IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

ISSN: 2664-9519 (Online); Vol. 1, Issue No 1, August 2019

Fog Computing Trust based Architecture for Internet of Things Devices

Shahid Mahmood, Amin Ullah and Anas Khalid Kayani

Department of Computer Science, Bahria University, Islamabad, Pakistan

Institute of Avionics and Aeronautics, Air University, Islamabad, Pakistan

* Corresponding Author: shahidmscs@yahoo.com

Received 10-April; Revised 25-May; Accepted 25-June; Published 15-August

Abstract: Fog computing has gained more popularity due to the rapid increase of Internet of Things (IoT) devices and their distributed nature. To handle these complex networks, cloud computing is used as a centralized processing, storage, security and network management capabilities. Cloud computing is not more efficient to handle all IoT operations due to limited processing power, storage, bandwidth, battery and sometime not able to fulfill the required real-time response. In addition, cloud computing is also time consuming and having latency and security issues. While fog computing has opposite architecture where edge devices are adopted to carry out a substantial amount of computation, storage, communication locally and routed over the internet backbone. Therefore fog computing is the most suitable solution, where processing is performed close to edge devices and provide all requirements and more useful for real-time applications. In this paper, we propose a trusted model based on fog computing for IoT. We also discuss the security issues and try to address the security issues in IoT.

Keywords: *Internet of Things, Fog node, Cloud, Security, Role of Fog, Certification Authority*

1. Introduction

Internet of Things (IoT) have gained popularity due to its various affordable and useful. With the passage of time, IoT data communication has suffered with security, storage and management issues. The Internet has affected positively almost in every field of life where users being become comfortable with it. It is a natural phenomenon that human always goes for a more comfortable environment and always consider easy to use, cost effective and smart applications. The most popular applications are includes smart or autonomous vehicles, smart buildings, health monitoring, energy management, construction management, environment monitoring, production, and assembly line management and supply chain management [1]. The curiosity of human being and technological developments led towards the rapid growth of IoT devices where any device connected to receive and send the data to other devices or edge devices. The edge devices are continuously increasing in number within the past few years. The Gartner said that 30% (6.4 billion) of edge devices are increased in 2016

as compared to 2015 [2]. It is also forecasted that in 2020 the number of connected edge devices will be 20.4 billion [3]. The Ericsson's mobility report has forecasted that approximately 29 billion devices will be connected by 2022 and out of these 18 billion will be related to IoT applications [4]. This increase of several edge devices is also increasing the data traffic between cloud servers and edge devices, which also result in delay or increasing response time. The edge devices are installed in various industries, control systems and monitoring systems where the nodes requires less than few milliseconds latency for connection with other control nodes [5]. Similarly, the delay time may be tens of milliseconds especially for autonomous vehicles on the roads, air traffic controlling systems, gaming applications and online financial transactions [6, 7]. This time cannot be achieved by mainstream cloud services. Some edge devices produce a large amount of data, for example, it was reported by the network world that one autonomous car will use 4,000 GB of data per day [8, 9]. On this point, Gartner said that quarter billion vehicle nodes will be connected by 2020. It means that only cars will produce 250,000,000 x 4000 GB of data per day. On October 17, it is reported that 2.5 quintillions bytes of data are created each day [10].

Keeping in view the growth rate and requirements of human, the development in the field of IoT for last ten years is focused on the conversion of standalone devices to communicating devices as well as improvement in computing power, energy capacity, storage capabilities and data security [1]. In spite of all these efforts, IoT devices or edge devices have still limited resources to provide real-time response [11]. The less time duration should be useful for route information especially for time critical applications. Recently, cloud computing based solutions have proposed to handle IoT applications data. However, due to limited resources of cloud computing still this area has suffered with various challenges. Fog computing is one of the most suitable solution, where processing is performed close to edge devices and this architecture fulfill the requirements of the IoT. The constant increase in several edge devices will be efficiently managed by hierarchical infrastructure, where a major portion of processing will be performed locally at the fog layer. The only global processing will be performed at the cloud. This will get a rid of extra communication between edge devices and the cloud. The processing capacity may be adjusted concerning the environment and the processing requirement of edge devices.

