QOSS IN 5G NETWORK FOR IOT SOLUTIONS USING CLOUD – A SURVEY

Nasreen Sultana Quadri
Department of Computer Science and Information, JJT University, Jhunjhunu, India
Zulfi
Department of Computer Science and Information Majmaah University, KSA
n.quadri@mu.edu.sa
Tasneem Mustafa Ghnaimat,
Department of Computer Information Systems
University of Jordan, Amman, Jordan
ghnaimat.tasneem@gmail.com
Kusum Yadav,
Department of Computer Science University of Hail , Hail, KSA
kusumasyadav0@gmail.com

ABSTRACT*— The Internet of Things (IoT) is the new technology which is being adopted and used to revolutionize the way the globe can be connected through seamless connection and through the use of smart and heterogeneous devices that are interrelated. The applications of the Internet of Things have immense potential of transforming the daily lives of people and the activities that are often carried. The future of the applications that rely on the Internet of Things is dependent on the strength of the network connecting devices to each other; therefore the security will be main criteria as millions of devices are interconnected. In this paper we will create an understanding of the 5G network, the limitations of the current cellular networks when they are applied in the development of the Internet of Things applications, also discuss Quality of Security Services (QoSS) like authentication, confidentiality, integrity, and availability using AWS firewall.*

Keywords— *QoSS (Quality of Security Services), Internet of Things, 5G Network, AWS (Amazon Web Services), Web Application Firewall*

I. INTRODUCTION

The applications that have been developed using the Internet of Things technology rely on devices that use low power and those that base their interaction through the internet. This means that the developers of the systems which use the Internet of Things use the internet as the network of communication and also target the devices [1]. Since the concept of the Internet of Things was introduced, a lot of attention has been drawn to the idea. The researchers in this field are working towards ensuring that sensors, wearables, smart devices, tablets, smartphones, transportation systems that are smart and other entities are connected to an interface that is common and will offer the systems with the ability to communicate with each other.

Through the Internet of Things applications, objects or things can be connected with one another; the interactions are through wired and wireless networks which allow them to create new services that will help the development of the community [3].

Through the Internet of Things, the benefits that are presented to the society can be said to be limitless; the technology has the potential to radically impose a change on how human beings run our daily lives. Through the provisions of saving time, sustainably utilizing resources and also fostering innovation and growth, the lives of individuals throughout the world can be changed.

The Internet of Things applications need to communicate with each other; this means that there has to be a way of communication between the heterogeneous devices and applications without any intervention of human beings. To achieve this, there is a need to use a seamless network or communication systems. Such a network will enable heterogeneous devices to work correctly and also offer results that are reliable when being used in systems that are critical or massive. Ericsson predicts that more than 28 billion devices will be connected to the Internet of Things across the world by the year 2021; 15 billion of these devices will be consumer electronics devices [4]. Further studies have indicated that 7 billion of these devices will be connected using the cellular network technologies which include; 2G, 3G, 4G.

These mobile technologies currently being used but have not been fully optimized for the low power wide area technology and the Internet of Things applications [5]. It is for this reason that the 5th generation wireless systems need to be integrated and used with the Internet of Things various devices. This cellular network technology system will be able to offer connections that are seamless and also connect more devices as it is more advanced.

As the communication happens between heterogenic devices the need for QoSS is very important to secure IoT devices from certain Malware attacks. Providing security for a different platform, network, and communication, as the IoT with 5G network require different operations we require a cloud-based Firewall which can operate on all these utilities. Amazon web service provides firewall protection with WAF firewall which can block/unblock different data packets and flow of information for secure communication. The sectors that will benefit from the implementation of the 5G network on the development of the Internet of Things applications including; automotive industry, entertainment industry, manufacturing industry, agricultural industry, and information technology sector [14].

Many solutions that implement the Internet of Things applications currently use the 4G network, however, it can be noted that the 4G cellular networks have reportedly many issues which might make the future Internet of Things applications become inefficient or limit the innovations that may be used for the Internet of Things. The paper is organized as follows: in the following section 5G network features are introduced, followed by section talking about 5G network usages in IoT applications, then QoSS for 5G network using Amazon cloud is given.

