International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I4P142

Volume 68 Issue 4, 266-272, April 2020

Original Article

Security and Privacy Concerns of the 'Internet of Things (IoT) in IT and its Help in the Various Sectors across the World

Sikender Mohsienuddin Mohammad

Wilmington University

Received Date: 26-03-2020
Revised Date: 09-05-2020
Accepted Date: 10-05-2020

Abstract *- The so-called Internet of things (IoT) is a form of technology advancement that has the capacity for driving change in our daily lives in a variety of sectors. The fantastic opportunity will help in the collection of data that is relatively exponential and in a manner that is continuous to present changes that are significant in our lives. Devices growth and the speed at which they are developed to attain the IoT era of technology offers the challenges of security and the battling of freedom as people establish policies and governance that rebuilds the developments without interfering with the innovations. Among the issues includes the concerns on the security and privacy brought by the technology. The vulnerabilities of security that are experienced by the IoT devices are a result of the contributing factors like the low capabilities of the devices in terms of energy and the capabilities of computing, the wireless channels are seemingly unreliable, and the vulnerabilities in the physical nature of the devices. This paper will focus on the IoT evolution, the definitions attached to IoT, and some of the many applications of IoT. It will create an emphasis on the considerations of security and privacy, including the challenges that are tied to the general IoT and the IoT application context. A critical assessment of the works done for IoT is presented by the literature review on the perspective of the developmental era and the evaluation of the trend. The paper will also give the IoT security risks taxonomy, mechanisms, and attacks related to the technology.*

Keywords *- Internet of things, threats, privacy, security, encryption, trust, protocols, authorization, data integrity, confidentiality, authentication*

I. INTRODUCTION

IoT began as an expression that was used in 1999 for the first time Kevin Ashton. The phrase started gaining definitions and has come to hold several of them that are more or less bold under the connotations that are linking. In this paper, IoT will be defined as the interconnection of computing devices that are embedded and exceptionally identifiable within the infrastructure of the Internet that is existing and offers connectivity to the devices in an excellent way, hence offering services that are beyond the scope of a machine to machine communications and has a variety of applications in its protocols and domains (James et al., 2018). The word thing refers to the things that are smart and can be observed in all the surroundings in recent days. The bright ideas can be categorized as having capabilities of data processing and aggregation and having the ability to communicate between themselves and with their users (Mendez et al., 2017). However, the critical feature is the ability of intelligence of contacting with its environment and by the use of individual sensors.

The technology of IoT is regarded as a development that is capable of delivering changes that are dramatic in our lives. It is also recognized as a technology that enables efficiency increase in several areas, including the logistics and transport, healthcare system, and the manufacturing field. IoT will optimize the process that is stated through excellently analyzing data and develop a catalyst in the segments of the new market by developing capital in the characteristics of the physical cyber (Guedalia et al., 2018). All this will result in a rise of applications that are cross-cutting and offer quality services. The scope is increased exponentially, especially within the last decades hence bringing the privacy and security issues as well. However, not all societies have full knowledge of the problem yet. When this problem is ignored, it will lead to consequences that will be seemingly unpleasant for people using smart devices as part of their daily life (Alaa et al., 2017). Since it is also deployed not only by individuals but also, organizations will also be affected as they too use the smart devices due to data protection being limited and the security of data being compromised.

Overly, IoT is an aspect that is growing and expanding the technology hence apparently tending to require countermeasures that are evolving in handling the privacy concerns that are arising. To protect the rights of the consumers, there have to be legal measures as an approach that will not hamper the innovations in any aspect (Li et al., 2017). The adaptation speed of the new

generation is nonetheless much less than the renovations and improvements of the technology of IoT. Therefore, the IoT of the modern era has features that are beyond the current legislation (Chen et al., 2017). Notably, the process of tracking the users of the web is already an experience that is relatively old fashioned.