There is no doubt in that, Fog computing will play a vital role in improving the efficiency of IoT devices but security concerns will also be raised due to its distributed nature processing environment. Fog layer is working as the integration of heterogeneous technologies which is a combination of the virtual environment, wireless communication, peer-to-peer system, and dynamic nature of IoT devices. The security issues of IoT environment will be inherited in fog computing. There is a need to address the following questions:

- Design a mechanism for ensuring the authentication among edge devices before data communication.
- Efficient distribution of information about revoked certificates among edge devices.

In this paper, we proposed a trust based architecture using for computing for IoT devices. The main objective of the proposed architecture is to ensure the authentication among edge devices because most of the vulnerabilities are exist in edge devices and most of the data volume is filtered at Fog node. Addressing security issues of edge devices, using digital certificates signed by Fog node. Fog node operates in a specified domain, this domain is considered as a trusted domain. The communication within the trusted domain of Fog node authenticated. The proposed trusted architecture is designed for authentication among edge devices using digital certificates. The proposed architecture is designed keeping in view the static edge devices, for example, home appliances, where edge devices are required to communicate with each other.

This paper discusses the security and privacy issues of edge devices and Fog or edge computing. In Section 2, there background of Fog computing and critical analysis of security issues edge devices and Fog layer in the context of IoT environment discuss. In Section 3, the proposed architecture discusses along with its performance. Finally, Section 4 concludes with results and future direction.

2. Fog Computing

This section explains the architecture on Fog computing. The role of Fog computing in IoT environments presents with security services, threats to edge devices and threats to Fog computing. Then the requirement of trust mode are highlighted.

2.1 Architecture of Fog Computing

Fog computing is also known as edge computing. Fog computing has a three-layer architecture called client, Fog nodes, and central server [12, 13]. The objective of Fog computing is to bring the services which are closer to the edge devices as shown in Figure 1. There is not a huge difference between cloud and Fog computing except processing power, which can be represented as (Processing power of Cloud > Processing power of Fog node > Processing power of edge devices) and the placement of Fog node at the edge of the local network [14]. The concept of Fog is in contrast to cloud computing.

2.2 Role of Fog Computing

In Fog computing, edge nodes can access local data without involving the cloud. Only filtered data travels to the cloud and leads to inefficient utilization of network bandwidth as well as storage capacity and processing resources of cloud [15]. Fog nodes capacity may vary from limited resources to high power computational devices. The purpose of the Fog layer is to provide temporary storage, computation and other services like communication between IoT devices whenever required. Fog services are very much advantageous in IoT environment like real-time processing and response and dynamically allocation of resources on the requirement of IoT devices, which is also called resource pooling.

