrity and confidentiality.

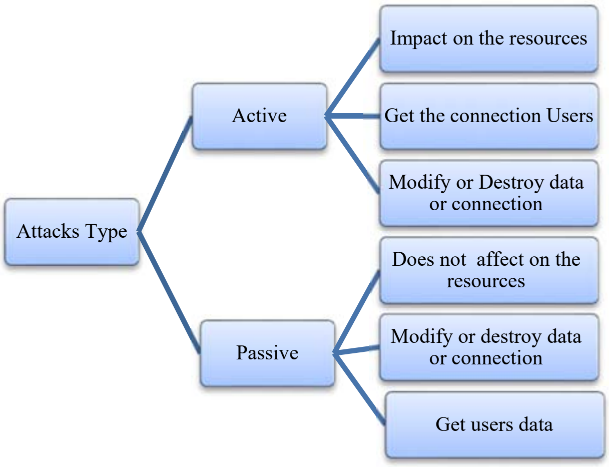

Attacks Type
Active
Passive
Impact on the resources
Get the connection Users
Modify or Destroy data or connection
Does not affect on the resources
Modify or destroy data or connection
Get users data

Figure 7: Types of Attacks on IoT Networks

There are several attack types in this layer such as *Eavesdropping attack, and DoS attack, or Virus infestation*. Data security is also a big obstacle. While transmitting data smoothly, it is significant to avoid from observing sensors on the Internet. The main problems in this layer are:

1) *Heterogeneity:*

It refers to the integration of various technologies. The networks require multi-access control approaches for being safer and interoperability.

2) *Network Congestion Challenges*

These congestions arise due to the multi-user controls which refer to a big number of required authentications devices on the network. This leads to congestions and requires high consistency and ordering data. The network challenges include several parameters like problems in trying to reach a stable and good network. These parameters are hardware, network connection, structure, software, and cloud network.

The IoT network requires a suitable hardware, powerful sensors, multiple protocols or standard systems. The IoT should guarantee constant connection of the wireless network to sensors that gather data. The main structure of an IoT network produces fundamental collaboration between billions of objects. To apply an IoT system, installing several software algorithms is required to predict the user's route. Therefore, the security is very significant for saving software.

3) *Eavesdropping Attack*

This challenge refers to knowing the environment of the wireless devices because every device type differs in the attack works.

4) *Denial of Service (DoS) Attack*

It refers to an overload of traffic on the network.

5) Sybil Attack:

It refers to the demand for recognizing the nodes [13, 14].

The third layer is entitled processing layer security. It is independent of other layers, and cloud computing security which is a large domain of security. It takes care of data security and interoperability that relies on confidentiality and securing data on the cloud. Interoperability is still the main challenge in security layers due to the variant nature of standards from users. It also includes identity theft or routing attack challenges. The challenge of identity theft means that the unauthorized user can detect authentication data like usernames and passwords. The routing attacks challenge is impacted by a big threat of IoT system security.

Finally, the last layer is known as the application layer that refers to the missing unification schema for building the applications based on IoT. But there are some common properties and features for these applications for example authentication privileges: all users are required to have access control page with username and password. A malware attack can pilfer the user's data by denial of service. Using some viruses such as the *Trojan horse* can be very harmful for the security of the system and data. Phishing Attacks refers to stealing the user's identity with emails and passwords for corrupting and managing them.

Table 2 shows a comparison between several implemented systems of smart IoT environment. It also presents strengths and weaknesses of each system.

Although there are several solutions for open challenges in IoT, there are still some problems in accuracy and performance results in IoT in the data or the network. Security of extracted big data and network is extremely important. Therefore, blockchain network is highly recommended to achieve the desired level of security of data. Blockchain network is very powerful due to the cryptography of blockchain system. Accuracy, performance, and reliability are the current measurements for any IoT system.

