Journal of Advanced Research in Instrumentation and Control Engineering
Volume 10, Issue 1 - 2023, Pg. No. 10-16
Peer Reviewed Journal

Review Article

Mobile App Secure Authentication for Unified Software Architecture for Smart Computing IoT Devices

Raman Chadha[1], Naveen[2], Sunil Khullar[3], Vinita Kaushik[4]

Professor, CSE Department, UIE, Chandigarh University, Punjab, India.
Dean IEC School of Engineering, Baddi, Solan.
Professor, CSE, Ludhiana College of Engineering & Technology, Punjab.
Assistant Professor, CSE Department, Maharaja Agrasen University, Baddi, Solan
DOI: https://.doi.org/10.24321/2456.1398.202301

I N F O

Corresponding Author:
Raman Chadha, UIE, Chandigarh University, Punjab, India.
E-mail Id:
dr.ramanchadha@gmail.com
Orcid Id:
https://orcid.org/
How to cite this article:
Chadha R, Naveen, Khullar S et al. Mobile App Secure Authentication for Unified Software Architecture for Smart Computing IoT Devices. *J Adv Res Instru Control Engi* 2023; 10(1): 10-16.

Date of Submission: 2023-04-11
Date of Acceptance: 2023-05-20

A B S T R A C T

IoT devices connect everything to the internet in this century. This allows users to remotely access and operate their equipment. Internet of Things (IoT) gadgets save time, allow remote access to resources, and connect things to the Internet. Since its inception, the Internet of Things (IoT) business has faced many difficulties, most of which involve data security. Only security authentication can establish a dependable system. Confidentiality and integrity are crucial to authentication. The Internet of Things protocols now offers varied degrees of authentication and authorization-based security. As time goes on, security against masquerade attacks, man-in-the-middle attacks, replay attacks, password-guessing Impounder assaults, DoS attacks, and others will require more protection at different stages. Because there are various sorts of system attacks. We used a DHT22 temperature sensor and a Node MCU to analyze security and find a clever solution. We received the data at Mobile via the Internet of Things protocol. We study secure data transfer from the Internet of Things devices to mobile devices. We also highlight our prototype development issues and solutions. We are also working on a prototype that reliably transmits data from Internet of Things devices to the cloud and from the cloud to mobile devices. We also focus on data transmission security from Internet of Things devices to the cloud.

Keywords: IoT, Security, Authentication, Secure Sockets Layer, IoT Devices, Iot Mobile Applications are Some of the Keywords That Should be Considered

Introduction

The Internet of Things (IoT) is a technology that is now evolving at a fast speed, almost all experts in the relevant sectors are of the view that IoT will ultimately be linked with everything, which will lead to a significant spike in demand.[1]