Literature review of cellular networks are introduced in section2, then the security issue for IoT applications is given in section 3, and finally, we provide an implementation of QoSS for 5G network using AWS WAF.

II. OVERVIEW

A. 5G Network

Fifth Generation (5G) wireless system is a wireless network that is improved, and that is said to offer speed performance of more than 20 gigabytes per second [1].

The 5G network is also supposed to have an ability to deliver more data to different users in a faster speed simultaneously. The network will have a reduced latency which will ensure that there is a seamless connection between two devices that are communicating in a network. In 5G mobile communications networks will improve data transfer speed, scalability, connectivity, and energy efficiency.

The 5G will be able to provide connection massive IoT, where billions of smart devices can be connected into the Internet. 5G networks will provide flexible and faster networks. The 5G can make significant contributions on the future of IoT by connecting billions of smart devices to create actual massive IoT, in which smart devices mutually interacting and sharing data without any human assistance [2].

B. 5G and the Internet of Things

In the recent past, the use of mobiles in communication and accessing the internet has increasingly become an integral part of the lives of people. There has also been a steady increase in the way people use these devices for communication. It is, for this reason, the need for a new network system has become a necessity, a proper network that will ensure that people have an efficient connection and also has the ability to support the new advanced technologies that are being rolled out. The concept of the internet of things and its development has made it necessary for the quantitative assessments of the estimates between the client base communications to be revised. A new network, 5G in this case, needs to be used so that it can support the increasing number of devices that are being used to offer the Internet of Things Solutions. A reliable network will ensure that important requirements are satisfied; there will be a high degree of reliability, the quality of data being transmitted will be higher and the speed of transmission will be better [2].

By using the 5G network in the Internet of Things applications, it will be possible for the implementation of a D2D communication model for the Internet of Things applications. The use of D2D communication will allow mobile devices to communicate with each other without their communication passing through the base station [5]. Communication that passes through a base station is efficient for data that needs low efficiency such as calls and short messages. In modern devices, high data rate services are used; this means that the base station communication will make the communication inefficient. It is for this reason that the 5G network becomes a necessity when developing the new Internet of Things applications.

A stronger connection such as that presented by the 5G technology can be able to make the devices in the system operating efficiency. The faster speeds that are provided by the 5G network will revolutionize the way the Internet of Things applications are developed and used. Current cellular networks such as the 4G network produce extensive data which needs to be processed; it takes more time in conducting the processes of this solution so that the use of the 5G network will provide a solution for the latency problem [3]. Companies processing such information will be able to use many devices and massive data without the fear of overcrowding which will lead to the lack of efficiency.

There is a projected potential increase in the demand of the users of the Internet of Things applications. This means that the 4G technology has to be replaced by the 5G connection technology that is known as Beam Division Multiple Access (BDMA) and Non- and quasi-orthogonal or Filter Bank multicarrier (FBMC) multiple access [4].

According to statistics, the new 5G systems will be able to handle data up to 1000 times more as compared to current systems. The technology will be used in the development of the Internet of things because of such capabilities [5]. For instance, self-driving autonomous cars will be able to be developed and other vending machines like [4]. The use of such technology will provide a new experience and also signify the start of the technological and economic revolution.

The Internet of Things applications are being developed around various sensors. In years to come, the systems are said to have more activities and also the devices that use the technology are also meant to grow [4]. The sensor systems will be able to allow different systems to communicate with each other. The 5G network and the Internet of Things applications are seen as the future basis of the technology paradigm [6].

Through the 5G network, the systems and solutions that are developed for the Internet of Things will be able to be more efficient and effective. The 5G network will enable the Internet of Things applications to have faster speeds as compared to the current rates; there will be a lowered latency as compared to the high latency that is experienced with the network that is currently being used for applications. There will be network support for the increased and massive data traffic that the applications use to process data and interact with each other.