Table 2: A Comparison of the Researchers' Studies in Various Smart IoT Systems

No.	Challenge	Challenge Type	Technique	Result	Strengths	Weaknesses
[51]	Secure the network	Attacks and hacks	Query processing algorithm	It saves the encrypted data of IoT on the cloud. Efficient database query processing	Security with encrypted data. Reduces latency. Improves performance time.	It requires encoding algorithms.
[52]	Secure the network from attacks	Attacks and hacks	It computes the latency hiding technique	It reduces the gap between computation and communication latencies in each iteration	The technique minimizes latency that applies a fraction of the large query size.	Requires improving the performance of the proposed algorithm.
[53]	Secure the network and data integrity	Attacks and data integrity	It uses integrity methods	Provides the Confidentiality and Integrity	Confidentiality, authenticity, and integrity protection of communication	Complex and requires negotiation between parameters to improve the trust and reliability results
[54]	Talos practical secure system	Data integrity	Provides encrypted data	The results combine the encrypted query processing into IoT systems.	The optimization encryption schemes	Limitation of reliability
[55]	Authentication	Authentication	Facial recognition combined with password	Good results but requires long time	Improve the security	Complex in the implementation
[56]	Social IoT	Various users' controls	Targets improving the Decisions	Good decisions in the real-time	That is very useful especially in huge systems such as smart organization or smart factory	Complex interpretation and requires solving the decisions and controlling concurrently

7. Discussion

This research discusses IoT technology that is used in smart environments that simulates real applications through communicating sensors. Previous researches that motivated the authors to examine the impact of IoT challenges have been illustrated in Figure.8. The figure shows that most of the challenges exist in various IoT applications, then in data integrity [28, 29, 36, 37, 38, 41].

The challenges also focus on security dimensions that include data and security issues. The figure presents the main architecture of constructing any IoT environment.

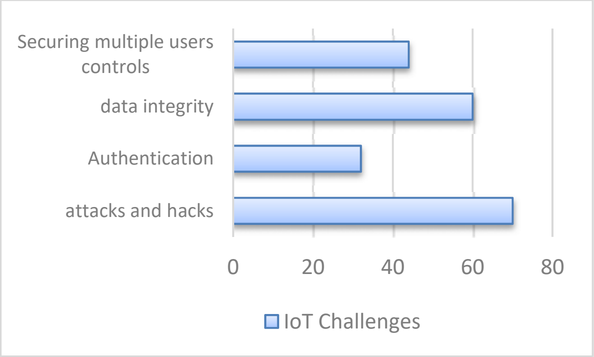


Figure 8: The Importance of IoT Challenges

Manuscript received November 5, 2020.
Manuscript revised November 20, 2020.
https://doi.org/10.22937/IJCSNS.2020.20.11.17

Table 3: The Most Common Attack Types in each layer of IoT Architecture (High rating happens)

IoT layer	**Attack Types in Each Layer**			
Perception layer	Physical attack	Fake node	Theft attack	Eavesdropping attack
Network layer	Eavesdropping attack	Hack virus	Sybil attack	Daniel-of- service (DoS)
Processing layer	Fake node (users)	Daniel-of-service (DoS)	Eavesdropping Attack	Routing attack
Application layer	Software attacks	Fake node (users)	Virus attack	Malware Attack

Table 4: Less Common Attack Types in each Layer of IoT Architecture (The lowest rating happens)

IoT layer	Attack Types in each layer	
Perception layer	Routing attacks	Daniel-of-service (DoS)
Network layer	Phishing attack	Theft attack (fake node)
Processing layer	False data attack	Phishing attack
Application layer	Daniel-of-service (DoS)	Eavesdropping Attack

Table 3 includes the classification of the highest number of attacks that occur due to constructing any IoT architecture. In the same context, table 4 depicts the lowest number of attacks that occur in each layer of IoT architecture.

The findings from Tables 3 and 4 reveal that *fake node, sybil attack and eavesdropping attack* are the most dangerous attacks in constructing IoT applications, as shown in Figure 9. *Phishing attack and false data* are the lowest occurring attacks with the lowest risk in real applications ofIoT.

Cryptography is the main dimension for securing any IoT system, and this requires measuring the accuracy, performance, and reliability for checking the qualified system. Though it increases the complexity of the system, the technique affords high security on the network. We recommend the use of blockchain networks in IoT systems which are more secure for multiple users.