II.LITERATURE REVIEW

Today, the revolution of the Internet has impacted our lives profoundly. The new technology of the data-led transformations is witnessed and is referred to as the Internet of Things (IoT) which is relatively transforming every industry in the world. It aims to create uniformity on everything in the world under one umbrella whereby the things cannot be easily controlled and monitored, but their state can be recognized (Singh et al., 2017). Internet of things tends to transform the objects of the real world to become objects that are smart and virtual, allowing the machine to be human and human to seamless machine communication. The recent studies address the concepts of IoT through the reviews of systematic scholarly research papers, including online databases (Xiaojiang et al., 2020). The research papers provide a focus on the IoT chronology, definitions, pre-requisites of the IoT and provide an architecture overview, the technologies, and the challenges and applications related to the adoption of the technology.

However, computing technology has had power advancement. In recent days, new connectivity levels sensing has become of lower costs, and analytics has become accessible by the use of the Internet. It has made IoT become possible and interweaving with the digital world and the mechanical world, bringing a transformation that is profound to many of the aspects of life (Alaba et al., 2017). The combination of access to data and data exchange in the field of IT has significantly opened new prospects that enable applications for IoT. Almost half of the connections on the Internet exists between things or with things. In 2011, there was witnessed over 15 billion things on the web (Yang et al., 2017). The anticipations are that by the end of 2020, there will be 30 billion and above things that are connected on the Internet hence enabled by the technologies that are key like the sensors that are embedded, recognition of image technology, and the NFC, therefore, transforming the Internet of Things become the Internet of everything.

IoT in recent days is expected to offer connectivity that is classic and goes beyond the machine to machine communications (M2M). Thus, IoT has promised to enable the real world to become one thing with the virtual world (Guedalia et al., 2018). A group of internet-based solutions referred to as the Cisco internet Business Group has forecasted that over a total of 50 billion devices will have an internet connection by the end of 2020 hence refuting the 30 billion approximation. Since technology is rapidly advancing, the association of devices per individual is also seemingly increasing (Razzag et al., 2017). The research is conducted by considering the population of the world, and every individual is placed into account; hence when considering the actual number of people connected to the Internet drastically increases the number.

The IoT core components:

Hardware: comprises the sensory devices, the actuators and the communication system that is embedded.

Presentation: tools for interpreting and visualizing and can be accessed widely across the different platforms of technology and its applications.

Middleware: a tool for the mechanism of request storage and data analysis tools.

For apprehending an IoT vision that is effective, it is a must for it to cater for security, scale, and the computing that is oriented to market and resources for storage (Yu et al., 2018).

A. Growth and Evolution of IoT

The concept of connecting ‘things’ on the Internet is dated back before the term ‘Internet of things came to be used. Students at the University of Carnegie Melon-fitted the photosensors that were Internet-connected in the 1980s to a machine that was used to vend soft drinks and was able to allow them easily count the total number of cans being dispensed at a given time (Sahmim & Gharsellaoui. 2017). The technology allowed anyone who had internet access to be able to determine the number of drinks dispensed and the number of bottles remaining in the dispenser.

John Romkey and his colleague Simon Hackett developed a toaster before the creation of the first webpage. The toaster had internet access in 1990. The presentation made by Romkey at the conference interop in 1990 was able to feature an internet connection that was referred to as the Automatic Radiant for the Sunbeam Control toaster and was able to rise as it challenged the conference of the previous years made by the president of Interop Dan Lynch to Romkey (Kumar et al., 2017). Lynch gave a promise to Romkey of occupying the centre stage at the event if the project was successful. TCP/IP connected the toaster and had a Simple Network Protocol that was Information Based controller (SNMP MIB). Its primary function was to turn on or off the power source (Bertino & Islam, 2017). The term ‘Internet of Things’ came in use much later and was attributed to Ashton when he implemented the use of the words as a title for his presentation in 1999 at Procter and Gamble, and the term gained its publicity.