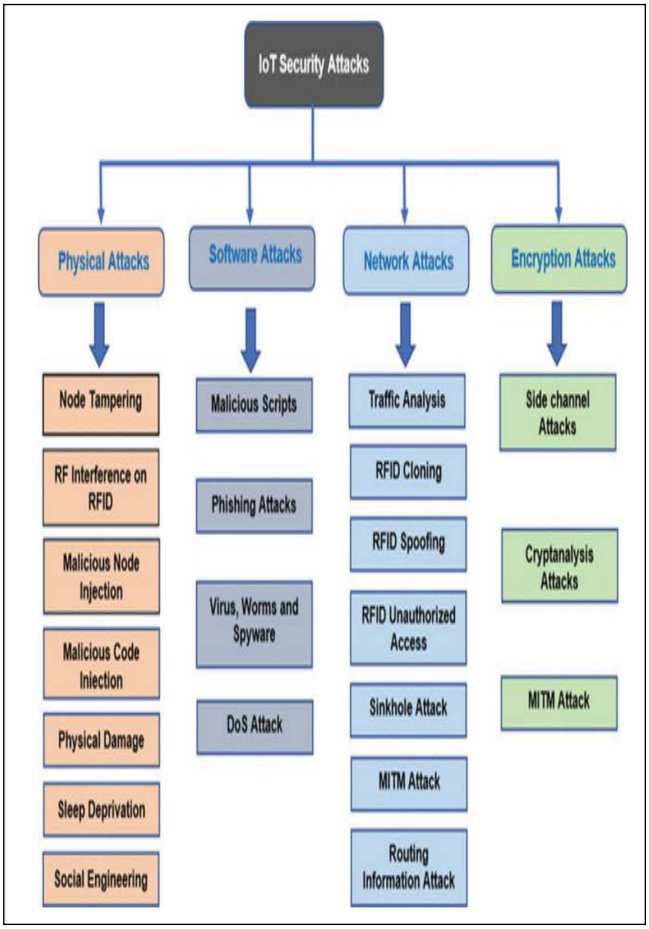

Figure 1.Various security attacks in the IoT system

The Internet of Things (IoT) is used in a number of different applications, each of which has its own individual set of hurdles; taken as a whole, these impediments inspire research into the topic of the IoT. Common applications include "smart cities" and "smart homes," in which residents have the ability to remotely control their home appliances and monitor their property for indicators of an impending break-in. One of the most significant uses of artificial intelligence is in the medical industry, which makes it possible to monitor patients, get real-time information on their health conditions and predictions while working in the field, even make decisions about policy during outbreaks of infectious diseases. The Internet of Things may potentially be beneficial to the emergency services that are provided by the military. In this context, "reaction preparation" may refer to a variety of activities, such as the administration of resources, the remote monitoring of the health and locations of military troops, the administration of resources. Crowd monitoring and traffic management are two additional applications of the Internet of Things. Both of these applications enable intelligent transportation by providing real-time traffic information and optimizing routes. Water management encompasses water quality, leakage, usage, distribution, waste management. The Internet of Things has a wide range of potential applications within the realm of environmental science, some of which include the monitoring of environmental factors such as air pollution, noise, rivers, even industry.[2]

The Internet of Things, often known as IoT, is a picture of the future in which everything is linked to one another and managed by means of intelligent devices; more specifically, we may use IoT technology to exercise control over any item that we choose. Every component that makes up the Internet of Things has to be able to connect to the Internet in order to function properly. As more and more things become linked to the Internet of Things (IoT), people's lives will become not only more convenient but also more efficient, allowing them to spend less time on mundane tasks. In this day and age, if the internet is not functioning properly, then with the assistance of LoRa devices, data may be sent up to 5 kilometers away without the internet.[2] It represents a significant advancement in the capability to link devices from the Internet of Things using LoRa in regions that are remote or inaccessible and do not have an internet connection. It may be difficult for some industries to either specialize in or accept the Internet of Things (IoT) due to the fact that there are now more connected devices than at any other moment in the history of the world. Concerns about the security of devices that are linked to the Internet of Things, data collecting, unwanted access to devices, data hijacking, data manipulation, network penetration, eavesdropping, IoT firmware upgrades, other issues often show themselves as obstacles. In order to find solutions to these issues, a significant number of industry experts have developed novel approaches and implemented significant technological advancements. Over the course of time, devices that are linked to the Internet of Things will also combine with artificial intelligence, which will result in artificial intelligence becoming more powerful and advanced.[26] The Internet of Things is playing an increasingly crucial role in a number of industries, including those in which someone must be physically present in order to control or monitor numerous pieces of equipment. One example of this is the healthcare industry. The most perfect illustration of this would be monitoring machines that are able to exert complete and remote control over the gadgets that are connected to the Internet of Things. The Internet of Things will see an exponential increase in demand, production, consumption over the course of the next several years,[3] as we all eventually make

ISSN: 2456-1398
DOI: https://doi.org/10.24321/2456.1398.202301

the transition from 4G Networks to 5G Networks over the course of time. A boost will be provided to both the technologies that make up the Internet of Things and the industry that helps support those technologies as a result of this new development. Because the hardware industry is now producing high-level AI-based integrated circuits (ICs), it is now much simpler to carry out AI operations, edge-level data processing, data management. This is due to the fact that edge-level data processing can now be done in real-time.

