Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability

Kholoud Y. Najmi [a], Mohammed A. AlZain [a], Mehedi Masud [a,*], N.Z. Jhanjhi [b], Jehad Al-Amri [a], Mohammed Baz [a]

[a] College of Computers and Information Technology, Taif University, P.O. Box 11099, Al-Hawiya-Taif 21944, Saudi Arabia
[b] School of Computer Science and Engineering, SCE, Taylor's University, 47500, Malaysia

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Internet of things
Threats
Confidentiality
Reliability

ABSTRACT

The idea of the Internet of Things that everything is linked to anything and everything interacts with the other is a great idea, and that the topic of integrating these devices will add a remarkable change in this world and increase its prosperity, and this interconnection occurs through the exchange of data and information and facilitating our communication with the things around us. But questions about security and privacy remain. When this massive amount of data is exchanged, it will certainly be an attractive environment for attackers and hackers.

In this paper, we will present the issues of security and privacy, their main requirements, potential risks and tools to defend these risks, and a detailed review of security attacks in order to be able to deter these attacks achieve confidentiality, security and reliability for users.

1. Introduction

The Internet of Things, which is called IOT, is a new term that refers to the new form in which technical devices began to communicate with each other via the Internet, and it is a vast world in which we began to live in some of its aspects, connecting everything and anything[3] in any place and at any time as see in Fig. 1.

It indicates a huge and unprecedented exchange of data and information among these things, and it adds some imagination to real life, in view of countless sensors and remote interchanges to improve the personal satisfaction and change the impression of things around us. For example, if we talk about the refrigerator, how to connect to the Internet through some sensors and protocols and provide additional benefits, such as storing data for the items inside it, setting expiration dates and receiving food use notices, or using internal cameras while you are in the store to check for shortcomings in Your food.

And when we talk about these features and benefits, we also don't lose sight of the surrounding risks, security issues, privacy and threats related to IOT.

The future of the Internet of Things is expected to be limitless [4]. By increasing the speed of networks, integrated artificial intelligence, widespread deployment, automation, and regulation of their uses, you will accelerate the progress of the industrial internet. You'll benefit from massive amounts of actionable data which in turn can lead to business process automation as well. There will be a big trend in the IT markets. The trend of the Internet of things is not limited to the industrial and commercial fields only, but it surrounds us at home by controlling various home appliances, hospitals, as it has become a follow-up tool for patients and an assistant to doctors and provides a lot of services in this domain, and we do not forget the field of communications and energy control, and now in some of our daily belongings such as watches, cars and devices the other portable. And when we use these different technologies, we must provide a true level of safety. Because as much as the benefit comes the harm, and in the event of insecurity, it may return to us with security dangers and threats, and it is possible to exploit the vulnerabilities by hackers and manipulators to gain access to data and information, it is possible to manipulate and misuse it and make it work for them. It is possible to be exposed to several different attacks such as interference and denial of service (DOS), flooding, black holes and wormholes, sinkhole and

* Corresponding author.
E-mail address: mmasud@tu.edu.sa (M. Masud).

https://doi.org/10.1016/j.matpr.2021.03.417
2214-7853/

Fig. 1. Internet of things.

Sybil types. The security needs change from layer to layer as each layer fills an alternate need [5].

Sicari et al. [6] introduced research difficulties and the momentum arrangements in the field of IoT security zeroing in on the fundamental security issues which were recognized in seven classes: validation, access control, classification, protection, trust, secure middleware, versatile security, and strategy implementation. This paper focuses more on IOT's importance and various areas of use in the home, how it helps us, and in healthcare and how it has become part of the growth and prosperity of the health field. We discussed its various layers which are the sensor layer, network layer, transport layer, application layer, and the activity of each layer, notwithstanding the conventions utilized and deciding the long haul and their restricted reach. We additionally referenced the security dangers and countermeasures for each layer of IoT.