Virtual and augmented reality can be able to use the speed that is provided as they need to interact immediately. 5G network will also enable predictions of connectivity.

From this, it can be noted that the current cellular network that is being used does not efficiently support the applications or solutions that are provided by the Internet of Things. The current technology will also not be able to support the future innovations of the Internet of Things applications. To ensure that the current issues are solved and that the efficiency of the Internet of Things applications is increased, there is a need to use a stronger and faster network.

In this case, the implementation of the 5G network will be able to solve the problems that are currently experienced. It will also help in the development of the future Internet of Things applications.

C. QoSS for 5G using Amazon Cloud

The latest innovation in 5G network in terms of architecture and technology require Quality of Security services. QoSS include Confidentiality Authentication, Availability, and Integrity. In section 5 detail descriptions of these services are explained.

III. LITERATURE REVIEW FOR EXISTING CELLULAR NETWORKS AND SECURITY IN CLOUDS

A. Overview of Existing cellular networks

Over the past, researchers and technology companies have been developing networks systems through which devices have been communicating with each. There has been an

evolution of the cellular networks from 1G and now we are headed to 5G. The 1G network's standards were developed in the 1980s and they use radio signals that are analog, they cannot be able to allow seamless communication between devices. The 2G network system standards were developed in the 1990s and they used signaling and data confidentiality with the use of authentication from the mobile base station [7]. The communication using these systems was quite slow and could not effectively connect the devices for the internet of things applications. The 3G network was commercially commissioned in 2001 and it was designed to ensure that there is support for high data capacity and that there is greater voice support.

4G is the existing cellular network and was recently commissioned commercially. The network is an improvement from the 3G cellular network system, the system has been used widely in the applications of the Internet of Things, and there has been a continuous evolution of this network to meet the future needs of the applications of the Internet of Things [6]. However, with the use of this connectivity, the Internet of things applications still faces some challenges.

The challenges that are faced include; security challenges, a large number of connected nodes and also the new standards that are being developed. This means that there is a need for a new connection network to be established.

Shortly, the 4G technology will not be able to meet the needs of the Internet of Things applications [6]. For instance, it will be hard for 4G to support the low latency that will be needed for the self-driving autonomous cars.

The existing cellular networks do not have the speeds and the network capacity that is required to ensure that the network communication of the devices using the Internet of Things are efficient and that they support the future innovations. There are different kinds of delays that are incurred when data is being processed over some network. 2G, 3G, and 4G networks have high latency levels which mean that they cannot be able to support the current capacity of data that needs to be processed over the internet.

The latency of data that is communicated in different networks has been analyzed over the past. In the 2G network, the data rate is between 100 and 400 Kbps, its latency is said to be 300 – 1000ms, and this is the highest latency levels recorded. The 3G network has data speeds of 0.5 – 5 Mbps, its latency is recorded to be between 100 – 500ms. The 4G network is one of the most used networks in the development of the Internet of Things solutions. Its speed is said to be 1-50 Mbps with latency time being less than 100ms [8]. Advancements are being made to reduce the latency time of the network which is being experienced with the current networks.

B. Security Challenges and solutions in clouds

Security goals can be classified as outside security and inside security; inside security includes confidentiality by making data accessible by only authentic users, this data should be authentic to ensure integrity, and should be available to users when needed.

Outside security includes query processing, access control and large scale anti-jamming services [15].

Cloud computing provides an efficient way for users to maintain data, services, and applications where multiple services can be employed to achieve a higher level of reliability and availability.

Low latency levels are required in order to be able to support the Internet of things applications that need high-speed network, such applications are autonomous cars, connected homes, moving robots, and sensors.

5G network will be used to interconnect critical devices and data which require more security to ensure privacy and safety. For example, a security violation in the online power supply systems or any other critical systems can be disastrous for all systems that depend on.

Since cloud computing systems consist of different resources that are shared between users, it is possible that users will make hurtful traffic which will decrease the performance of the system, and use more resources or access resource of other users of the system [12].

