Informatics Bulletin, Faculty of Computers and Artificial Intelligence, Helwan University
Published Online ***Vol 3 Issue 2, July 2021***
(https://fcihib.journals.ekb.eg)

A Review on IOT Protocols, Architectures and Security Mechanisms

Ahmed M. Al-Badawy
Computer Science Department,
Faculty of Computers and Artificial Intelligence, Helwan University
Cairo, Egypt.

Mohammed Belal
Prof.,Computer Science Department,
Faculty of Computers and Artificial Intelligences, Helwan University
Cairo, Egypt.

***Abstract*—Nowadays, IOT presents a lot of benefits to people and countries in many fields which in turn makes it one of the most important fields on both research and industry. Recently, NO of IOT connected things has been increased due to rapid network and communication development which in turn leads to increase amount of data exchanged especially critical data. Critical data can be military, industrial, agricultural, health and even personal data which makes IOT networks a main goal for many attacks in order to leak this critical data or even use it in order to cause catastrophic destroy for data owners. A lot of security mechanisms tried to provide a protection for both devices and things but due to devices constrained nature and IOT used protocols, a lot of them failed to provide required protection. In this paper, an introduction to IOT field, its importance and a review for IOT protocols, architectures, a lot of security and privacy challenges and a lot of solutions to that are presented.**

***Index Terms*—** IOT, IOT architectures, IOT Protocols, IOT Security, IOT Privacy, Fog Computing, Edge Computing

I. Introduction

Internet of Things (IOT) is a physical network of things (ex: sensors, actuators, smart phones) which can communicate with each other in order to rapidly exchange data and communicate outside network with servers to process and store huge data. Networks in IOT have many topologies: point to point topology which each node has a direct connection to other nodes, star topology which all nodes are connected to a central point and mesh topology which all nodes can be connected to others [1].
Recently, IOT applications have been increased and invaded a lot of areas and industries [2]. Smart cities industry is one of IOT areas that make use of IOT devices in order to manage traffic, cut pollution, regulate city lights which in turn saves energy consumption and introduces smart parking. Smart agriculture and farming are another areas which regulating all activities related to agricultures such as monitoring green houses, and agricultural lands in terms of water level and temperature, humidity level measurement and automated Irrigation. Manufacturing industry is another IOT area which concerns in automating and regulating process in manufacturing. Health industry is another area that depends mainly on IOT services starting from full monitoring of patients inside and outside hospitals till automated surgeries.

The advances in IOT devices and their platforms in both hardware and software and popularity of them [3] lead to Increase number of connected devices to billions which in turn lead to emergent of many challenges, scalability, availability, synchronization, integration, privacy and security. In this paper, A review on IOT architectures, protocols in terms of security and privacy challenges is presented with a lot of solutions to that challenges.
The rest of this paper is organized as follows: Section 2 gives a review on IOT architectures and protocols. Section 3 presents a lot of IOT security and privacy challenges. Section 4 discuss a lot of methodologies to overcome these security and privacy challenges. Section 5 presents concluding remarks.

II. Literature Review

There are various researches tried to discuss IOT most important areas. Denis and jari [4] tried to review IOT in terms of security and privacy which focuses only issues on the architectural level. Hui and zou [5] tried to focus only on IOT security on architectural level with determining which algorithms needed to provide needed security. Parul and bhisham [6] focuses on IOT architectures in terms of availability, confidentiality, integrity and QOS and addressed a lot of security issues. Minhaj and khaled [7] reviewed IOT in terms of architecture and security issues and categorized issues into low, intermediate and high level security issues with a lot of recommended solutions to these issues. Anne et al [8] focused mainly on security issues on middleware layer with small survey on existing related protocols. Yu Wei et al [9] tried to compare edge computing with traditional cloud systems in order to provide security for IOT systems. Jie Lin et al. [10] tried to focus only on fog computing, issues on it and its relationship with IOT. Although, these papers tried to focus on

some areas IOT but does not give the whole picture for IOT so on this paper, we reviewed all the IOT areas: architectures, Protocols, relationship between architectures and common protocols, security attacks and categorizing them according to architecture layers and defending security mechanism for these attacks which makes this paper a good starting point for any researcher interested in IOT in general and IOT security and privacy specifically.