The first section will deal with background on the Internet of things and its most important applications, and in the second section we will talk about the layers of components and protocols used in IOT, and in the third section we will discuss risks, threats and potential attacks, and in the final section we will discuss the most important security measures, tools used and techniques to deter attacks.

2. What is IoT?

Kevin Ashton defined the term "Internet of Things (IoT)" [7] and was used primarily to describe basic things. A basic creation by "adding radio frequency identification and restart operation to everyday things."

We used the term "things" instead of "devices" because, quite simply, this technology includes everything that we can connect to the Internet. Despite the fact that the term is somewhat recent to our ears, its actual existence in life dates back to the seventies of the last century, specifically in 1974, which witnessed the emergence of automated teller machines, which are considered one of the models of IoT devices. But despite this age, studies indicated that approximately 87% of users in 2015 do not know the true meaning of this term or what it indicates exactly. These are very strange paradoxes because in 2008, according to Cisco, there are more devices connected to the Internet than humans connected to it. On the globe. This number almost reached five billion devices in 2018[8].

2.1. Applications of IoTs

IOT, this broad expression, is the most recent qualitative transfer in our life, and it has become an integral part of everything that surrounds us. It has been applied in many fields and we have different models for smart cities, smart homes, smart factories, smart security, healthcare and many areas of its application. Here we mention the most important applications of "healthcare" and "smart home".

2.1.1. Healthcare

In this time, the Internet of things has become important in several domains, most notably the health care domain. Here, we cannot do without it, as it function a very big role in providing services and saving lives. And it helped us to make a unique paradigm transmit by improving the condition of hospitals and taking more care and monitoring of patients. Also, its role is to assist doctors in diagnosing patients' condition and needs. Where it became possible to identify the patient's problem through the information and data that it provided on a timely basis. The (RMMP-HI) platform for remote monitoring and management of healthcare information has set the goal of prevention and early detection of diseases related to lifestyle through continuous monitoring and observation[1].

(Chu) and others [9] from Stanford University presented a wearable notch known as (BodyNet), which consists of wireless sensors that adhere directly to the skin to degrade the physiological signals emitted by the human body. To achieve this, the team used a variety of RFID language. When the chip is attached to the body, the hopper sends and receives radio waves from the device, stays energy to charge the chip and sends information on the physiological parameters of the person being tested. Currently, the slide is producing readings on respiration and pulse rate, but the team is endeavoring to integrate a scale. Heat and other sensors in their suggestion system. As in the Fig. 2 The employ of the MQTT protocol is light on the nodes rather than the protocols usually used in Internet applications. The results exhibit the ability of the proposed system to receive and serve a large number of requests in real time[1].

2.1.2. IoT in smart home

In this paper, we notice one of the main applications of the IOT, which is the smart home, and how this technology is able to control everything that contains the house and make it harmonious and compatible with the environment, and provides an unprecedented quality of life. In Fig. 3, the Internet is the link that connects several home appliances together. The Internet is the link that connects various home appliances together. Through it, it is possible to send and receive information and data, and by using platforms or application, these devices have been controlled remotely, such as

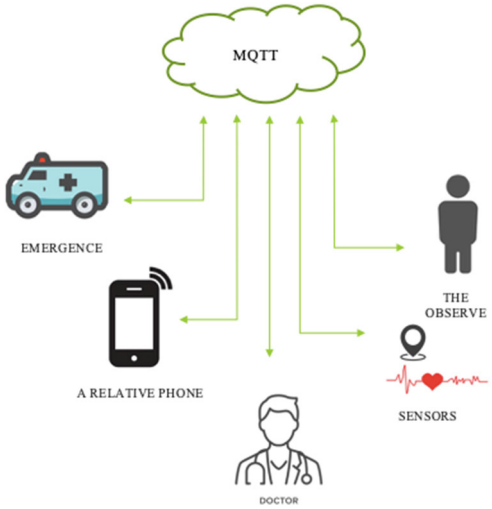

Fig. 2. Follow The Patient by (MQTT) . adopted from [1]

Fig. 3. Smart Home.

counters, windows, air conditioning, washing machine, oven and others. And also monitor the home to make sure of safety. The deployment of various sensors helps provide smart services to the user. And it helps to conserve energy by turning off electrical appliances and lights automatically when not in use. It offers users to automate their tasks and memorize their routines[10].