In the future, it's possible that the proliferation of devices linked to the Internet of things (IoT) may make smart cities and smart homes even more appealing and technologically advanced. The absence of technology related to the Internet of Things in the past led a variety of resources to be squandered; nevertheless, the practices of a smart society contribute to the improvement and protection of these resources.[6,7] Not only does the Smart Agriculture system assist in the development of the crops in a manner that is more fruitful, but it also helps the farmer save both time and money in the process. The use of technologies that are associated with the Internet of Things also results in increased profits for a variety of different industries. The vast majority of customers are blissfully unaware of the potential risks associated with the use of these devices; as a result, they are content to continue using them despite the fact that security is the primary concern in every setting in which Internet of Things devices are utilized. This is despite the fact that security is the primary concern in every setting in which Internet of Things devices are utilized. It's very uncommon for companies who create devices for the Internet of Things to fail to establish compliance for their goods in order to protect them in accordance with OWASP standards. This is often the case due to the fact that doing so is an attempt that is not particularly cost-effective. It is of the highest significance to adhere to the standards that have been established and to construct a secure connection in order to eliminate the chance of any data breaches or hacking of these devices. This can be accomplished by preventing any potential vulnerabilities in the system.[5]

The following is an overview of the components that make up the format of the document; these sections may be broken down into the following subsections: In the next section, we will discuss the pertinent work that has been done in the field of Internet of Things security and privacy throughout the course of the previous section. The third portion provides a description of the model that was suggested, the fourth section provides an analysis of the experiments, the final section provides a summary of the study in the form of a conclusion along with some recommendations for the next work that needs to be carried out.

Work Connected to This

Internet of Things

IoT is an abbreviation that stands for "the Internet of Things." Some devices are connected to others, this allows for the devices to be directly connected to the internet and managed remotely from anywhere in the world thanks to the connections that exist between them. The Internet of Things gives rise to a novel kind of network in which all of the devices may be connected to one another and controlled with a fair amount of simplicity. [10]. The Internet of Things makes it possible for gadgets to connect with one another or with other machines in a very seamless way, which is something that is happening even as technology is being accepted by industry and families. This takes place in tandem with the incorporation of several additional technologies that confer smart and intelligent properties onto the gadget.

Impediments to Safety and Security in the Workplace

Fundamental Safety: As a result of the tremendous demand, the vast majority of devices are being deployed with less stringent security, which makes it possible for attacks to take place [9]. Nevertheless, the security of the Internet of Things (IoT) is of utmost significance; if a linear approach is not adopted, not only the integrity of the whole system but also the data's privacy and security are at danger of being breached.

When it comes to the healthcare industry as a whole, the usage of this kind of technology requires a comprehensive degree of security in addition to privacy inside their networks. The extra problems that confront the bulk of the healthcare industry, with the exception of COVID, are connected to privacy. Both the General Data Protection Regulation (GDPR) and the Hazard Analysis and Critical Control Points (HACCP) have been revised as a direct consequence of the proliferation of Internet of Things devices on the market. [10]. and "because there are not enough privacy and security safeguards built into the Internet of Things," it is vulnerable to privacy and security breaches. [11]. According to Turgot et al., (2015), the attacks that have been the most common and well-known over the last few years have been linked to Internet of Things (IoT) devices that have inadequate levels of security. These attacks have occurred over a period of many years. DoS attacks and Man in the Middle attacks are included in these assaults. Devices Data collection, data management, data sharing, data privacy and sharing Concerns about personal privacy and data safety are not exclusive to the healthcare profession; rather, they are relevant to a wide range of other fields as well, all of which include the transmission of confidential information.