Actually, shared environments are vulnerable to violating privacy where data is stored in the same infrastructure, also there is no control over the data stored in cloud resources.

One of the security challenges is Denial of Service (DoS) attacks on the infrastructure; where the nature of network control elements is visible, and unencrypted control channels.

The use of networking in the Internet of things imposes the challenge of flash network traffic, where there will be a high number of resources which include devices and other things [12].

Another challenge is the need to have proper communication channels security in order to prevent possible threats and to maintain centralized policy management and global network visibility. [13]

The IPsec protocol can be used in the case of securing 5G communication channels as mentioned in [14].

Those security mechanisms have high overhead and consumption of resources as well as lack of coordination; therefore, there is a need to use physical layer security by using Radio-Frequency fingerprinting, symmetric security schemes and changing security parameters dynamically [12].

Using clouds to store data means that there should be a strong ability to store and process sensitive and critical data, as the cloud will be public. Moreover, the use of 5G networking will require better techniques for access control, transparency, availability, and transparency.

IV. SECURITY FOR DIFFERENT IOT APPLICATIONS AND CLOUD COMPUTING

The systems and applications of the Internet of Things systems have immense potential of transforming the daily lives of people and the activities that are often carried. Through the Internet of Things applications, objects or things can be connected with one another; the interactions are through wired and wireless networks which allow them to create new services that will help the development of the community [5].

The Internet of Things applications need to communicate with each other; this means that there has to be a trusted way of communication between the heterogeneous devices and applications without any intervention of human beings. Trusted network means that all communications should not be attacked by unauthorized access; this also means that these communications should have a high quality of services regarding the security of data and processes done [9].

All IoT applications can benefit from the Cloud capabilities and resources to reimburse its technological constraints, for example, storage, processing, and energy. The cloud acts as an intermediate layer between the nodes and the applications.

While the number of connected devices increased, more data is required. To store a large amount of data, more space, and more processing is required. More processing and computation are only possible with cloud computing.

Cloud computing gives an effective solution to implement IoT service management. The cloud can support an actual solution to implement IoT service management as well as applications that make use of things or data formed by them. Also, the Cloud can benefit from IoT by distributing its opportunity to deal with real things in a more distributed manner, and for having more facilities in a large number of real situations. Cloud computing and IoT is working in integration makes better orientation [16].

V. IMPLEMENTATION OF QOSS FOR 5G NETWORK USING AWS WAF

As 5G is mainly revolutionizing due to drastically evolution in IoT devices providing a secure communication is an important criterion. We introduced some of QoSS for making a secure communication for IoT applications [10].

A. Authentication:

User authentication is very important in 5G network devices in terms of message and entity to ensure that both ends are authenticated before communication as shown in figure (a). Using WAF Rules and conditions different conditions and rules can be provided for message and entity authentication.

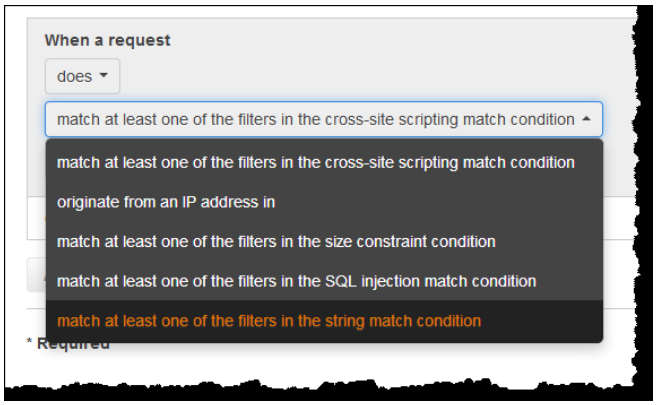

Fig-a Authentication Request

B. Confidentiality:

Confidentiality for network communication devices in terms of data security and privacy. Data security in terms of data security and privacy to protect the flow of traffic from attackers using geolocation.