2.1.3. Smart cities

Smart cities are one of the applications of the Internet of Things, such as self-monitoring, automated mobility, smart environmental monitoring, and energy management. It is a real right to many problems pollution, poor infrastructure and poor energy supply. These cities consist of layers, each layer comprise technologies that assist in data production, analysis and manufacture, and what backing these layers is the strong communication infrastructure [11].

3. IoT architectures and protocols

This section provides a discussion of the four layers of the Internet of Things, what are the protocols used for networks and the protocols used for data.

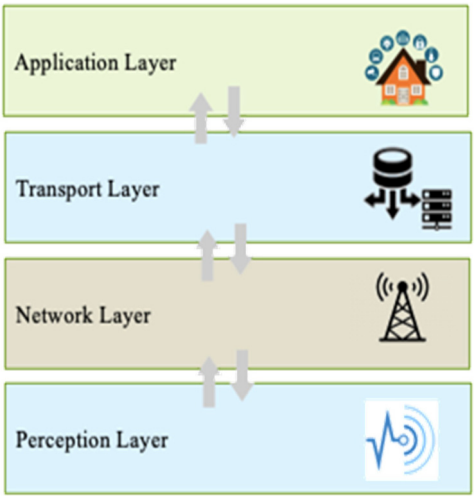

Fig. 4. IoT Architecture Layer.

3.1. IoT architectures

We can divide the Internet of Things into three layers ، As we can consider in Fig. 4.

3.1.1. Perception layer

It can be called (the physical layer) and it is the nursery layer for sensors, and it senses what is in its surroundings, and can collect information about it. This layer contains wireless sensor networks (WSNs) which monitors the physical and environmental conditions and passes this data across the network, and determines the radio frequency identification (RFID) through which we can send and receive data through radio waves, (GPS), (IMD) and others[12].

3.1.2. Network layer

It is a relationship that connects smart devices, network devices, and servers, and it is also possible to transfer and process sensor data. It included various networks of 3G, 4G, Wi-Fi, Infrared and WiMAX. Responsibility for carrying the incoming packets from the transport center on the network layer. A routing protocol has been developed for low power and lost networks called (RPL)[13].

3.1.3. Transport layer

Data floods are generated due to the heterogeneity of devices in the Internet of Things (IoT) architecture. This is where the middle layer works to fulfill two very important purposes, one is to manage the service and the other is to store the flow of information from the various layers in the database [8].

To merge with the vast amount of data that could affect IOT. The service may be disrupted in the Internet of Things through attacks that extend its impact to the processing layer such as (Burnout) and this occurs as a side effect of a hostile result. attacks, such as a DOS attack when the victim is overwhelmed with requests for a deficit in the system and make the network unavailable to the user. It is possible that the purpose of the attack is to exhaust the resources such as memory and battery [14].

3.1.4. Application layer

It is the interface responsible for providing services for the application or user.

It is responsible for the data format. Its dependence on the HTTP protocol although it is not sufficient when it enters in a resource-limited environment because it causes a large analysis burden due to the length. Alternative protocols such as MQTT and CoAP have been developed to deal with IoT environment[10].

3.2. IOT protocols

Here in this section we discuss protocols and how to ensure optimal security of data that is swap between IOT devices. We often hire IP (Internet Protocol) to establish a connection in IOT devices, and if the connection is local, then using Bluetooth and RFID is appropriate in this case[12]. There is a variation in the power range and memory used, we can say that IP networks are more intricate and their consumption of energy and memory increases, and the extent here is not a problem, unlike other networks that do not depend on the Internet protocol, the power consumption and memory is less and it has a narrow and limited extent. We can categorize IOT protocols into two main parts. We have summarized their most important features in Table 1 at the end of the section:

3.2.1. IOT network protocols

We can say that it allows data transfer from one party to the other, party, is used to connect devices over the network.