ISSN: 2456-1398
DOI: https://doi.org/10.24321/2456.1398.202301

Data Management: There are many industries that use multiple sensor data and equipment, data management that generates billions of data points constantly and in a single day is a huge issue for the industries, as is processing such data and deriving relevant information from such data. There are numerous industries that use multiple sensor data and equipment. It is important to have a thorough comprehension of Extraction, Applied Machine Learning, Deep Learning in order to derive useful information from such data.[25] Data Management: Many different types of businesses nowadays rely on various sensor data and equipment, as well as data management, to produce billions of data points constantly and in a single day. Edge computing is a relatively new technology breakthrough that helps ease many of the challenges and time-consuming processes that are connected with transmitting data that is unneeded or redundant and receiving the result after storing the data and processing it on the cloud. Edge computing is a very recent technological development. IoT-based smart devices are adaptive and give data with their full meaning to the cloud, which enables the cloud to execute fewer computational activities and consume less resources. This difficulty may be circumvented by using IoT-based smart devices.[12,14]

Communication Protocols

Internet connectivity is required for all Internet of Things (IoT) devices to function properly. LoRA devices, on the other hand, have a range of up to 5 kilometers without incurring any loss of packets in transmission, in contrast to Internet of Things devices, which are unable to operate unless they are linked to the Internet.

Internet of Things security in comparison to more traditional information technology security

Internet of Things (IoT) and traditional wireless networks in terms of how they deal with concerns of privacy and security. As Frustaci, Pace, Aloi, Fortino (2018) point out, Internet of Things devices have a high risk of being compromised via WiFi. In addition, the number of assaults that have been carried out against Internet of Things devices has been rapidly increasing over the last three to four years. Authentication issues, management issues, information storage issues, a whole host of other issues lie at the heart of this predicament, which has resulted in this position.

Concerns Regarding the Security of IoT

The Internet of Things (IoT) is fraught with a number of challenges, the most widespread of which is Devices are only susceptible to attacks like node capture when they are exposed to the elements, such as when they are left out in the open. One kind of attack involves inserting malicious code into the memory of the node. Malicious code injection attacks are the name given to these kinds of assaults. Interference and eavesdropping are two common kinds of assault that are committed often. Monitoring the target in order to sneak up on it later and launch an assault is one of the most common attack strategies. Jamming is the practice of interfering with communication by interrupting signals in an effort to gain an advantage. This assault is quite similar to a denial of service attack, in which the adversaries keep the server busy by flooding it with traffic in order to increase the load on the individual machines that comprise the cloud. Attacks Using SQL Injection The target of this assault is the database, the attacker's objective is to either get access to it or directly access it. Man-in-the-Eavesdropping is extremely similar to a technique known as a middle attack, which involves penetrating a network, continuous monitoring, listening in on conversations in order to gather information. One of the most urgent problems in IoT applications is the theft of data; occasionally, sensitive data requires a greater security level, whether the data is at rest or in transit.[21] Malicious codes, like as viruses and worms, are capable of compromising the system's integrity and propagating themselves over the network. In a nutshell, there are two approaches to combat: one is an aggressive strategy, the other is a passive one. Active assaults can be easily identified, at the application layer, we have the ability to activate them if there is a likelihood that the victim would be subjected to an active assault. It is often more difficult to identify passive assaults. Eavesdropping, on the other hand, is an example of a kind of passive aggression that may be difficult, if not impossible, to resist against. It is one of the most difficult challenges to effectively protect oneself against all of the many kinds of attacks, which might occur in a broad range of different ways. DoS attacks are among the most prevalent kinds of cyberattacks, they consist of making repeated attempts to overload or target a server in an effort to stop it from listening to other users' valid requests.

System Ports

One of the ways to support the level of security at the Transport layer, which is one of the ways to make it safe, is via the use of network ports. This is one of the ways that it can be made secure. SSL must be used with a key size of at least 128 bits,[8] which is a requirement if encrypted communications are to be successfully transferred from one encrypted tunnel to another. It is impossible to emphasize the relevance of this mechanism in terms of securing the secure transfer of data, despite the fact that the Internet of Things protocol employs a range of ports for secure communication. When interacting with online applications, web browsers will almost always go with HTTPS; the same is true for communication that is based on the Internet of Things. Both in terms of its capacity for communication and

ISSN: 2456-1398
DOI: https://doi.org/10.24321/2456.1398.202301

its level of security, the MQTTS protocol is an improvement over its predecessor, the MQTT protocol.