III. IOT ARCHITECTURES AND PROTOCOLS

A. IOT Common Architectures

IOT as mentioned previously, is a network of devices that works together in order to fulfill the required tasks therefore, it needs flow of work to move data from sensors until reaching storage devices, this flow is called IOT architecture. IOT has different types of architectures [11]:

- Layered architectures consist of a set of layers, each one has a specific task to do in order to fulfill moving data from physical layer to storage devices. One of most common layered architecture is three layer architecture as shown in fig. 1A which consists of
  - *Perception layer* which is responsible for gathering required information from devices.
  - *Network layer* which is responsible for transferring data from physical layer to servers and also connect smart devices to network devices.
  - *Application layer* which is responsible for managing services and applications that users needs for ex: smart home applications.
- Another layered architecture is five layer architecture as shown in fig. 1B which consists of the same three layered architecture and in addition two other layers:
  - *Transport layer* which is responsible for transferring physical layer data to processing layer.
  - *Processing layer* which is responsible for processing and storing data transferred from transport layer, also known as middleware layer.

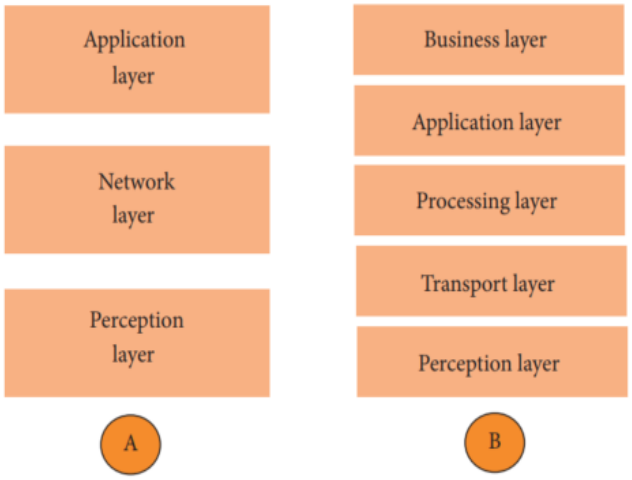

Figure 1: Layered Architectures, A is three layer architecture, B is five tier architecture [11]

- Fog based architecture [12]: is a special type of layered architecture as shown in fig 2, its purpose is to import network and processing capability to IOT network via fog computing. It consists of six layers:
  - *Physical and virtualization layer* which is responsible for gathering data from physical and virtual devices.
  - *Monitoring layer* which is responsible for monitoring devices activities and resources.
  - *Preprocessing layer* which is responsible for data preparation, filtering and trimming which in turn lead sometimes to new data generation.
  - *Temporary storage layer* which is considered fog resources where preprocessed data is stored. Once data is uploaded to cloud, it is removed from temporary storage.
  - *Security layer* which is responsible for providing security solutions to data for ex: encryption/decryption of data, integrity and privacy.
  - *Transport layer* which is responsible for uploading preprocessed and secured data to the cloud.

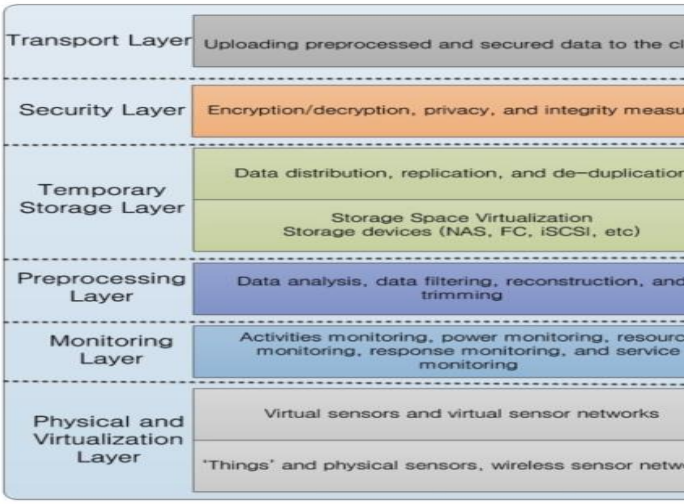

Figure 2: Fog architecture [12]

B. IOT Protocols

IOT devices will be just hardware devices without existence of working protocols that will help these devices to continue required tasks. These protocols [13] must satisfy set of requirements:

- Low power consumption due to devices constrained nature.
- High reliable.
- Provide internet connection.