The table below indicates the features of the IoT today that are evolving. The predictions are based on the literature research and the past and current analysis developments of the IoT:

Year	Type of Technology	Size of usage	Type of connection	Data collection technique	'Thing' Interaction	System interaction
2000s	RFID	Millions	Wired	Identification	None	None
2010s	Phones, Sensors, Cloud	Billions	Wireless, H2M	Sensing	Buttons, Touch	Smartphones, Speech, Web
2020s	ICT in things, advanced technologies	Billions to Trillions	M2M, E2E, interoperability	Passive human, Coverage	Web interfaces, Haptic	Environment usage, Haptic
Uncertainties	Invisibility	Billions to Trillions	Standards, Ubiquity	Extent, Penetrating	Web interface prevalence	Using human sensing

The devices that are connected to the Internet has achieved rapid growth significance in recent days. The estimations that are made on the number of tools that will be joined in the future are becoming challenging to be asserted with confidence, and the estimates are being revised with the number tending to increase (Stojkoska & Trivodaliev, 2017). The reason behind the difficulties in the predictions is that the figures are not matching for the total devices that are connected with the Internet in this era of technology. According to Miraz (2017), not only do the statistics have significant differences by the use of same definitions but also there is the issue that concerns the interpretations that are varying on the IoT, thus creating an impact. However, some of the figures state that the difference that exists on the IoT devices and machine to machine (M2M) such as the GSMA, in which its analysis on M2M focuses on the cellular connectivity excluding the devices of computing in the consumer electronics (British Land, 2017). The gadgets include smartphones, tablets, and all the types that involve the connections technology of M2M and supports the IoT in a broader universe. A report was done in 2015indicated that the M2M total numbers of connections would rise from 5 billion in the year 2014 to approximately 27 billion by the year 2024. Therefore, there are no figures that are consistent for the approximation of the IoT devices that are connected since some devices are enormous, and they are still growing, and the growth is rapid (Ni et al., 2017).

B. Applications of the IoT in the United States and its Security and Privacy issues

Several domains have faced a significant impact from the IoT. Also, many researchers have provided analysis and insights on the applications of IoT. Researchers have adopted their fields of classifications on the implementation of the presentation of IoT applications (Mendez et al., 2017).

Merits are also attached to every taxonomy and do not primarily depend on the achieved objectives but also the context and definitions of the considerations of IoT. The following are the applications of IoT:

C. Autonomous Vehicles

One of the most significant areas that have experienced growth is the sensor application in the automotive sector. Cars use a considerable number of sensors in everything, starting from the operation of the engine to monitoring the system, emission control, and the brakes system. Examples are the tyre pressure monitoring systems that are Bluetooth-enabled, the position crank, the position of cam, absolute pressure manifold, and the position of the throttle (Maple, 2017). In the United States, sensors are embedded to form the part that is integral for the infrastructure of transport, such as the introduction of smart motorways on the highways programme. Also, the country has initiated infrastructural development and enhanced communications in urban surroundings (Sun et al., 2018). The cars are being platooned to reduce the consumption of energy and provide notice that is advanced during the occurrence of an incident by the use of communication called the V2V interface and adopts the DSRC technologies, the vehicle evolution long terms, and the connections through visible lights (Yang et al., 2017). Such a system of transport that is intelligent when deployed utilizes the cloud and edge technology which assists in the management of accidents, traffic that is locally based, and notifications of weather hence supporting driving assistance.

D. Security and Privacy issues in Autonomous vehicles

The field of connection on autonomous cars is complex and involves several sectors of sensing, actuators, infrastructure, protocols of communication, and other services. The services attached varies from the simple ones that run a few components up to the global services that involve the parts that are significant on the nation's infrastructure (Alrawais et al., 2017). The works of IoT cannot encompass the system types and potentials, including the attacks that are implemented. However, some of the most attacks that are significant can be highlighted. Communication in modern vehicles through the ECUs is channelled through several networks that include the CAN, MOST, and the LIN, among many others (ABI research, 2017). However, the design protocols of this system are prioritized on safety and efficiency rather than its security.

In 2015, the work of Miller and Valasek implemented the use of executing remotes to exploit the vulnerability of the IoT, which came along with weaknesses in the remotes that are Sprint enabled in the access UConnect. According to Alrawais et al. (2017). They were only able to control the vehicle when it was in motion. However, it seems that the likelihood of an occurrence of a cyber-attack on a car that is connected is low, making the vehicle importance increase and ransomware rise creating a more emerging risk to the availability and integrity of the connected vehicle and the automatic systems (BITAG, 2016). This also includes the motivations of finance, whereby attempts are seen by terrorists compromising these systems. Many CAV

involves data being sent externally. The data sent can be breached in various ways. An example is the use of stations that are sniffing. It is also capable of involving middle attacks on the communication that is wireless and enters a vehicle hence compromising the data integrity (Razzaq et al., 2017). Since the connections on the cars include Cloud and Edge infrastructures, the attack risks and impacts will increase on the availability of the system.