Because of the increasing proliferation of smart gadgets in every environment, concerns about security and privacy are always growing. Earlier versions of WSN favored lightweight encryption due to concerns about power consumption. This kind of encryption is less secure for communication, in the event that data is important, the outcome might have disastrous effects. Battery usage and battery backup of devices are both becoming much better as a result of improvements made to technologies such as IoT devices. These improvements are made possible by the adoption of more recent technology and a variety of new strategies. According to the findings of our study, we need a robust authentication system in order to transport data from one device to another end. In the model that we have developed, the data are transmitted directly from the devices to the cloud, subsequently from the cloud to the mobile device, without the need for any specialized platform or application.

Proposed Model

Applications based on the Internet of Things are very quick and simple to use. This study presents a paradigm that we have presented, in which we combine Internet of Things devices with mobile and employ temperature monitoring-based apps to measure parameters using mobile. Directly connecting Internet of Things (IoT) devices with mobile applications eliminate the need for an Internet platform. Just certain settings were added, then we linked it remotely. Our very own server, which reliably answers in a Pub/Sub fashion, has been put up by us. Users have the ability to switch subjects at any moment and remotely adjust the device setup. We demonstrate for you in the figures how users may take use of this service and get a great deal of profit from the application, which is now in the testing phase. The vast majority of apps that are used nowadays are web-based, here we will launch with all of the required capabilities to ensure that people can simply access our product.

Hardware

In order to put this into action, we are using an ESP8266 (microcontroller) and a DHT22 (Temperature sensor). The DHT22 is the most common instrument for detecting temperature and humidity, its precision is noticeably superior to that of other instruments. For the purpose of better understanding the communication and security of Internet of Things applications, we have produced prototypes for this application. In order for the preceding component to function correctly, we have established suitable connections and uploaded our algorithm, which is the means by which it communicates with our server.

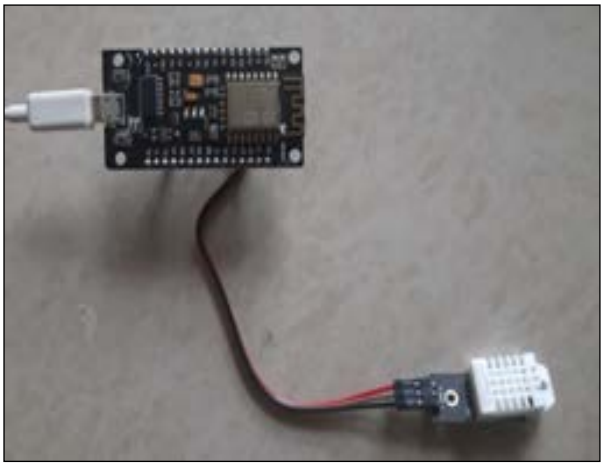

Figure 2.Prototype of IoT device

Software

We have developed a mobile application in the software department that allows us to integrate devices together with all of the characteristics that are required, the devices remain linked with it permanently. There is no need for customers to update their software, the gadget continually transmits data that is easy to monitor and regulate. Within this program, data is kept locally on mobile devices, users have the ability to access that data in an Excel format so that it may be analyzed at a later time. while pub/sub-request handlers are the only ones allowed on the server. With this, we are able to simply connect with any device, data may transfer extremely frequently and without any lag thanks to the MQTT protocol that we are using here. MQTT is one of the greatest and most prominent protocols used in IoT, which stands for the Internet of Things. The Publish/Subscribe protocol is one of the most effective methods available for subscribing to a number of different publishers and subscribers. In the illustration, a mobile application displays real-time data from IoT devices. The green line represents the most recent value, the red line denotes the highest level, the yellow line indicates the lowest level.