Table 1
Internet of things protocols and important feature.

Protocol		The most important feature
IOT network protocols	HTTP	lack of energy savings and battery life.
	Bluetooth	perfect communication safe, short area, low cost and energy,
	LoRaWan	helps reduce energy consumption.
	ZigBee	provides less energy consumption.
IOT Data Protocols	MQTT	requires less memory and low energy.
	CoAP	uses UDP.
	AMQP	ensure the safe and successful exchange and storage of messages.
	M2M	manage applications remotely.
	XMPP	this serves as the basis for presence.

3.2.1.1. HTTP. This protocol is commonly used for IOT devices, and is the basis of data communication over the web, but due to lack of energy savings and battery life, we cannot make it the preferred one.

The 3D printer is one of the models that uses the HTTP protocol.

3.2.1.2. Bluetooth. I don't think there is anyone in this world who has not heard the word (bluetooth) before. But do they know that it is one of the important protocols in the IOT?

It is one of the generality popular and widely used communication protocols in the surrounding field, providing us with perfect communication safe, short area, low cost and energy, and implements the wireless transmission between electronic devices. This protocol is existing in smart devices, smart watches and many devices that surround us, as it is the most advanced protocol in Internet technology[12].

3.2.1.3. Lorawan. It's a beautiful protocol mainly used in smart cities due to its low energy consumption and long area, and LoRaWan can connect battery-powered objects to the Internet wirelessly. One of the field of enforcement of this protocol is smart lighting in the streets, where we can control the intensity of lighting automatically according to the ambient lighting, which helps reduce energy consumption[15].

3.2.1.4. ZigBee. If we want smart objects to work together, ZigBee is the most appropriate protocol here, as it is frequently used in security systems in smart homes and provides less energy consumption [15].

3.2.2. IOT data protocols

When we need a protocol that connects between low-power IoT devices without any connection to the Internet, the IoT data protocols are the desired here. Here are some of the protocols in this section:

3.2.2.1. Mqtt. We say it is one of the preferred protocols in the Internet of Things, it is based on the TCP protocol, and it collects data from various devices such as smart watches, fire detectors and car sensors. It is economical, requires less memory and low energy. In it, information is exchanged over a communication, as in Figure 3 when it was used to monitor the patient's condition [1,15].

3.2.2.2. CoAP. Through this protocol, a request can be sent to the server, and the server can send a response [15]. It uses the UDP protocol, which is one of the important protocols in smartphones and controllers.

3.2.2.3. Amqp. Mention here one of the very secure protocols used mainly in banks and used in reliable communications, where the protocol tracks the message until it reaches its destination without fail. It consists of exchange, binding, and Message Queue. These three components ensure the safe and successful exchange and message storage[15].

3.2.2.4. M2M. If we want to manage applications remotely, this protocol is the most appropriate, and it is one of the protocols used in automated teller machines, smart homes and vending machines, and it uses public networks for communication and data exchange.

3.2.2.5. XMPP. It is a messaging and presence protocol utilized for multi-party chat, instant messaging and video calls, and this serves as the basis for presence.

4. Security threats and attacks in IoT

The benefits of the Internet of Things and its various applications in many domains have another aspect that we must not overlook, and it is full of risks and security threats that may affect the user. A lot of recent research indicates that 90% of consumers lack confidence in the safety of their internet devices. As a result, security is a prerequisite for us to be able to enable privacy and trust in the devices system[16,17]. IoT safeness is the area to focus on to secure connected devices and conserve networks, data and organizations in the IoT [9]. In view of the continuous increase and doubling of the use of Internet devices, the safety problems multiply and significantly. The traditional security technology of IoT technologies cannot be implemented directly due to its designed system. The large number of devices associated with this limited force presents us with problems of heterogeneity and scalability [10]. Therefore, it is necessary to take into consideration that the system is strong and flexible to face expected and unexpected risks. We must also execute the integration of safety mechanisms with the Internet of things, in order to be able to implement the appropriate algorithms and protocols. And since reliance in the exchange between Internet of things devices is done via wireless communication, this is considered a basic method for multiple attacks and breaching privacy. Given this, we urgently need to provide strict protection measures for the data exchanged.

