Secured Channel Access in Internet of Things-A Review

Karamvir Singh, Guneet Kaur
Department of Electronics and communication Engineering
Amritsar College of Engineering and Technology, Amritsar, Punjab.

Abstract: There are numerous real-world applications of IoT devices within the daily lives of us individuals through which it is easy to perform various tasks. Although this technology provides various advantages, there are numerous challenges also arising within the IoT devices. The authentication amongst various entities of all the nodes within the network is required in a proper way so that there is no type of impersonation identified within the malicious entity. There exists various challenges that are required to be removed from the system and provide a solution which can provide efficient communication between IoT devices.

Index Terms—*Clock Synchronization, Key security, Cloud, Elastic time control, Precision time control*

I. INTRODUCTION

The technology that comprises of multiple network platforms is known as Internet of Things (IoT) in which various wireless protocols are utilized to provide communication amongst the devices. There is high speed of transferring of data such that various activities and operations can be supported with the help of connections provided by IoT-enabled devices. There is an operational enhancement found within the IoT technologies through this manner such that the environment in IoTs is efficient and secure [1].

There is a need to develop “Smart Home” that can provide a secure and efficient scenario to users within various home automated areas. There are various home automation components and energy management devices generated here. The manner in which the healthcare services are being delivered is transformed with the help of various IoT devices such as health monitoring and network-based medical devices. The people that have numerous disabilities and are of old age have numerous advantages of this technology [2]. The cost of independence and quality of life is very reasonable and thus very beneficial for users. The idea of Smart cities has been seen to be successful on the basis of various roads and bridges generated within the intelligent traffic systems within IoT. This results in reducing the congestion as well as the amount of energy being consumed. The availability of information that includes the value chain of production with the help of networked sensors is increased with the help of transformation of agricultural, industrial and energy production technologies provided by IoT.

Although this technology provides various advantages, there are numerous challenges also arising within the IoT devices [3]. The various computing and connectivity related trends that have been arising recently within the IoT scenarios. Fig 1 represents the numerous applications of IoT related to healthcare fields, home and consumer electronics, automotive services and various other sectors.

II. LITERATURE REVIEW

C. Mahapatra et.al [4] stated that the systems that enable the various actions to be performed on the real time sensors as well as virtual online sensors are known as the IoT system. These systems help in sensing, collecting, storing, processing and transmitting the required data from the sensors. The main aspects here are the energy efficiency as well as the robust data delivery within these systems. Here, the active RFID tags that were based on cluster head determination as well as energy harvesting of the IoT systems are proposed. As per the results it is seen that the IoT based WSN heterogeneous systems provide enhancement in the case of energy efficiency and data delivery. There is a great improvement seen through the simulation results achieved here. The energy consumption models have been formulated here as per the sensor nodes that were sent to the base station by the gateway nodes. The simulation depicted considerable improvement in lifetime of network and data delivery to the base station.

J. Yun et.al [5] presented oneM2M standards-compliant device software platform for consumer electronics in light of the Internet of Things, called &Cube. It leverages a standardized resource model and REST (Representational State Transfer) APIs (Application Programming Interface) to work with oneM2M service platforms, prompting to interoperability crosswise over various IoT consumer electronics built on the &Cube. The developing adoption of the &Cube in consumer electronics would lower the barriers for the manufacturers and developers to create innovative products and altogether new services.

L. Atzori et.al [6] provided an integration of various technologies and communication solutions within the Internet of Things. There are various components that together build in the deployment of Internet of Things. There are wired, remote sensor and actuator networks present within such systems along with the improved communication protocols. There are various activities performed by the IoT systems which can be monitored as per the needs. The activities performed can result in providing advancement in the IoTs and help perform learning mechanisms within them. There were applications that required a complex scenario to be established, which could be done with the help of performing various tasks within it that could support the complex nature and help in enhancing its development as compared to the previous one. The achieved results showed the enhancements made.

O. Novo et.al [7] proposed that the potential of this era is boundless, getting new communication opportunities in which ubiquitous devices blend seamlessly with the environment and embrace each aspect of our lives. The development of IoT has been proposed by the capillary networks which further helped in providing local remote sensor network for connecting and efficiently utilizing the capabilities of the gateways present within them. As a result, a vast range of constrained devices equipped with just short-range radio could use the cellular network capabilities to increase global connectivity, supported with the security, management and virtualization services of the cellular network. The authors also introduced another Capillary Network Platform and depicted the rich set of functionalities that enabled this platform. To demonstrate their practical value, the functionalities were connected to a set of typical situations. The aim of their research was to give the reader insight about the Capillary Network Platform and illustrate how this work could be utilized to enhance existing IoT networks and tackle their problems.

J. Gubbi et.al [8] realized that on the basis of the growing remote technologies such as RFID tags, embedded sensor and actuator nodes there was need to enhance the IoT systems. The enhancements made so far have converted the Internet into a completely incorporated future Internet. The Internet services provided were on a very large scale and the enhancements to be made were to be performed in a very careful manner. There was an increase in the need of data-on-request with the help of sophisticated queries being made when the data moved from www to web2 and further to web3. For the complete implementation of IoT systems, a Cloud driven version has been presented in this research which provides the necessities. The future technologies and application domains that are going to enhance the research work related to IoT are proposed. It is concluded by the experiments being conducted that the IoT systems viewed the expansion of their needs on the basis of various requirements within the networks.