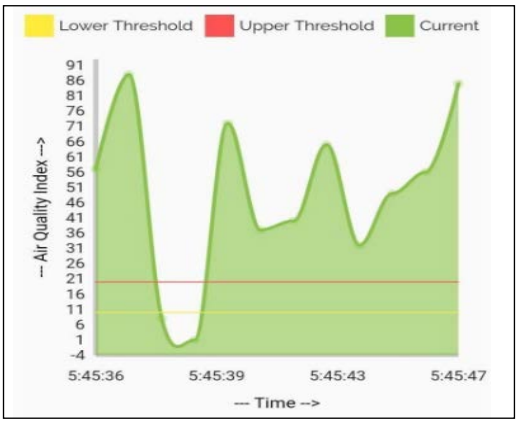

Figure 3.Mobile Application shows Live Temperature

ISSN: 2456-1398
DOI: https://doi.org/10.24321/2456.1398.202301

Experiment Analysis

We are able to control and monitor live data from any location thanks to the Internet of Things. Our primary objective is to provide access to the Internet of Things devices in a manner that is secure, user-friendly, portable. In order to provide consumers with access to our services at this time, we are now testing a prototype that functions correctly in every environment state and scenario. In order to conduct an analysis of experiments, we are making use of DHT22, which is more precise than DHT11. The error rate of the DHT22 is also extremely insignificant for common applications, which makes it suitable for measuring temperatures ranging from very cold to very hot. The DHT22's temperature measuring range is -40 degrees Celsius to 80 degrees Celsius. Using DHT22, we have carried out a number of experiments, based on those experiments, we have determined that data is transmitted in a safe manner, that the level of security identity is high, that the data is highly encrypted, that there is a possibility of a DoS attack, but that a Man in the Middle attack is unlikely. For graphical analysis, we are utilizing Wireshark. If we are not using parameters, then the possibility of attack is very high; however, if we are using parameters, then the level of a security breach is less but with additional parameters such as SSL security and topic name encrypted f the possibility of attack is negligible and the result is shocking. In figure 2, we tested 1000 attempts through a Python script and tested various types of attacks on the proposed IoT devices; the possibility is negligible and the result is shocking.

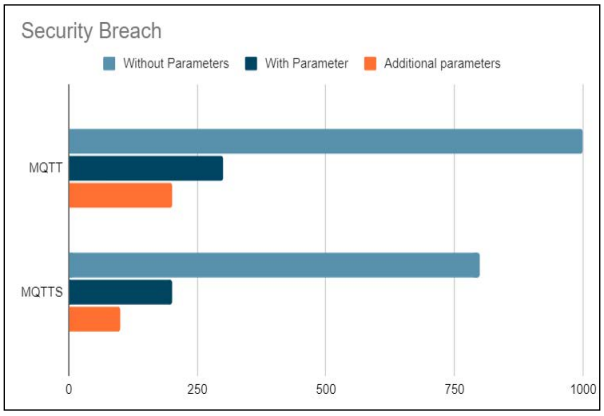

Figure 4.Security breach analysis on IoT devices

Conclusion

The Internet of Things (IoT) domain is one of the most popular domains. It will save time, cut down on losses, enable instant connection from any location in any part of the globe. All of these benefits will contribute to the expansion of the industry. In this work, the study was carried out on the data security of IoT devices, as well as the data security of data propagated to Mobile Apps, for that purpose, we made use of DHT22, which was capable of capturing ambient temperature extremely precisely. We are concentrating on developing easy-to-use and secure Internet of Things devices that can connect to servers and mobile devices. Because this connection provides the most reliable link between mobile and Internet of Things (IoT) devices, we decided to develop a smartphone application to which any device may connect. At the same time, we are coming to the realization that the degree of privacy and security is also quite significant. Therefore, attacks such as man-in-the-middle, denial of service, jamming, tempering are not conceivable. Therefore, in order to integrate all different kinds of devices, protocols, apps, etc., the Internet of Things devices need to have defined standards in the form of standardization. In the future, we want to make use of AI in order to make it simple for users to get early alerts about temperature, we also plan to build a variety of prototypes and platforms in order to ensure that users can make efficient use of the technology.