C. Availability:

It is one of the important services in 5G network so providing security at this point is crucial, at the same time we need to check whether the user is legitimate or not. This service can be implemented using a filtering scheme in WAF condition.

D. Integrity:

It is another important criteria in a 5G communication device to check that the flow of information between two parties is protected against eavesdropping when a packet request arrived we can block/unblock to check whether the request is from a legitimate user or not using AWS cloud. If the flow of packets is more we can reduce the traffic using filtering policies [11].

VI. CONCLUSION:

In a few years, the use of cellular networks in the design and development of the Internet of things applications have been implemented.

5G networks will have increased support for intelligence, capabilities of communication and the power of processing. This means that in the future, the internet of things applications will be able to carry out computational activities that are heavy and they will also be able to do tasks that are data intensive. Through the 5G networks, the devices that will be used in the development of the internet of things solutions will be a lot smarter.

It is likely that new kinds of security threats and challenges will emerge along with the use of 5G technologies and services. However, taking these challenges into account from the initial phases to the deployment will decrease the possibility of having security and privacy faults.

The increasing use of networks in IoT applications has shown the need for the high quality of security services provided, therefore, we have discussed Security Services (QoSS) like confidentiality, integrity, and availability using AWS firewall.

REFERENCES

[1] R.Mitra, D. Agrawal, “5G mobile technology: A survey”, ICT Express-Elsevier, Vol. 1, 2015.

[2] 2. W. Ejaz, A. Anpalagan, M. Imran, W. Wang, "Internet of Things (IoT) in 5G Wireless Communications”, IEEE Access, Vol 4, 2018.

[3] 3. R.Mitra, D. Agrawal, “5G mobile technology: A survey”, ICT Express-Elsevier, Vol. 1, 2015.

[4] 4. Cellular Networks for Massive IoT: Enabling Low Power Wide Area Applications, Ericsson, Stockholm, Sweden, 2016, pp. 1–13.

[5] 5. E. Cero, J. Baraković Husić,and S. Baraković, "IoT’s Tiny Steps towards 5G: Telco’s Perspective", Symmetry, vol. 9, no. 10, p. 213, 2017.

[6] 6. B. Cortés, A. Boza, D. Pérez, L. Cuenca, "Internet of Things Applications on Supply Chain Management", International Journal of Computer and Information Engineering, Vol.9, 2018.

[7] 7. A. Gupta, R. Kumar. “A Survey of 5G Network Architecture and Emerging Technologies”, The Journal for rapid open access publishing, Vol.9, 2015.

[8] 8. Nokia, ‘‘LTE evolution for IoT connectivity,’’ Nokia, Espoo, Finland, White Paper, 2017, pp. 1–1.

[9] Valery Tikhvinskiy, Grigory Bochechka, and Andrey Gryazev, “QoS Requirements as Factor of Trust to 5G Network”, Journal of Telecommunications and Information Technology, 2016.

[10] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu”Security for 5G Mobile Wireless Networks”,IEEE Acess 2017.

[11] Nasreen Sultana Quadri, Dr kusum Yadav, "Efficient Data Classification for IoT Devices using AWS Kinesis", ieeexplore, 2018.

[12] Ijaz Ahmad_, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, Mika Ylianttila{, Andrei Gurtov, "5G Security: Analysis of Threats and Solutions", IEEE conference on standards for communications and networking, 2017.

[13] A. N. Bikos and N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," IEEE Security Privacy, vol. 11, no. 2, pp. 55–62, March 2013.

M. Liyanage, M. Ylianttila, and A. Gurtov, "Securing the controlchannel of software-defined mobile networks," in Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, June 2014, pp. 1–6.

[14] M. Siddiqi, AA. Mugheri, M. Khoso, "Analysis on Security Methods
of Wireless Sensor Network (WSN)", SJCMS, Vol. 2, No. 1, January – June 2018

[15] K. Swarnalatha, Supriya N. Alankar, Y. Bhagyalakshmi, "IOT Security Challenges and Issues – An Overview", UGC Sponsored Two Day National Conference on Internet of Things, February 2016.