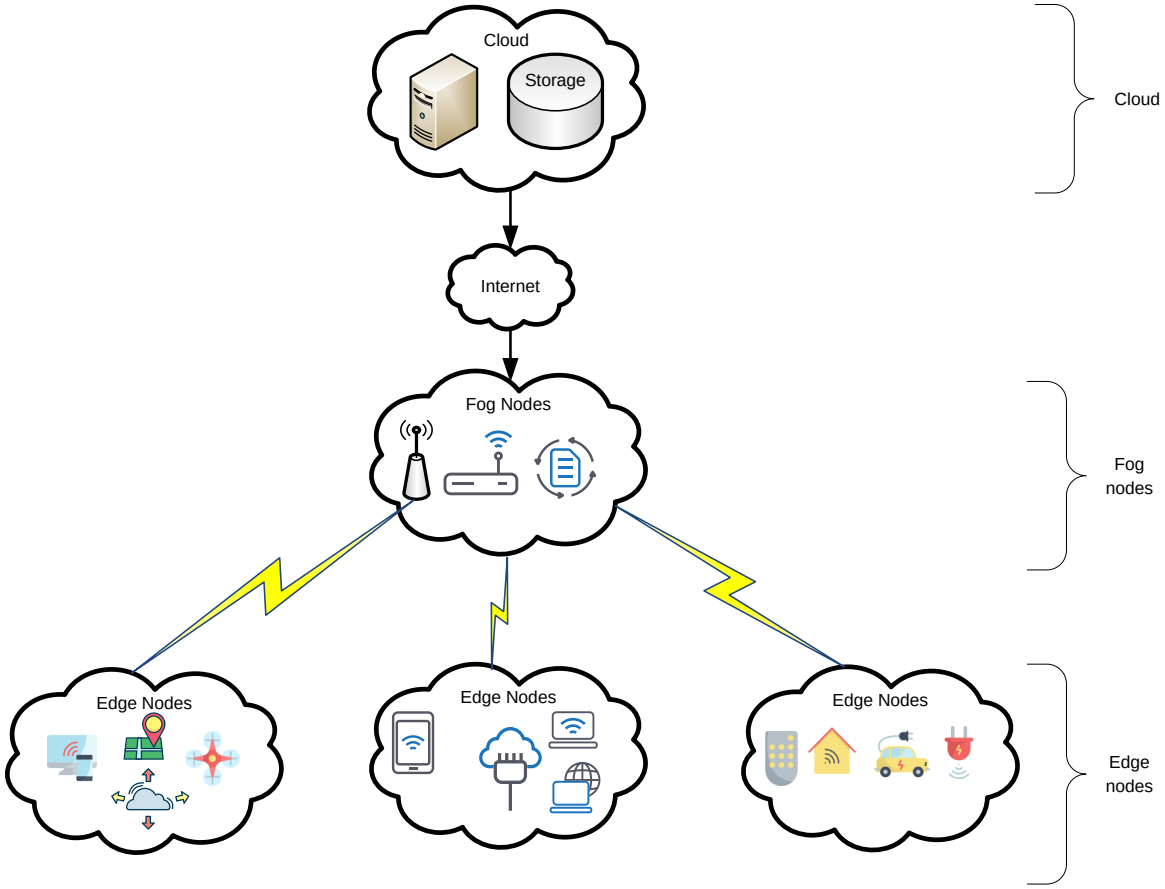

Figure 1. Three Layers Architecture of Fog Computing

Table 1. Role of Fog Computing in IoT

Scenario	Fog Role
Smart Grid	Data Filtering to be consumed locally and send to the rest to the higher tiers for visualization, real-time reports and transactional analytics [16].
Smart Traffic Lights and Connected Vehicles	Neighboring smart lights serving as Fog devices coordinate to create a green traffic wave and send warning signals to approaching vehicles [17].
Wireless Sensor and Actuator Networks	Fog devices can control the measurement process
Decentralized Smart Building Control	Fog devices can keep sensors collaboratively, which can be used to conserve energy, water and other resources.
IoT and Cyber-physical systems (CPSs)	IoT is a network that can interconnect ordinary physical objects with identified addresses [18].
Software-Defined Networks (SDN)	Intermittent connectivity, collisions and high packet loss rate by augmenting vehicle-to-vehicle with a vehicle to infrastructure communications and centralized control [19].

2.3 Security Services

There are many security issues are highlighted in [1]. Each of the security issue can lead to compromise many services off Information, Assurance, and Security- Operationally Critical Threat, Asset, and Vulnerability Evaluation (IAS-Octave) standard. There are many other security issues are highlighted in [14, 16, 20-22]. All these issues are related to one of the security breaches in IAS-Octave. However digital Certificates can be used to solve most of the issues and provide IAS-Octave shown in Table 2. Authentication is one of the most critical and important issue for the security.