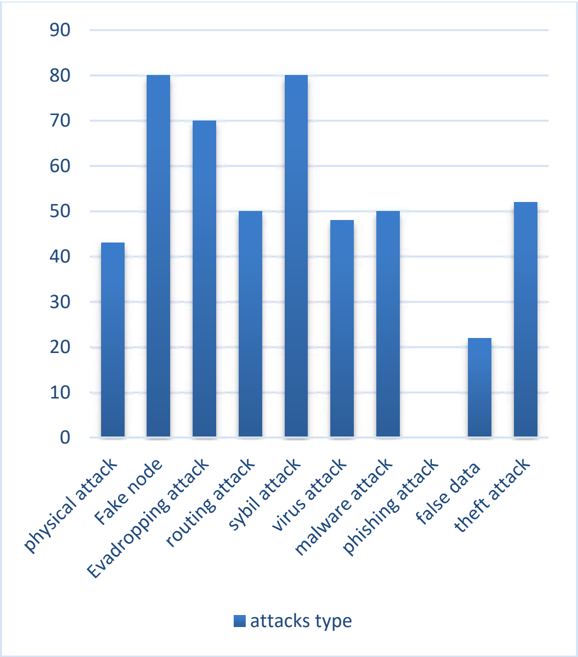


Figure 9: The Dangerous Level of Attacks on IoT Networks

8. Conclusion and Future Works

Internet-of-Things (IoT) is defined by the communication between group of devices and sensors via Internet that can improve decision making. It can observe and manage the extracted data from these devices and sensors remotely at the same time. IoT field, because of its pivotal role in the present context of digital world, has become a subject of intensive research as more and more sectors are aiming to implement the real smart environment to automate systems and manage them remotely. By 2020, the expected number of communicated sensors through Internet for smart domains is likely to be thirty billion. There are four challenges of IoT. These are: authorization, big data, security, integrity. This paper extracted the risks impact level (from highest to lowest) on various smart applications. Besides this, the study also mapped a comparison between multiple smart IoT applications in various fields and the main challenges faced by them. This research discussed the importance of IoTs and provided a survey of these challenges. The study presented a relationship between each layer of IoT architecture and attacks' types. The result of this relationship concluded that there are three dangerous attacks which are repeated continuously. These are- Fake node, Sybil attack, and Eavesdropping attacks. On the contrary, Phishing attack and false data have the lowest impact on IoT layers.

Acknowledgement

This research was financially supported by Umm Al-Qura University. We gratefully acknowledge the support and the generosity of the University without which this study could not have been completed.

References

[1] Guobao Xu , Yanjun Shi, Xueyan Sun, and Weiming Shen, Internet of Things in Marine Environment Monitoring: A Review, Sensors, volume 19,2019.

[2] Mohamed Abomhara and Geir M. Køien, Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security, Vol. 4, 65–88,2015.

[3] Statistics: precentage of increasing usage Internet-of-Things devices, avaibale online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[4] AlejandroFernández-Montes,JuanAntonioAlvarez-Garcia,JuanAnto- nio Alvarez-Garcia, Luis Gonzalez-Abril, Smart Environment Software Reference Architecture, Conference: INC, IMS and IDC, 2009. NCM '09. Fifth International JointConference on, 2009.

[5] Gomez, Carlesa, Chessa, Stefano, Fleury, Anthony, Roussos, Georged, and Preuveneers, Davye, Internet of Things for enabling smart environ- ments: A technology-centric perspective, Journal of Ambient Intelligence andSmartEnvironments,vol.11,no.1,pp.23-43,2019.

[6] Heike Bach and Wolfram Mauser, Sustainable Agriculture and Smart Farming,Inbook:EarthObservationOpenScienceandInnovation,2018.

[7] Maxv.Schönfeld,ReinhardHeil,andLauraBittner,BigDataon a Farm—SmartFarming,book:BigDatainContext,2018.