E. Healthcare system

The healthcare and medical technologies that are emerging adopts the use of sensors on the parts that are integral. IoT has the capabilities of being integrated into the services of healthcare that are numerous and its applications. The service in healthcare that will have a more significant benefit is the living ambient assistant system, whereby it's an application that is significant and involves the use of homes that are digitalised to enable the patient to monitor and care on the independent surroundings (Kumar et al., 2017). Also, the use of the Internet on mobile health integrates medical sensors into the technologies of mobile. The access to sematic medical, which utilizes the semantics applications for IoT healthcare services whereby rules for medicals are engineered to analyze a large number of data sensors. Also, the system for the reaction of an adverse drug whereby the drugs are labelled and examined in a medical database and the case of an adverse reaction such as allergy, or the drug reaction to the body is detected and avoided (Bertino & Islam, 2017). Other healthcare applications that are yet to be developed and have been developed include the monitoring systems for blood pressure, monitoring of rehabilitation systems, oxygen saturation systems and the management of wheelchair systems.

F. Security and privacy issues in the healthcare system

Attacks have risen recently when victims are hospitalized. There has been significant potentials and attacks that are actually on the connected devices of an individual, including the system of delivering drugs, implants that are electronic, pumps for insulin, and the pacemaker systems. In recent years, it has been discovered that there are unprecedented attacks on the surface and scale. Seizures have been targeting communication devices and protocols (Singh, 2017). The contemporary protocols for communication have experienced security flaws of many implantable cardiac defibrillators (ICDs). The medical systems have therefore posed significant risks to the patient. They have also disrupted integrity availability and have also been compromised, including confidentiality issues (Yu et al., 2018). The medical data can be used in the identification of theft and fraud as well as discovering the prescriptions of a drug, therefore, enabling the hackers to order particular medication by use of the online platform.

Hackers can also distort and develop a habit of blackmailing people who have a specific illness that they do not want to disclose. The IoT enabled attacks on confidence, integrity, and availability, such as the trackers for fitness, exist (Singh, 2017). However, its integrity on the availability and potential is not considered to be much severe. This case does not regard information confidentiality.

G. Logistics

IoT technologies support logistics dynamically due to the large numbers of increased shipment inventories enabling the provider of the service to increase the efficiency of operation while also integrating an increase in the automation and decreasing the processes that are done manually (Alaba et al., 2017). When IoT is deployed in logistics, there is an experience of an impact that is pronounced on the management of smart inventories, detecting damages, visibility on a real-time mode, and control of stock in an accurate way, utilization of assets in an optimal way, maintaining a prediction, and the management of freight services (Yang et al., 2017). When RFID technology is applied in the logistics sector, it enables the industries to be able to forecast Information trends of future identification, estimate the probability of an occurrence of an accident, and allow the adoption of remedial measures in an early stage (Guedalia et al., 2018). All these factors will enable the ability of an enterprise to respond to the needs of the market and cater for and risks attached to the supply.

H. Security and privacy issues on Logistics

Efficiency and business opportunities are offered significantly by the logistics of IoT. The attack surfaces on this framework have several scenarios that pose significant risks. An example of a recognized incident of attack is the manipulation of private data that is embedded by maliciously substituting the tags and modifying tag information (Mendez et al., 2017). Logistics are thought by many as being part of the network of a road, and it should be known that logistics are also done in air, sea, and rail services. A vulnerability concerning the shipment details modifications includes the speed, name, cargo, position, and the Mobile Maritime Service Identity status (MMSI) (Chen et al., 2017). The attack can be intensified further by creating a vessel that is fake and has all the details of the existing boat hence exploiting it. A good example is having a ship from Iran appear at the coast of the US (Singh et al., 2017). This leads to a system being compromised on confidentiality and integrity.