Table 2. IAS-Octave

Requirement	PKI	Remarks
Confidentiality	Yes	Secure exchange of Symmetric Key Asymmetric Encryption
Integrity	Yes	Cryptographic hashes encrypt with private key
Availability	No	Can help Indirectly
Accountability	Yes	Usage of Private Keys
Auditability	Yes	Partial
Trustworthiness	Yes	Root CA and intermediate CA
Non-repudiation	Yes	Usage of Private Keys
Privacy	No	Partial

2.4 Security Issues of Edge Devices and Fog Computing

There are many security attacks which can be addressed using digital certificates by incorporating Fog computing [11]. Specifically, it is pertinent to mention that authentication, integrity, privacy and key exchange can be efficiently achieved by digital certificates. Similarly, prevention from DOS (Denial of Service) attacks can be easily achieved. Fog computing since, services are offered to massive-scale end-users by front Fog nodes [23]. These security threats can cause really serious cyber security attack on edge devices and edge computing. Most of the security attacks cause after bypassing the authentication. An environment defined in scope can be made safe against most of the network attacks by establishing a trusted domain. An overview of the role of Fog computing is given and security threats are discussed. These issues are showing the importance of security of edge devices and edge computing. It is earliest presented that most of the communication is done locally because only filtered data can be sent to the cloud, therefore the security of local communication is important. Therefore a trusted model is being proposed for ensuring the security of edge devices in the next section.

Table 3. Security Issues

Security Issues of IoT Devices or edge Devices	Security Issues at Fog or edge Computing
Corrupted/ malicious node	Malicious injection
Physical attacks/ tampering	Integrity attacks against learning
Tag cloning	Non-standard framework
Counterfeiting	Insufficient/Inessential logging
DoS attacks	Side-channel attacks
Eavesdropping	-
Inventorying	-
Hardware Trojan	-
Non-network side-channel attacks	-
Denial of Service (DoS) attacks	-
Physical attacks/ tampering	-
Node replication attacks	-
Camouflage	-

3. Proposed Architecture

3.1 Fog Node as a trusted Intermediate Certification Authority

The proposed architecture shown in Figure 2. It can be easily deduced that local communication among edge devices is huge rather than communication with the cloud. Therefore the focus of the trusted model is to ensuring the trusted communication among edge devices. The Fog node acts as a Certification Authority (CA) for the specified trusted domain. Internal communication is held using local certificates issued by Fog node. Only first-time edge node has to verify the certificate traditionally. However once trust is established then later all communication will be done through local certificates.

Fog node is responsible for the distribution of revoked certificates' information amount edge devices. This information is required only when a device communicates with the outside world.