[8] M Sajid Khan, Mina Woo, Kichan Nam, and Prakash K. Chathoth, Smart City and Smart Tourism: A Case of Dubai, Sustainability volume 9(12, pp.2279,2017

[9] Hamad Al Mansoori, Asbi Bin Ali, and Mohammad Khaled, Nature and Quality of Smart Government Services: The Case of the UAE Services: The Case of the UAE, International Journal of Enhanced Research in Science,Technology&Engineering,Vol.5Issue1,January-2016

[10] V. Kepuska and Humaid Alshamsi, Smart Car Parking Sys- tem,International Journal of Science and Technology Volume 5 No. 8, August,2016.

[11] HamidMedjahed,DanIstrate,JeromeBoudy,Jean-LouisBalginger,and Bermadette Dorizzi, A pervasive multi-sensor data fusion for smart home healthcare monitoring,IEEE International Conference on Fuzzy Systems (FUZZ-IEEE2011),2011.

[12] "Iot logo png," Iot logo download free clip art with a trans- parent background on Hercules cliparts 2019. [Online]. Available: https://retohercules.com/explore/iot-logo-png.html. [Accessed: 25-Dec- 2019].

[13] Molugu Surya Virat, et al., ,Security and Privacy Challenges in Internet of Things,Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018), 2018.

[14] Md Husamuddin, and Mohammed Qayyum, Internet of Things :A Study on Security and Privacy Threats, Conference: The 2nd International Conference on Anti-Cyber Crimes (ICACC) organized by IEEE, 2018

[15] Negar Memarian a,b,n, Sally Kim b, Sandra Dewar, Jerome En- gel , Richard J. Staba , Multimodal data and machine learning for surgery outcome prediction in complicated cases of mesial temporal lobe epilepsy,Computers in Biology and Medicine,issue 64, 2015

[16] Milos Radovic, Mohamed Ghalwash, Nenad Filipovic, and Zoran Obradovic, Minimum redundancy maximum relevance feature selection approach for temporal gene expression data, BMC Bioinformatics, Vol- ume 18, issue 9,2017

[17] Antonino Galletta, Lorenzo Carnevale, Alessia Bramanti, Maria Fazio,An innovative methodology for Big Data Visualization for telemedicine, IEEE TRANSACTIONS ON INDUSTRIALINFORMAT-ICS, 2018.

[18] Shahbaz Pervez, Shafiq ur Rehman, and Gasim Alandjani, ROLE OF INTERNET OF THINGS (IOT) IN HIGHEREDUCATION,Proceedings ofADVED2018-4thInternationalConferenceonAdvancesinEducation and Social Sciences, 15-17October 2018- Istanbul, Turkey

[19] Shruthi Mudaliar , Shreya Agali , Sujay Mudhol, and Chaitanya K Jambotka, IoT Based Smart Car Parking System,IJSART - Volume 5 Issue 1 –JANUARY 2019 ISSN [ONLINE]:2395-1052

[20] ZaiedShouran,AhmadAshar,andsTriKuntoroPriyambodo, Internetof Things (IoT) of Smart Home: Privacy and Security, International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 39, February 2019

[21] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, IoT Based Smart Security and Home Automation Sys- tem,International Conference on Computing, Communication and Au- tomation (ICCCA2016)

[22] Governament of Abu Dhabi. (2008). The Abu Dhabi economic vision 2030. Abu Dhabi: Abu Dhabi Council for Economic Development & others.

[23] Lee, J. H., & Hancock, M. (2012). Toward a framework for smart cities: A comparison of Seoul. Research Paper. San Francisco andAmsterdam:Yonsei University and Stanford University

[24] Eleonora Riva Sanseverino, Raffaella Riva Sanseverino, Valentina Vaccaro, Ina Macaione and Enrico Anello, Smart Cities: Case Studies,SpringerInternationalPublishingAG,SmartCitiesAtlas, 2017

[25] Jyoti Deogirikar and Amarsinh Vidhate, Security Attacks inIoT: A Survey, International conference on I-SMAC (IoT in Social,Mobile,Analytics and Cloud), 2017

[26] JariPorra*,JaydenKhakurel,AnttiKnutasandJouniPänkäläinen, Security Challenges and Solutions in the Internet of Things,Nordic and BalticJournalofInformationandCommunicationsTechnologies,volume 2018, issue 1, pp. 177-206,2018