The following are protocols for generic IOT architecture:

- *Physical layer*: IEEE 802.15.4 is the common protocol for that layer which supports low power devices ex sensors.
- *MAC layer*: IEEE 802.15.4E MAC which is responsible for transmitting frames through physical layer. ZigBee which is a low power, low cost and low bandwidth wireless technology and suitable for IOT application.
- *Convergence layer*: 6LowPan is a low power wireless personal area network which provides sending and receiving over IPV6 packets over IEEE 802.15.4 based networks.
- *Transport layer:* User datagram protocol, IPv6, routing over low power (ROLL), routing protocol for low power (RPL) and datagram transport layer security (DTLS) are common protocols for that layer.
- *Application layer***:** CoAP is document transfer protocol which is used in constrained devices to get value read from devices, MQTT which is an open message protocol used for machine to machine communication in form of publisher subscriber model. AMQP is advanced message queuing protocol which is used for exchanging information between applications.

The protocol stack is shown in fig. 3.

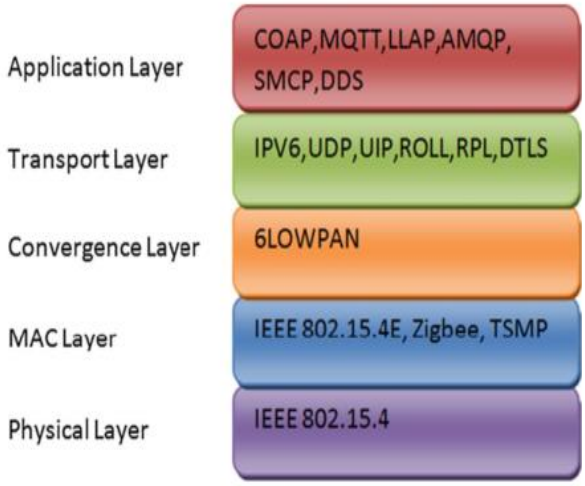

Figure 3: The protocol stack [13]

The below are a comparison between most common IOT used protocols:

TABLE 1
A COMPARISON BETWEEN IOT COMMON PROTOCOLS

Comparison Key	Stands for	Description	Layer	Goal
COAP	Constrained Application Protocol	Is a compressed version of HTTP and designed to be over UDP in order to provide simplicity which is used restricted networks with constrained devices ex IOT in order to transfer data. [14]	Application Layer	Is used to transfer messages with low power in order to save things batteries
MQTT	Message Queuing Telemetry Transport Protocol	Follows publisher/subscriber model which is designed for publishing messages to MQTT broker which clients are registered in order to get these messages. [15]	Application Layer	Is used to transfer messages in low bandwidth and unreliable networks.

IPV6	Internet protocol V6	Is used to give each constrained node IP as IPV4 has limitation on NO of IPs can give versus needed and cannot satisfy these number of nodes plus old connected one. [16]	Transport Layer	Is used to solve limitation of IPV4 by having a big NO of addressed that can satisfy any needs
6LOWPAN	IPV6 over Low power wireless personal area networks	Is built over IEEE 802.15.4 which used to carry data on low bandwidth wireless sensor networks which is considered to be low power which in turn enhance power consumption on devices. [17]	Convergence Layer	Is used to carry out data on IPV6 with low cost and low power consumption
ZigBee	Zonal Intercommunication Global-standard	Is wireless technology which obeys the IOT strict requirements in low power consumption and low cost [18]	MAC Layer	Is used to form device to device communication network with low cost

IV. IOT COMMON SECURITY ATTACKS

As mentioned previously, IOT nearly invaded a large sector of areas and industries which increases exchanging and storing of valuable information which as a consequences, leads to increase NO of security attacks on IOT applications and networks. IOT attacks can be categorized according to IOT layers that can be affected:

- *Physical Layer:*

  - *Node capturing attack [19]:* IOT networks consists of set of nodes connected together in order to exchange information. The attacker can gain control to one node and replace it with another malicious one. This node will appear to be part of system although it is controlled by attacker which in turn leading to information leakage and wrong information exchange.

  - *Malicious code injection [20]***:** attacker tries physically to inject malicious code into existing node in order to control node, stop service or even modify the captured data.

  - *Sleep deprivation attack [21]:* attacker tries to drain the constrained node battery by running infinite loops injected by malicious code which makes it out of service.