H. Suo et.al [9] the author presented the security architecture and features of the IoT applications and provided the enhancements in the architecture. The challenges or vulnerabilities of the system are stated here along with the measures required to remove them. Various encryption mechanisms are proposed along with the communication security measures and cryptographic algorithms that could help in avoiding the loss of privacy of the systems. The studies being proposed in the research has provided various guidelines to ensure the privacy and security of the IoT devices such that there could be no issues faced in the future. However, even with the advancements made, there are lots of challenges being faced. The four layers present within the IoT systems are perceptual layer, network layer, support layer and the application layer. In this research the problems or attacks possible in all four layers are studied along with their characteristics and requirements. There is a need for various encryption mechanisms, protection for sensor data and encryption algorithms. The challenges being faced here are removed with the help of various measures and the results achieved are better as compared to the earlier mechanisms.

J. Granjal et.al [10] proposed that the architecture of IoT devices has IP-based communication protocols that provide the connectivity of devices as per the required applications. It was realized that there was a need of presence of such communication technologies in the areas where information sensing was very important. Keeping in context the goals of ensuring efficiency, reliability and internet connectivity, the various applications of IoT systems are proposed.

III. FEATURES OF IOT

The major characteristic features of IoT can be categorizes as :

A. *Interconnectivity*

In order to connect all the devices with the information and communication infrastructure, a favorable platform is generated by IoT devices [11].

B. *Things-related Services*

A good platform is required in order to provide things that are relevant to services that remain within the constraints of users. Amongst the physical devices, privacy protection is provided by IoT and with the virtual things, the links are formed[12].

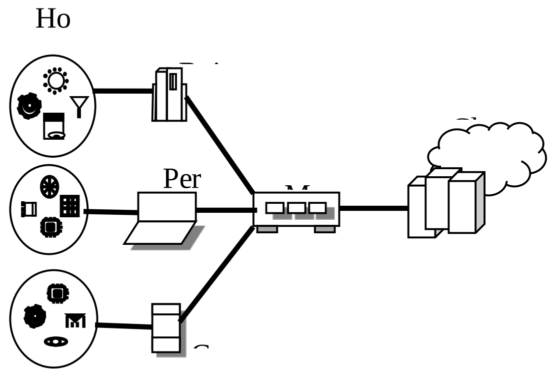

Fig. 1.1: IoT architecture

C. *Heterogeneity:*

An interaction amongst other devices and technologies is provided by the IoT devices by utilizing networks in a direct manner [13]. There are varieties of platforms in which the IoT devices are generated due to which this is known as heterogeneous in nature.

D. *Enormous Scale*

Even though there are large numbers of devices present within the applications that require management in comparison to those that are linked to Internet, there is a need to provide efficient data handling mechanisms. Within critical conditions, data can be handled in efficient manner with the help of IoT.

IV. CLOCK SYNCHRONIZATION

The inaccurate clock synchronization causes where issues to arise amongst which some are explained below :

A. *Network Forensics*

Due to the absence of public Ipv4 addresses, the NAT (Network Address Translation) is utilized by various telecom operators. For multiple numbers of connections, one single IP address can be utilized with the help of NAT. The maintenance of accurate log of time is vital in order to identify the subscribers that include similar IP at various time durations. On the basis of time set upon severs, there is the maintenance of log of time. However, there is no possibility of consistency of time in this case. The identification of exact subscriber is not possible due to the issues related of variation of time of the connection of service providers. Within the IoT systems, this occurs to be a huge challenge[14].

B. *Reliability of time dependent services*

On the basis of time inaccuracy, there are huge affects caused upon the services that are time dependent. It is however, very important to provide accurate server and router log files, reliable IP telephony, and various other VoIP services. There are hue impacts caused on the working model of VoIP services due to the inaccuracy of time [15].

V. MAINTENANCE OF CLOCK SYNCHRONIZATION IN IOT

In order to attain accurate clock synchronization, following are the techniques that can be applied:

A. *Network Time Protocol (ELASTIC TIMER)*

A proper synchronized time can be achieved by utilizing GPS (global positioning system) within the ELASTIC

TIMER. There is higher level of accuracy attained along with reliability with respect to clock synchronization by utilizing ELASTIC TIMER system.

B. *Precision Time Control (PTP)*

In the complete computer network, a clock can be synchronized with the help of PTP protocol. Within the sub-microsecond range, the time and clock accuracy can be attained within the local area network [16]. In order to match with the measurement and control systems, this method proves to be better. The applications that cannot include GPS tracker within every node can use this method.

VI. NEED FOR SECURE CHANNEL ACCESS

A technique through which a secure channel can be established from source to destination within the IoT system is known as secure channel establishment technique. A shared key is generated in order to maintain secure channel from source to destination. The data that is travelling on a channel by including similar key is encrypted and decrypted with the help of shared key. There are few aspects that highlight the need to introduce a secure channel in IoT system [17].