Data security issues [18–21] aim to achieve reliability, confidentiality, availability and integrity, through which security problems can be solved using safety measures. When we ensure that authorized users have access to network resources and restrict any unauthorized users here, we have achieved reliability, and when we maintain data integrity and data accuracy by users The unauthorized people here achieve data integrity, and when there is no obstacle to the authorized access to network resources, applications and services here, availability is achieved [22]. We can utterance that security and privacy are a real challenge under the current circumstances[23].

5. Countermeasures

In this part of the paper look at and emphasize the necessity of securing the infrastructure for the Internet of Things. Ask manufacturers to seriously consider the importance of searching for the most effective and safe practical solutions. The manufacturers must ensure that the devices contact only approved services and ensure that they are not replaced by harmful instructions affecting the operation of the device. It is imperative to make sure in every communication of the authentication process before sending and receiving data and that this data is issued by a reliable and approved source. Fig. 5 shows us attacks on the various layers that manufacture the Internet of Things and countermeasures.

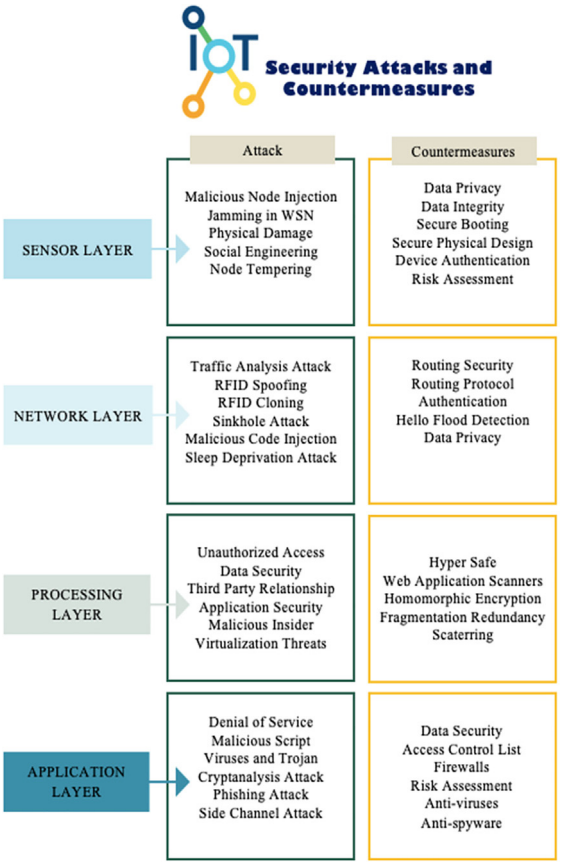

Fig. 5. IOT Attack and Countermeasures.

5.1. Security tools of IoT

In this section of the paper we will discuss the protection tools used in the Internet of Things.

5.1.1. M2MLabs mainspring

It is applied to build applications (M2M) such as remote monitoring or smart networks, and it is an open source application. Its capabilities extend to include device configuration and communication between device and application, it can verify data validity, store and recover lost data and rely on Java and Cassandra No SQL as a database[24].

5.1.2. Flutter

Flutter is a basic processor that can be programmed, and it is designed for students and engineers, and it contains a wireless transmitter that may reach more than half a mile, and is characterized by ease of use[24].