  - *False data injection attack [22]:* after the node is captured, the attacker can inject false data into IOT system which will lead to false result which in turn will lead to wrong decisions.

  - *Eavesdropping and interference [23]***:** attacker tries to eavesdrop on both wired and wireless networks in order to leak information or modify sent information which in turn lead to false result in case of modifications.

  - *Side channel attack***:** a lot of side channel attacks can be more dangerous than normal attacks. Attacker makes use of processors power consumption and electromagnetic emersion in order to reveal sensitive information.

  - *Booting attacks*: while booting or restarting node, the security mechanisms are not loaded yet. The attacker makes use of that and tries to attack edge devices which can lead to full control of edge device and disabling security mechanisms from loading.

- *Network Layer:*

  - *Unauthorized access Attack [24]***:** attacker tries to gain access to IOT network in order to leak important information or damage network or modify sent data. The attacker can stay inside network undetected for long period.

  - *Routing attacks***:** as a result of node capturing attack or malicious code injection mentioned previously, the malicious node may try to redirect data to another paths or changes all routing paths by pretending to its neighbors that it has the shortest paths to route. An example of this attack is sinkhole attack [25] which malicious node sends fake routing information to its neighbors in order to get data routed through it.

  - *DDOS or DOS attack [26]:* the attacker tries to submit a large number of requests in order to make server with its service down. This attack can be performed from one source which termed DOS or multiple sources which termed DDOS attack.

- *Data transit attack***:** the main goal of any attacker in IOT is to steal valuable data so attacker tries to steal data while it is being transferred from network to storage devices or cloud.

- *Middleware Layer:*

- *Man in the Middle attack (MITM) [27]***:** IOT uses message queuing protocols as a machine to machine communication such as Message Queue Telemetry Transport (MQTT) [28]. MQTT follows publisher subscriber model in order to provide a communication broker between publishers – sensors- and subscribers. The attacker tries to gain access to this broker in order to control sent messages which in turn helps him/her in controlling all communications which is known as MITM.

- *SQL Injection Attack [29]:* the attacker tries to embed malicious SQL statements in order to obtain sensitive data or destroy it which in turn puts users' privacy in danger.

- *Cloud Malware Injection***:** the attacker tries to inject a virtual machine in cloud which pretends to be a legal service. Therefore, the attacker can gain access to users' requests as being a legal service which enable him to capture all users' sensitive information.

- *Flooding attack in cloud***:** this attack is similar to DDOS or DOS but targets cloud. Attacker tries to drain all cloud resources by continuously submitting requests to specific service which in turn leads to a heavy load on cloud servers to satisfy these requests which can down the service for a period.

- *Application Layer:*

- *Data Theft attack*: IOT depends mainly on exchanging and storing sensitive data which encourages attacker to try more and more in order to steal it which in turn puts users' privacy in danger.

- *Access control attack*: attacker tries to break authorization mechanism in order to gain access to services. This attack is very critical, once the attacker gains access, all IOT application becomes vulnerable to that attack.

- *Service interruption attack*: attacker tries to deprive legal users from using services/applications by making network or servers too busy to respond via continuously dummy requests.

- *Malicious Code Injection*: attacker tries to use cross scripting attacks (XSS) in order to inject malicious code via malicious scripts running. This, in case of successful attack, can lead to fully control IOT system.

- *Reprogramming attacks*: the attacker, in case of services source codes are not protected enough, can reprogram the services to do what is needed to leak all sensitive data and even tamper it.

- *Gateways attacks:*

- *Man in the Middle attack***:** gateways is an intermediate layer between IOT network and Fog/ cloud based on architecture used. Therefore, it is highly susceptible to this attack in order to capture/tamper critical data or encryption keys.

- *Data breaches attack***:** gateways are susceptible to this type of attack as they required to decrypt and re-encrypt data in order to translate from protocol to another.