References

1. Ray, Pratim P. A survey of IoT cloud platforms. *Future Computing and Informatics Journal* 1.1-2 2016; 35-46.
2. Gaitan, Nicoleta Cristina. "A long-distance communication architecture for medical devices based on LoRaWAN protocol." Electronics 10.8 (2021): 940.
3. Shah, Rushabh, Alina Chircu. "IOT and ai in healthcare: A systematic literature review." Issues in Information Systems 19.3 (2018).
4. Samie, Farzad, Lars Bauer, Jörg Henkel. "IoT technologies for embedded computing: A survey." 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS). IEEE, 2016.
5. Lee, Suk Kyu, Mungyu Bae, Hwangnam Kim. "Future of IoT networks: A survey." Applied Sciences 7.10 (2017): 1072.
6. Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.
7. Ishaq, Isam, et al. "IETF standardization in the field of the internet of things (IoT): a survey." Journal of Sensor and Actuator Networks 2.2 (2013): 235-287.
8. Gilchrist, Alasdair. IoT security issues. Walter de Gruyter GmbH & Co KG, 2017.
9. Shah, Sajjad Hussain, Ilyas Yaqoob. "A survey: Internet of Things (IOT) technologies, applications and challenges." 2016 IEEE Smart Energy Grid Engineering (SEGE). IEEE, 2016.
10. Deogirikar, Jyoti, Amarsinh Vidhate. "Security attacks in IoT: A survey." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE, 2017.
11. Schurgot, Mary R., David A. Shinberg, Lloyd G. Greenwald. "Experiments with security and privacy in

ISSN: 2456-1398
DOI: https://doi.org/10.24321/2456.1398.202301

IoT networks." 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE, 2015.
12. Safdar, Noreen, Hala Asif, Fatima Farooq. "Energy Use and Human Health Nexus in Pakistan." Review of Economics and Development Studies 6.3 (2020): 661-674.
13. Gravely, Shannon, et al. "Discussions between health professionals and smokers about nicotine vaping products: Results from the 2016 ITC Four Country Smoking and Vaping Survey." Addiction 114 (2019): 71-85.
14. Abu-Elkheir, Mervat, Mohammad Hayajneh, Najah Abu Ali. "Data management for the internet of things: Design primitives and solution." Sensors 13.11 (2013): 15582-15612.
15. Bohli, Jens-Matthias, et al. SMARTIE project: Secure IoT data management for smart cities. 2015 International Conference on Recent Advances in Internet of Things (RIoT). IEEE, 2015.
16. Zhang, PeiYun, MengChu Zhou, Giancarlo Fortino. "Security and trust issues in fog computing: A survey." Future Generation Computer Systems 88 (2018): 16-27.
17. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, solution architectures." IEEE Access 7 (2019): 82721-82743.
18. Bertino, Elisa, Nayeem Islam. "Botnets and internet of things security." Computer 50.2 (2017): 76-79.
19. Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." Internet of Things 5 (2019): 41-70.
20. Ramotsoela, Daniel, Adnan Abu-Mahfouz, Gerhard Hancke. "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study." Sensors 18.8 (2018): 2491.
21. Abomhara, Mohamed, Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." 2014 international conference on privacy and security in mobile systems (PRISMS). IEEE, 2014.
22. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, solution architectures." IEEE Access 7 (2019): 82721-82743.
23. Cerullo, Gianfranco, et al. "Iot and sensor networks security." Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. Academic Press, 2018. 77-101.
24. Tang, Xiao, Ren P et al. Jamming mitigation via hierarchical security game for iot communications. IEEE Access 2018; 6: 5766-5779.
25. Thakkar, Ankit, Lohiya R. A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, challenges. *Archives of Computational Methods in Engineering* 2021; 28(4): 3211-3243.
26. Lin, Wei Y, Lin YB. AItalk a tutorial to implement AI as IoT devices. IET Networks 2019; 8(3): 195-202.

ISSN: 2456-1398
DOI: https://doi.org/10.24321/2456.1398.202301