5.1.3. Ssl/Tls

This protocol uses asymmetric encryption to achieve the necessary security for the data and can guarantee the verification of the client's identity. Enhancing security using certificates may be smart locking by installing an authenticated server certificate and requiring client certificate and encryption.

5.1.4. Node-Red

It is a security tool that links the application programming indicator, IoT devices, and services provided using a browser-based flow editor[24].

5.2. Internet of things safety techniques

In this section, we will talk about the most important technologies for the security and protection of the Internet of things, how they work and their uses.

5.2.1. Network security

The biggest challenge in the world of the Internet of things is securing networks due to their vulnerability to problems and because of the intricacy associated with them, the diversity of protocols used and standards of wired and wireless communication.

5.2.2. Authentication

Managing multiple users for a single device requires authentication, static passwords are not of the required security level and may be vulnerable to spoofing. Therefore, we need an authentication that gives strength to protection from infringements, such as digital certificates, two-factor authentication, and also biometrics. And do not forget to mention that the approval is mostly dependent on (M2M) away from human intervention[2].

5.2.3. Encryption

Due to the need to preserve data integrity and prevent hackers from intruding, we need here to use standard encryption algorithms and protocols, in addition to strong management of encryption keys, because in the case of poor management, this may reduce the overall safety of IoT devices[2].

5.2.4. Security-side-channel attacks

Indeed, even with sufficient encryption and verification, another danger is conceivable, to be specific, side-channel assaults as in Fig. 6. Such assaults center less around data move and more on how that data is being introduced. Side-channel assaults (SCAs) gather operational attributes—execution time, power shoppers, electromagnetic spread of the plan to recover keys, and deficiency inclusion[25].

5.2.5. Security analytics

When we say analysis, we mean here collecting various data and monitoring them, looking and checking how they work, and submitting reports. If there is any defect or unauthorized activity here, the necessary ultimatum are issued regarding the activity behind the work policy. And with the techniques of big data and artificial intelligence, it provided more models for prediction and detection of suspicious activities. Because of the urgent need for detection of attacks and breaches, the need for more and more various security analysis techniques is increasing[24].

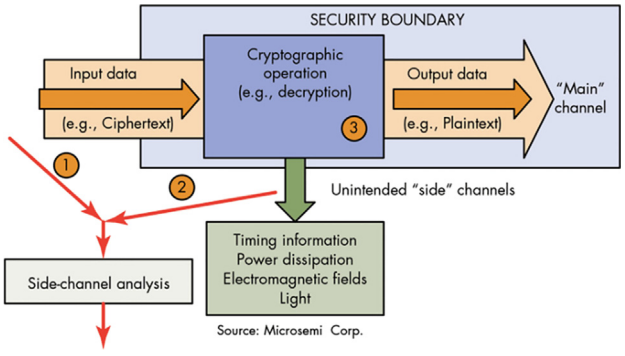

Fig. 6. Security-side-channel attacks . Adapted from [2]