V. IOT SECURITY METHODOLOGIES

As shown previously, IOT is vulnerable to a lot of attacks that have ability to leak all sensitive data or even destroy the whole IOT network. A lot of security solutions tried hardly to protect users' data and IOT resources but either it totally failed or succeeded in resisting set of targeted attacks:

- *Block-chain***:** it is one of technologies that aims to provide security, privacy and increase level of trust. It consists of replicated log file – also called ledger- which contains set of order time-stamped entries. Each entry is correlated with its previous entry using hash key. Each individual transaction is stored in a tree called merkle tree and the root of the tree is stored in block chain. The root can be continuously verified in order to ensure that the transactions associated with that root are not tampered. Block-chain has two types based on architecture: permissioned-less block-chain which does not require permissions to join/leave it such as bitcoin, permissioned, require users to obey set of rules in case of joining or leaving [30]. IOT sensitive data can be stored on block-chain which will provide it confidentiality and integrity due to its

distributed architecture. Block-chain uses 256-bit has keys for the data to be stored rather than data itself. The data are stored on cloud then while retrieval, can be mapped to hash keys for verification. Block-chain tried to resist spoofing attacks by providing a strong mechanism for devices to identify and authenticate each other which in turn forbid injection of malicious nodes or users. Moreover, block-chain uses public private keys in communication which means no unauthorized access to data as it is encrypted by these keys. Therefore, block-chain provides a basis for IOT in terms of security.

- *Fog Computing*: fog computing is an intermediate layer between IOT devices and cloud. Its main job is to handle IOT data early before sending them to cloud in order to take rapid decisions as shown in fig. 4. Fog computing has two types: fog device architecture which responsible for both storing and processing data no need for cloud while fog-cloud device which fog is responsible on for processing and taking simple decisions while storage will be in cloud as well as complex decisions [31]. As being secured intermediate layer, all requests must pass through it which in turn overcome a lot of attacks, man in the middle, data transit, and eavesdropping attack by securing communication channels and tries to protect edge devices from compromising in order not to be a weak entry point for system. Moreover, it provides ways of revealing suspicious data or requests which overcome DDOS/DOS attack in order not to take wrong decisions.

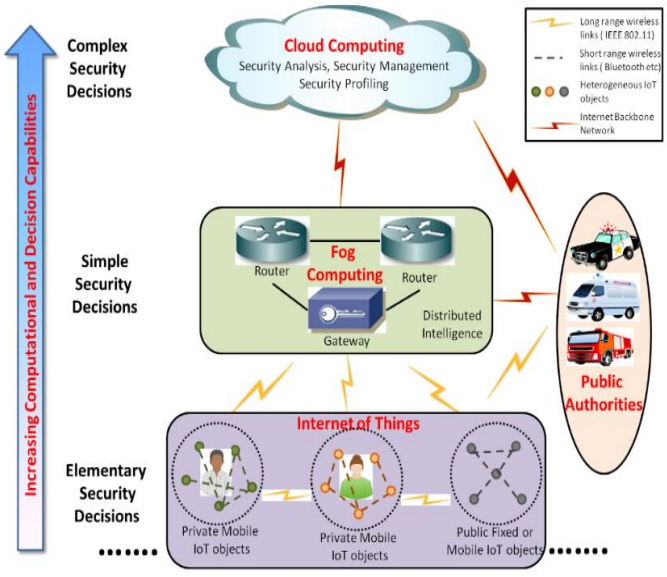

Figure 4: Fog computing architecture [31]

- *Edge Computing [32]:* is considered as an extension to cloud computing capability. The edge node is a small server which is deployed on IOT network in order to take rapid decisions instead of consulting cloud. Edge nodes must be deployed closely to IOT devices in order to provide fast response time and minimize bandwidth usage [33] as shown in fig. 5. Edge computing tries to overcome a lot of security attacks by moving processing of critical data into edge nodes instead of cloud which in turn provide data privacy and minimize data being on transit which eliminating risks of data theft and breaches. Moreover, edge nodes tries to secure all its communications with gateways in order to overcome man in the middle attacks, data transit attack and tampering attack.

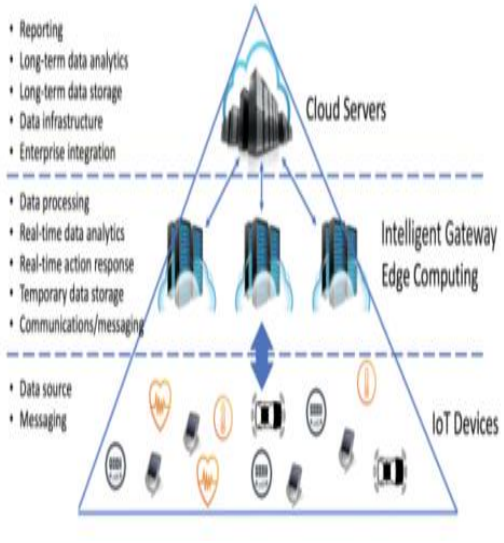

Figure 5: Edge Computing Layered architecture based IOT [32]