I. Buildings and Offices

Smart home devices have faced demands and significant growth in recent days. Between the years 2010 and 2016, there were over 161 million units that were shipped, according to the HIS Markit. The increase tends to have over 64% every year (ABI Research, 2017). The expansion includes the purchasing of management systems for energy such as the Nest thermostats, the August intelligent locks security solutions, and some other personal assistants like Google Home, Amazon's Alexa, and Bosch's Mykie. On the other hand, the adoption of the consumer to smart technologies has resulted in growth and

increased demand within the environments of an office (BITAG, 2016). In the United States, nearly a quarter of the decision-makers deduced that 90 per cent of the expressed responses had a wish of controlling their environments for work to be a better and more luxurious place. The study also indicated that a smart office has an impact that is significant on the performance of the company and its environment, with the productivity predictions surpassing an increase of 37 per cent, increased loyalty of over 38 per cent, and workers well-being and happiness having an improvement of more than 40 per cent according to Li et al., (2017). The growth of the demand for houses having IoT, offices and buildings contributes to the smart cities development.

J. Security and privacy issues in the Building and Offices

Security risks are compromised because the services and devices offer functional economic benefits. Privacy and confidentiality are the key risks that the tools represent. The Dyn attack is always exposed to the devices connected to the tools at homes (Chen et al., 2017). The lack of the tools being available is an inconvenience when the device power comes from one botnet hence creating a significant global impact. Apart from targeting smart home devices, hackers also target the automation of the building and the control system of the building (Xiaojiang et al., 2020). The attack on target was the most significant attack that utilized the buildings' internet connection control system. Therefore, access to the network of buildings, homes, or offices carries a threat that is wide not only to confidentiality but also to availability and integrity.

K. Media and Entertainment

The sector of media and entertainment is benefiting from IoT advancement. Research is also conducted for enabling services that will allow media to content sharing over the IoT networks that are home-based. It, therefore, provides the personal content to be able to become seamlessly and easy sharing of the media. Also, ads can be made private for individual families and communities, according to James et al. (2018). Potentials in the filtering of content based on age is an expectation that will have a significant impact on the industry of entertainment. Other applications on the gathering of news that is based on the user's location are also set to be enhanced. The entertainment sector has a significant area that is the game industry, and it is one of the sectors that a considerable impact will be established due to IoT (Guedalia et al., 2018). It has already been evidence of how the IoT combination with the system for augmented reality plays a significant part in the creation of game experiences that are new due to the popularity of Pokémon Go.

L. Security and privacy issues in the Media and Entertainment

The Internet of Things tends to change how industries operate by helping the management and valuing of data. The improvements also come with its risks since the media and entertainment industry is among the largest enterprises. The industry is a highly profiled target for cyber-attacks and, in some instances, provides malicious attackers with plenty of opportunities to launch their attacks (Mendez et al., 2017). The industry use data as a prominent subject and a vital tool to be able to figure out the needs of the customers. Therefore, developing a trustworthy and secure company becomes essential in revenue increase. Sensitive data is, therefore, a key element in this industry (Li et al., 2017). However, when the IoT becomes helpful, it can also face the security being compromised and leaving the company not being able to offer protection to its assets.

III.DISCUSSION

As it has been mentioned, balancing the personal services and the optimized services is very important to achieve the privacy that is desired. One way is ensuring that the context of the consumer to their data requires the collection, storage, and sharing security protocols (Kumar et al., 2017). However, several challenges have also been seen. The transparency of the system is, therefore, a vital element leaving the service providers of IoT with the task of ensuring that the data is made clear on what is collected for and the data requirements. A system of interaction that has no physical interface is required in the vision of IoT to become ubiquitous to its users (Razzaq et al., 2017). In this case, the consumer will be given data that has utmost privacy, and there will be no gap for the Information being compromised. The consent is also required to be quickly withdrawn and have a granular state.

When the IoT technology becomes embedded, the challenge of privacy and security being compromised will be faced up to the public areas. A good example is a data of a smart fridge that can be used in determining the habits of eating and health. Therefore, it may tend to affect the insurance of an individual's life with a company of insurance (Bertino & Islam, 2017). Also, in the field of smart toys, sensors and intelligence have been implemented in toys production. Therefore, they are made to have the ability to recognize voices, analyze, and be able to interact with the child. Thus, the toys can be used as a device for surveillance and can be hijacked to misbehave, according to Sahmim and Gharsellaoui (2017). The issue makes the toymakers being faced with the challenge of incorporating security on the connected toys. Personal data that has no explicit consent should not be handled. However, it seems challenging to separate the sets of data, and it appears that the handling of data on the toys will be without explicit consent.