[27] Inayat Ali, Sonia Sabir ,and Zahid Ullah, Internet of Things Security, Device Authentication and Access Control: A review, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016 459 https://sites.google.com/site/ijcsis/ ISSN 1947- 55003.2.6

[28] Aleksandr Ometov, Vitaly Petrov, Sergey Bezzateev,Sergey Andreev, Yevgeni Koucheryavy, and Mario Gerla, Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications,IEEE, arXiv:1901.06977v1 [cs.NI],2019

[29] H. Shafagh, A. Hithnawi, A. Droescher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing for the Internet of Things," in Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom),Paris,France, 2015, pp. 251–253

[30] R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query processing on encrypted data for the Internet of Things," in Proc. 25th Int. Conf. Comput. Commun.Netw. (ICCCN), Aug. 2016, pp. 1–7

[31] C. Katsini et al., "Security and Usability in Knowledge-based User Au- thentication: A Review," in Proc. 20th Pan-Hellenic Conf. on Informatics, p. 63, ACM,2016.

[32] Suhardi and Alfian Ramadhan, A Survey of Security Aspects for Internet of Things in Healthcare,Information Science and Applications (ICISA), pp 1237-1247, 2016.

[33] Nitesh Rastogi, Avinav Pathak , and Shweta Rastogi, Enhanced Authen- ticationSchemeusingPasswordIntegratedChallengeResponseProtocol,International Journal of Computer Applications 62(9):15-19, 2013

[34] Syed Zulkarnain Syed Idrus , Estelle Cherrier, Christophe Rosenberger, and Jean-Jacques Schwartzmann, A Review on Authentication Methods, Australian Journal of Basic and Applied Sciences 7(5):95-107,2013.

[35] D. Dinesh Kumar, K. Vijay, S. Bhavani, E. Malathy, and R. Ma- hadevan, A STUDY ON DIFFERENT TYPES OF AUTHENTICATION TECHNIQUES IN DATA SECURITY,International Journal of Civil Engineering and Technology (IJCIET),Volume 8, Issue 12, December 2017, pp. 194–201,2017

[36] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Sta- jano, Passwords and the Evolution of Imperfect Authentication, appeared in Communications of the ACM vol. 58 no. 7, July 2015pp. 78–87

[37] Mohammed El-hajj, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni, A Survey of Internet of Things (IoT) Authentication Schemes, sensors ,2019

[38] N. Modadugu and E. Rescorla. The Design and Implementation of Datagram TLS. In Network and Distributed System Security Symposium (NDSS),2004.

[39] HosseinShafagh,AnwarHithnawi,AndreasDröscher,Simon Duquen- noy, and Wen Hu, Talos: Encrypted Query Processing for the Internet of Things,SenSys'15, Republic of Korea, ACM,2015

[40] Gift Matsemela, Suvendi Rimer,Khmaies Ouahada, Richard Nd- jiongue,and Zinhle Mngomezulu,Internet of things dataintegrity,IST-Africa Week Conference (IST-Africa), 2017

[41] Lei Hang and Do-Hyeun Kim, Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity ,Sensors (Basel), volume 19 (1),2019

[42] Roopa M.S., Santosh Pattar, Rajkumar Buyya, Venugopal K.R., S.S.Iyengar, and L.M.Patnaike, Social Internet of Things (SIoT): Foun- dations, thrust areas, systematic review and future directions,Computer CommunicationsVolume139,1May2019,Pages32-57

[43] SeungminRho and YuChen, Social Internet of Things: Applications, architectures and protocols,Future Generation Computer Systems Volume 82, May 2018, Pages667-668

[44] Shahbaz Pervez, Shafiq ur Rehman, and Gasim Alandjani, ROLE OF INTERNET OF THINGS (IOT) IN HIGHER EDUCATION,4th International Conference on Advances in Education and Social Sciences, 15-17 October 2018- Istanbul, Turkey,2018

[45] Luigi Atzori, Antonio Iera, Giacomo, MorabitoMichele, and Nit- tiMichele Nitti, The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization, Computer Networks 56(16),2012.