The following are comparison between three mechanisms in order to show similarities and differences:

TABLE 2
A COMPARISON BETWEEN IOT COMMON SECURITY MECHANISMS

Comparison Key	Fog Computing	Edge Computing	Blockchain
Description	Extend IOT network capability by carrying out computation tasks and decisions that would be normally carried out on cloud and provide security mechanisms for IOT networks	The same fog purpose	Provide security mechanisms for the IOT network by making use of blockchain features such as decentralization, consensus mechanism, data encryption, and smart contracts
Integration With IOT	Outside network devices themselves on LAN [34]	Inside network devices themselves which can be attached to sensors direct or gateway [35]	Any layer of IOT paradigm such as cloud or edge. [36]
Architecture	Added as a new layer between physical and network layer [37]	The same as fog [37]	A digital ledger that can be used to maintain continuously growing data in a secure way [38].
Common Security Threats to Overcome	Man in the Middle Attack, Data transient Attack, Eavesdropping	Data Breaches, Safety issues due to being inside network, Bandwidth issues	Mutual Authentication, data breaches, authorization, access control , malicious injection

VI. CONCLUDING REMARKS

In this survey, an entry point for IOT and its security challenges are presented. IOT is considered present and future technology for nearly all industrial, agricultural, medical fields and even for people and their life. With the advances in IOT technology and increasing number of connected devices led to increase in sharing critical information which made IOT networks and their data main goal for many attackers. Therefore:

- Currently IOT architecture must be well revised and weak architecture in terms of security must be excluded.
- Currently IOT protocols must be revised and enhanced in terms of both performance, security and power consumption.
- Currently, fog devices are considered to be backbone of IOT networks, therefore, all attacks especially long term attacks on these devices must be solved for safety of critical information.
- All other attacks, especially attacks that targets IOT nodes (edges and things) as being constrained devices must be solved.

By following robust architecture and protocols in IOT and applying powerful security and privacy mechanisms, IOT will be future technology for the whole world.

VII. REFERENCES

[1] Yaqoob, Ibrar, et al. "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges." *IEEE wireless communications* 24.3 (2017): 10-16.

[2] Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." *Wireless personal communications* 58.1 (2011): 49-69.

[3] Dean, Andrew, and Michael Opoku Agyeman. "A study of the advances in iot security." *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*. 2018.

[4] Kozlov, Denis, Jari Veijalainen, and Yasir Ali. "Security and privacy threats in IoT architectures." BODYNETS. 2012.

[5] Suo, Hui, et al. "Security in the internet of things: a review." 2012 international conference on computer science and electronics engineering. Vol. 3. IEEE, 2012.

[6] Datta, Parul, and Bhisham Sharma. "A survey on IoT architectures, protocols, security and smart city based applications." 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2017.

[7] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[8] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, ‘‘IoT Middleware: A survey on issues and enabling technologies,’’ IEEE Internet Things J., vol. 4, no. 1, pp. 1–20, Feb. 2017

[9] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, ‘‘A survey on the edge computing for the Internet of Things,’’ IEEE Access, vol. 6, pp. 6900–6919, 2018.
[10] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ‘‘A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,’’ IEEE Internet Things J., vol. 4, no. 5

[11] Sethi, Pallavi, and Smruti R. Sarangi. "Internet of things: architectures, protocols, and applications." Journal of Electrical and Computer Engineering 2017 (2017).

[12] Aazam, Mohammad, and Eui-Nam Huh. "Fog computing and smart gateway based communication for cloud of things." 2014 International Conference on Future Internet of Things and Cloud. IEEE, 2014.

[13] Sobin, C. C. "A survey on architecture, protocols and challenges in iot." Wireless Personal Communications 112.3 (2020): 1383-1429.

[14] Halabi, Dana, Salam Hamdan, and Sufyan Almajali. "Enhance the security in smart home applications based on IOT-CoAP protocol." 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC). IEEE, 2018.

[15] Yassein, Muneer Bani, et al. "Internet of Things: Survey and open issues of MQTT protocol." 2017 international conference on engineering & MIS (ICEMIS). IEEE, 2017.