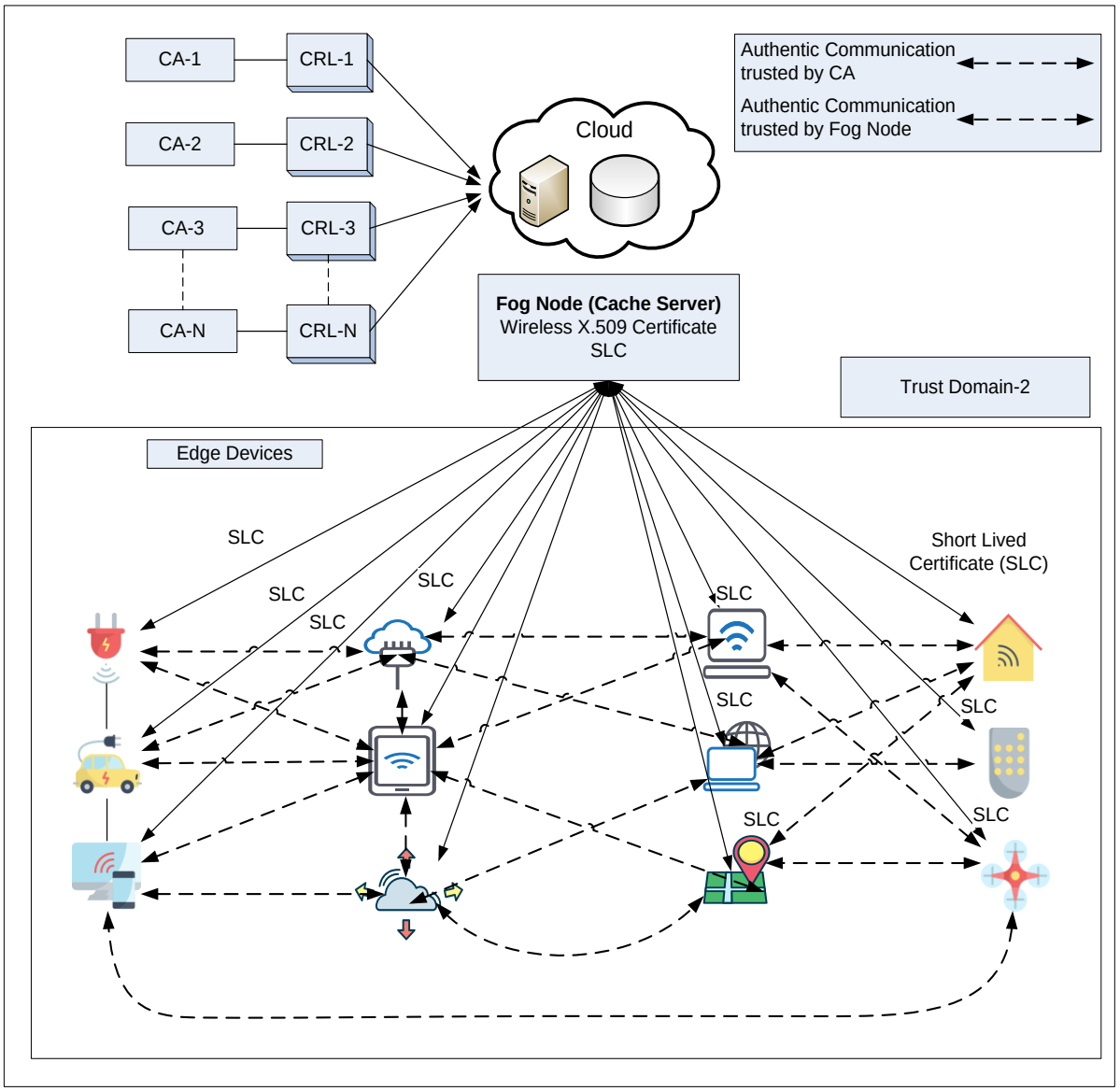

Figure 2. Proposed Architecture - Trusted Domain

3.2 Messaging of Fog Node as a trusted Intermediate Certification Authority

Figure 3 illustrates the messaging between the edge node, the Fog node, and CA. Initially, it is assumed that the Fog node contains information about CRL of all CA. Node-1 establishes a connection with Fog Node and verifies its certificate using normal OCSP. Node-1 verifies the certificate of Fog node using the public key of CA. Once Fog node becomes trusted then

it may work as an intermediate CA is capable of issuing SLC. SLC is duly signed by the private key of Fog node and Node-1 is verifying using the public key of Fog node. Similarly, Node-2 verifies the certificate of Fog node which is using the public key of CA. Once Fog node becomes trusted then it may work as intermediate CA and capable of issuing SLC to Node-2. The SLC is duly signed by the private key of Fog node and Node-2 is verifying using the public key of Fog node. Now, Node-1 and Node-2 are in same trusted domain and certificate of Fog node is placed at edge device like other CA's certificates. Emin Topalovic implemented a prototype CA and certificate update plugin for Apache that shown the viability of SLC in [24].