6. Conclusion

This research discusses security and privacy issues in IoT systems and presents its most important applications such as smart home and smart city, and potential risks and threats. We have also detailed the protocols used, the use of each protocol and the work based on it, and mentioned that the threats and security measures needed for defines are every layer of the Internet of Things, in addition to a review of the most important tools used to provide protection and the techniques needed to build a safe environment for the Internet of Things.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H.A. Salam, A. Ahmed, A. Muhammad, The Internet of smart things in the field of health care, J. Acad. Res. (2019).
[2] M. Humayun, M. Niazi, N.Z. Jhanjhi, M. Alshayeb, S. Mahmood, Cybersecurity threats and vulnerabilities: A systematic mapping study, Arab. J. Sci. Eng. 45 (4) (2020) 3171–3189.
[3] M.A. AlZain, B. Soh, E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds, J. Softw. 8 (5) (2013) 1068–1078.
[4] H. Alshambri et al., Cybersecurity attacks on wireless sensor networks in smart cities: an exposition, Int. J. Sci. Technol. Res. 8 (1) (2020).
[5] M. Aazam, et al. PRE-Fog: IoT trace based probabilistic resource estimation at Fog. 2016 13th IEEE Annual Consumer Communications and Networking Conference. CCNC. 2016.
[6] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Computer Netw. 76 (2015) 146–164.
[7] D.K. Alferidah, N.Z. Jhanjhi, A Review on Security and Privacy Issues and Challenges in Internet of Things, Int. J. Computer Sci. Netw. Sec. IJCSNS 20 (4) (2020) 263–286.
[8] B. Atoum. History of Internet of things. 2020; Available from: https://e3arabi.com/.
[9] B. Chu, W. Burnett, J.W. Chung, Z. Bao, Bring on the bodyNET, Nat. News 549 (7672) (2017) 328–330.
[10] P. Sethi, S.R. Sarangi. Internet of Things: Architectures, Protocols, and Applications. 2017.
[11] D.K. Alferidah, N. Jhanjhi. Cybersecurity Impact over Bigdata and IoT Growth. 2020 International Conference on Computational Intelligence (ICCI). Bandar Seri Iskandar, Malaysia. 2020. 103–108. doi: 10.1109/ICCI51257.2020.9247722..
[12] P. Sethi, S.R. Sarangi, Internet of Things: Architectures, Protocols, and Applications, J. Electric. Computer Eng. 2017 (2017) 1–25.
[13] J. Vasseur, et al. The ip routing protocol designed for low power and lossy networks. Internet Protocol for Smart Objects (IPSO) Alliance. 2011.
[14] Q.M. Ashraf, M.H. Habaebi. Autonomic schemes for threat mitigation in Internet of Things. Netw. Comput. Appl. 2015.
[15] K. Uppalapati, How IoT protocols and standards support secure data exchange in the IoT, Ecosystem? (2019).
[16] M.A. Alzain, E. Pardede. Using multi shares for ensuring privacy in database-as-a-service. In: 2011 44th Hawaii International Conference on System Sciences. 2011. IEEE.
[17] B.O. Al-Amri, M.A. AlZain, J. Al-Amri, M. Baz, M. Masud, A comprehensive study of privacy preserving techniques in cloud computing environment, Advanc. Sci. Technol. Eng. Sys. J. 5 (2) (2020) 419–424.
[18] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, E.A. Naeem, M.A. Alzain, J.F. Al-Amri, B. Soh, F.E.A. El-Samie, Investigation of chaotic image encryption in spatial and frft domains for cybersecurity applications, IEEE Access 8 (2020) 42491–42503.
[19] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, M.A. Alzain, J.F. Al-Amri, F.E. A. El-Samie, Efficiently encrypting color images with few details based on rc6 and different operation modes for cybersecurity applications, IEEE Access 8 (2020) 103200–103218.
[20] M.A. AlZain, et al. Managing Multi-Cloud Data Dependability Faults, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019. IGI Global. 207–221.
[21] O.S. Faragallah, M.A. Alzain, H.S. El-Sayed, J.F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, B. Soh, Block-based optical color image encryption based on double random phase encoding, IEEE Access 7 (2019) 4184–4194.
[22] H. Ning, H. Liu. Cyber-physical-social based security architecture for future internet of things. Adv. Internet Things. 2012.
[23] H.E. Samra, B. Soh, M.A. Alzain. A Conceptual Model for an Intelligent Simulation-Based Learning Management System Using a Data Mining Agent in Clinical Skills Education. In: 2016 4th International Conference on Enterprise Systems (ES). 2016. IEEE.
[24] S.K. Arora. What is IoT Security (Internet of Things)? – Tools & Technologies. 2020. Available from: https://hackr.io/blog/what-is-iot-security-technologies.
[25] https://www.electronicdesign.com/industrial-automation/article/21805420/8-critical-iot-security- technologies. 8 Critical IoT Security Technologies. https://www.electronicdesign.com/industrial- automation/article/21805420/8-critical-iot-security-technologies].