[16] Lamaazi, Hanane, et al. "Challenges of the internet of things: IPv6 and network management." 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. IEEE, 2014. [25] Tahir, S., Bakhsh, S. T., Abulkhair, M., & Alassafi, M. O. (2019). An energy-efficient fog-to-cloud Internet of Medical Things architecture.International Journal of Distributed SensorNetworks, 15(5), 155014771985197

[17] Yeole, Anjali, D. R. Kalbande, and Avinash Sharma. "Security of 6LoWPAN IoT networks in hospitals for medical data exchange." Procedia Computer Science 152 (2019): 212-221.

[18] Froiz-Míguez, Iván, et al. "Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes." Sensors 18.8 (2018): 2660.

[19] Kumar, Sudeendra, et al. "Security enhancements to system on chip devices for IoT perception layer." 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS). IEEE, 2017.

[20] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Applications (0975 8887), Volume 111 - No. 7, February 2015

[21] Vashi, Shivangi, et al. "Internet of Things (IoT): A vision, architectural elements, and security issues." 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

[22] Bostami, Biozid, Mohiuddin Ahmed, and Salimur Choudhury. "False data injection attacks in internet of things." Performability in Internet of Things. Springer, Cham, 2019. 47-58.

[23] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, ‘‘Eavesdropping prevention for heterogeneous Internet of Things systems,’’ in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018, pp. 1–2.

[24] Naik, Swapnil, and Vikas Maral. "Cyber security—IoT." 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, 2017.

[25] Md. I. Abdullah,M. M. Rahman and M. C. Roy, “Detecting SinkholeAttacks in Wireless Sensor Network using Hop Count” I. J. Computer Network and Information Security, pp.50-56, 2015.

[26] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ‘‘DDoS in the IoT: Mirai and other Botnets,’’ Computer, vol. 50, no. 7, pp. 80–84, 2017.

[27] Cekerevac, Zoran, et al. "Internet of things and the man-in-the-middle attacks–security and economic risks." MEST Journal 5.2 (2017): 15-25.

[28] Dinculeană, Dan, and Xiaochun Cheng. "Vulnerabilities and limitations of MQTT protocol used between IoT devices." Applied Sciences 9.5 (2019): 848.

[29] Tweneboah-Koduah, Samuel, Knud Erik Skouby, and Reza Tadayoni. "Cyber security threats to IoT applications and service domains." Wireless Personal Communications 95.1 (2017): 169-185.

[30] Henry, Ryan, Amir Herzberg, and Aniket Kate. "Blockchain access privacy: Challenges and directions." IEEE Security & Privacy 16.4 (2018): 38-45.
[31] V. K. Sehgal, A. Patrick, A. Soni, and L. Rajput, ‘‘Smart human security framework using Internet of Things, cloud and fog computing,’’ in Intelligent Distributed Computing. Springer, 2015, pp. 251–263.

[32] Yu, Wei, et al. "A survey on the edge computing for the Internet of Things." IEEE access 6 (2017): 6900-6919.

[33] E. Oyekanlu, C. Nelatury, A. O. Fatade, O. Alaba, and O. Abass, ‘‘Edge computing for industrial IoT and the smart grid: Channel capacity for M2M communication over the power line,’’ in Proc. IEEE 3rdInt. Conf. Electro-Technol. Nat. Develop. (NIGERCON), Nov. 2017, pp. 1–11

[34] Desai, Shivani, Tarjni Vyas, and Vishakha Jambekar. "Security and privacy issues in fog computing for healthcare 4.0." Fog Computing for Healthcare 4.0 Environments. Springer, Cham, 2021. 291-314.

[35] Alwarafy, Abdulmalik, et al. "A survey on security and privacy issues in edge computing-assisted internet of things." IEEE Internet of Things Journal (2020).

[36] Al Sadawi, Alia, Mohamed S. Hassan, and Malick Ndiaye. "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges." IEEE Access 9 (2021): 54478-54497.

[37] Tahir, S., Bakhsh, S. T., Abulkhair, M., & Alassafi, M. O. (2019). An energy-efficient fog-to-cloud Internet of Medical Things architecture.International Journal of Distributed SensorNetworks, 15(5), 155014771985197

[38] Singh, Saurabh, ASM Sanwar Hosen, and Byungun Yoon. "Blockchain security attacks, challenges, and solutions for the future distributed iot network." IEEE Access 9 (2021): 13938-13959.