A. *Mutual Entity Authentication*

The authentication of all the nodes within the network is required in a proper way so that there is no type of impersonation identified within the malicious entity.

B. *Asymmetric Architecture*

Amongst various entities, the proper exchange of certified public keys is to be ensured here.

C. *Mutual Key Agreement*

While generating a key during the execution of a protocol, there is a need to make sure that the communicating parties agree.

D. *Joint Key Control*

A weak key needs to be avoided from being chosen by one party while developing a mutual control in the system.

E. *Key Freshness*

It is very important to ensure that the newly generated key is fresh in order to prevent replay attacks in the systems.

F. *Mutual Key Confirmation:*

The creation of similar key amongst the communicating parties is to be ensured here.

G. *Known-Key Security:*

The assessment of long terms secrets is needed to be made impossible when a session key is attained by a malicious user.

H. *Perfect Forward Secrecy:*

The earlier generated session keys should not be compromised by the malicious user in can there is any compromise .

The communications being held within these systems was ensured to be protected which might only provide the usage of such applications more frequent. If the privacy or security was not assured, the users might not opt for their usage. The existing protocols as well as mechanisms that are required to secure the communications being held within IoT were broken down and completely studied. There are various challenges recognized within various IoT applications that are required to be removed from the system and thus, enhancements in the future are also stated in this research.

In order to improve security in IoT, there is a need to come up with a solution which will provide efficient communication between IoT devices.

CONCLUSION

The IoT is the self configuring and decentralized type of network in which sensor nodes sense information and pass it to server. The sensor node transmits the data on the wireless channels and these channels are allocated to each sensor node with the elastic time technique. There is need to improve security and efficiency of IoT network

REFERENCES

[1] Fevgas, P. Tsompanopoulou, and P. Bozanis, "iMuse Mobile Tour: a personalized multimedia museum guide opens to groups", in Proc. of IEEE Symposium on Computers and Communications (ISCC), pp. 971-975, 2011.

[2] M. Kanda, R. Arai, Y. Suzuki, Kobayashi, and Y. Kuno, "Recognizing Groups of Visitors for a Robot Museum Guide Tour", in Proc. IEEE 7th International Conference on Human System Interactions (HSI), pp. 123-128, 2014.

[3] N. Yu and Q. Han, "Context-Aware Community Integrating Contexts with Contacts for Proximity-Based Mobile Social Networking", in Proc. of IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 141- 148, 2013.

[4] C. Mahapatra, Z. Sheng and V. Leung, "Energy-efficient and Distributed Data-aware Clustering Protocol for the Internet-of-Things", in Proc. of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), vol. 1, pp. 1-6, 2016.

[5] J. Yun, I. Ahn, N. Sung, and J. Kim, "A Device Software Platform for Consumer Electronics Based on the Internet of Things", IEEE Transactions on Consumer Electronics, vol. 61, no. 4, pp. 564-571, 2015.

[6] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Journal of Computer Networks, vol.54, no. 15, pp. 2787-2805, 2010.

[7] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen,"Capillary Networks – Bridging the Cellular and IoT Worlds", in Proc. of IEEE World Forum on Internet of Things, vol. 2, pp. 571-578, 2015.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements and future direction", Journal of Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, 2013.

[9] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, pp. 648-651, 2012.

[10] J. Granjal, E. Monteiro, and J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in Proc. of IEEE on Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.

[11] D. Guo, Z. Zhang, Z. Wang , Z. Yu, and X. Zhou, "Opportunistic IoT: Exploring the Harmonious Interaction between Human and the Internet of Things", Journal of Network and Computer Applications, vol. 36, no. 6, pp. 1531– 1539, 2013.

[12] H. Lin, "Applying location based services and social network services onto tour recording", in Proc. of IEEE International Joint Conference on Computer Science and Software Engineering (JCSSE), pp. 197-200, 2012.

[13] Huang, C. Lee, and H. Lai, "Energy-aware Group LBS using D2D Offloading and M2M-based Mobile Proxy Handoff Mechanisms over the Mobile Converged Networks", IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 4, pp. 528-540, 2016.

[14] B. Guo, Z. Yu, L. Chen, X. Zhou, and X. Ma, "MobiGroup: Enabling Lifecycle Support to Social Activity Organization and Suggestion with Mobile Crowd Sensing", IEEE Transactions on Human-Machine Systems, vol. 46, no. 3, pp. 390-402, 2016.

[15] Namiot and M. Sneps-Sneppe, “Social Streams based on Network Proximity,” 2013, International Journal of Space-Based and Situated Computing, vol. 3, no. 4, pp. 234-242, 2013.

[16] G. Giorgi, C. Narduzzi, “Configurable clock service for time-aware IoT applications”, IEEE International Conference on Distributed Computing in Sensor Systems, pp. 1-6, 2017S. Jisha, M. Philip, “RFID based security platform for Internet of Things in Health Care Environment”, in Proc. of IEEE Online International Conference on Green Engineering and Technologies (IC-GET), pp. 1-3, 2016.