IoT privacy concerns are also an impact on the industries in the United States apart from consumers. Due to the broad track surfaces of the IoT, then it becomes complex for the industrial level due to the vectors of attacks that are numerous (Alaa et al., 2017). A formulation of the privacy requirements is, therefore, required to have a proper definition. Beyond the violation of risks to the sensitive employees or the details of the customer, the possibilities of the competitors replicating the knowledge of an organization is opened up by the

potential loss of data that is intellectual (Jindal et al., 2018). This can significantly undermine the advantages of competition. This era has therefore received very little attention to the framework of privacy and security on the IoT.

IV.CONCLUSION

In this paper, I have discussed the origin of IoT and how it has resulted in a challenge that is major in the standardization of a single vision overly. It has henceforth given rise to security issues and the privacy of the assurance in IoT. The challenge that is the most significant one is in the coordination of the IoT. The task is difficult in the processes of technology and the aspects of politics. Considerations should be implemented of all the stakeholders and all the views they have that are conflicting on the IoT. There are different projects related to IoT that has indicated the involved difficulties in enabling trust between the parties with visions and interests that are different. A system for the IoT that is analogue will seemingly be beneficial but challenging in ensuring relevant outcomes that are acceptable to everyone.

It is relatively essential to consider that, for a standard to become successful, the project should consider the political factors in the creation. The advocates for privacy may utilize the development as an industrial deception and a criticism platform. The protocols of the system should not enable the services provided by the system to create illusions of privacy when acquiring personal data. It should be noted that a likely part of the solution can be from any standards of the system and in a manner that when the rule is implemented alone will not provide the system with adequate protection that is required. Therefore, the standards should be achieved with the tools for enhancing privacy.

The U.S departments provide numerous guidelines and practices that are best in the availability of IoT to organizations and individuals. The standards should also be in line with the compliance that is legal and regulatory. If there are no requirements of agreement or implications for finance when the protocols are implemented, the case business of the contracts will incur failure. The industry adoption probability may be maximized, and user acceptance should follow the managerial consent protocols of the IoT. It is therefore made clear that significant processes are made for the IoT, but there is still a gap for battling security and privacy issues.

REFERENCES

[1] ABI Research., What Is the Internet of Things? Accessed, (2017) https://www.abiresearch.com/pages/what-is-internet-things/,

[2] Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M., A Review o Smart Home Applications Based on Internet of Things. Journal of Network and Computer Applications, 97 (2017) 48-65.

[3] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. ., Internet of Things security: A Survey. Journal of Network and Computer Applications, 88, (2017). 10-28. https://www.researchgate.net/profile/Alaba_Fadele/publication/315835782_Internet_of_things_Security_A_Survey/links/58eb0ecf0f7e9b978f840e72/Internet-of-things-Security-A-Survey,

[4] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X., Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, 21(2) (2017) 34-42. https://www.researchgate.net/profile/Chunqiang_Hu/publication/314162879_Fog_Computing_for_the_Internet_of_Things_Security_and_Privacy_Issues/links/594924170f7e9b1d9b2765f8/Fog-Computing-for-the-Internet-of-Things-Security-and-Privacy-Issues.pdf

[5] Bertino, E., & Islam, N., Botnets and Internet of Things security. Computer, 50(2) (2017) 76-79.

[6] BITAG., Internet of Things (IoT) Security and Privacy Recommendations. BITAG Broadband Internet Technical Advisory Group (2016). http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[7] British Land., Smart Offices | British Land – The Office Agenda. Accessed(2017). http://officeagenda.britishland.com/smart-offices.

[8] Chen, J., Hu, K., Wang, Q., Sun, Y., Shi, Z., & He, S., Narrowband internet of things: Implementations and applications. IEEE Internet of Things Journal, 4(6) (2017) 2309-2314.

[9] Guedalia, I. D., Guedalia, J., Chandhok, R. P., & Glickfield, S., U.S. Patent No. 9,900,171. Washington, DC: U.S. Patent and Trademark Office., https://patentimages.storage.googleapis.com/01/32/2e/64461abca6c4a2/US9900171.pdf

[10] James, S. D., Fregly, A., & Cathrow, A., U.S. Patent No. 10,083,291. Washington, DC: U.S. Patent and Trademark Office, (2018). https://patentimages.storage.googleapis.com/d6/9b/8e/75d2a5949af424/US10083291.pdf

[11] Jindal, F., Jamar, R., & Churi, P., Future and challenges of Internet of Things. International Journal of Computer Science & Information Technology (IJCSIT) 10 (2018) 13-25. http://www.academia.edu/download/57176429/10218ijcsit02.pdf

[12] Kumar, N., Madhuri, J., & ChanneGowda, M.,Review on Security and Privacy Concerns in the Internet of Things. International Conference on Iot and Application (ICIOT), IEEE, (2017) 1-5.

[13] Li, N., Liu, D., & Nepal, S., Lightweight Mutual Authentication for IoT and its Applications. IEEE Transactions on Sustainable Computing, 2(4) (2017) 359-370.

[14] Maple, C., Security and privacy in the internet of things. Journal of Cyber Policy, 2(2) (2017) 155-184. https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536?scroll=top&needAccess=true&

[15] Mendez, D. M., Papapanagiotou, I., & Yang, B., Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879, (2017). https://arxiv.org/pdf/1707.01879

[16] Miraz, M. H., Ali, M., Excell, P. S., & Picking, R., Internet of Nano-Things, Things and Everything: Future Growth Trends. Future Internet, 10(8) 2018) 68. https://www.mdpi.com/1999-5903/10/8/68/pdf

[17] Ni, J., Zhang, K., Lin, X., & Shen, X. S., Securing Fog Computing for the Internet of Things Applications: Challenges and Solutions. IEEE Communications Surveys & Tutorials, 20(1) (2017) 601-628. https://bccl.ir/wp-content/uploads/2018/07/Securing-Fog-Computing-for-Internet-of-Things-Applications-Challenges-and-Solutions.pdf

[18] Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S., Security issues in the Internet of Things (IoT): a comprehensive study. International Journal of Advanced Computer Science and Applications (IJACSA), 8(6) (2017) 383-388. https://pdfs.semanticscholar.org/c192/7578a61df3c5a33f6bca9f9bd5c181e1d5ac.pdf

[19] Sahmim, S., & Gharsellaoui, H., Privacy And Security in Internet-Based Computing: Cloud Computing, Internet of Things, A Cloud of Things: A Review. Procedia Computer Science, 112 (2017) 1516-1522. https://www.sciencedirect.com/science/article/pii/S1877050917313923/pdf?md5=739a8c53ba3155cb85e808e6cc77624d&pid=1-s2.0-S1877050917313923-main.pdf&_valck=1

[20] Singh, B., Bhattacharya, S., Chowdhary, C. L., & Jat, D. S. (2017). A review on Internet of Things and its Applications in Healthcare. Journal of Chemical and Pharmaceutical Sciences, 10(1) (2017) 447-452.

[21] Stojkoska, B. L. R., & Trivodaliev, K. V., A review of Internet of Things for the Smart Home: Challenges and solutions. Journal of Cleaner Production, 140 (2017)1454-1464. https://iotiran.com/media/k2/attachments/A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions.pdf

[22] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G., Security and Privacy in the Medical Internet of Things: A Review. Security and Communication Networks, (2018) http://downloads.hindawi.com/journals/scn/2018/5978636.pdf

[23] Xiaojiang, X., Jianli, W., & Mingdong, L., Services and key technologies of the Internet of Things. ZTE Communications, 8(2) (2020) 26-29.

[24] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H., A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5) (2017) 1250-1258. https://www.researchgate.net/profile/Longfei_Wu3/publication/316173391_A_Survey_on_Security_and_Privacy_Issues_in_Internet-of-Things/links/5a256ec10f7e9b71dd087b26/A-Survey-on-Security-and-Privacy-Issues-in-Internet-of-Things.pdf

[25] Yu, Y., Li, Y., Tian, J., & Liu, J., Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Wireless Communications, 25(6) (2018) 12-18.