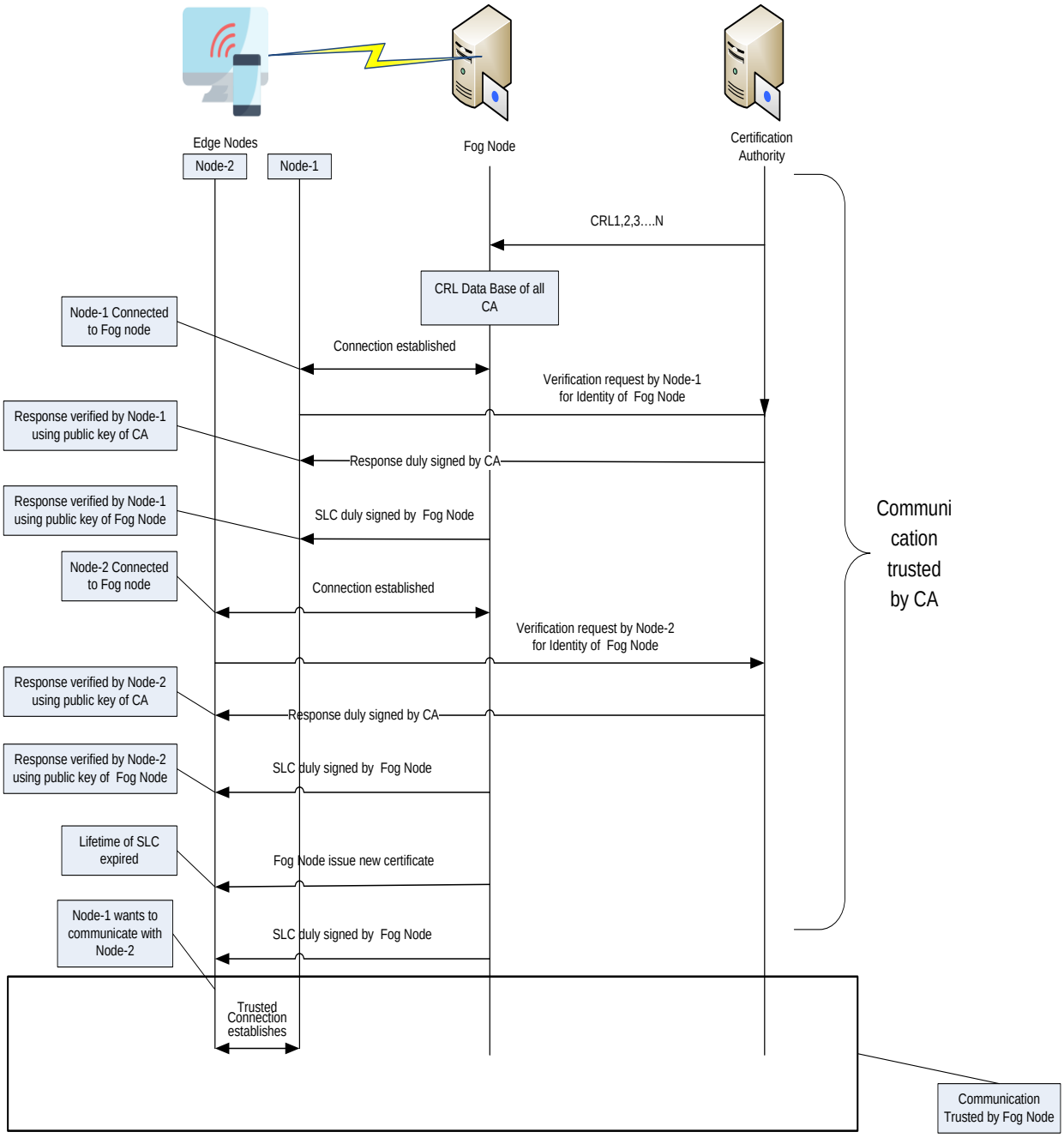

Figure 3. Messaging of Fog Node as a Trusted Node

4. Conclusion

Fog computing has gained popularity especially in the domain of IoT where a large amount of data exist. Cloud computing has played its role to handle IoT data but still suffered with processing, storage, and network management

services. On the other hand, Fog computing is one of the opposite architecture where processing is performed close to edge devices and fulfill the requirements of the IoT. .This makes it more useful for real-time applications. In this paper, the role of Fog computing in IoT is discussed and proposed a trusted architecture to address the security issues. It is concluded that when data communication is done without the involvement of cloud then security can be achieved efficiently. In future, we test this model with stat of the art existing models.

References

[1] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, pp. 586-602, 2017.

[2] C. STAMFORD. (Nov. 2015). *Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in2016 Up 30 Percent from 2015*. Available: www.gartner.com/newsroom/id/3165317

[3] R. v. d. Meulen. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016*. Available: www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[4] R. Ström, M. Vendel, and J. Bredican, "Mobile marketing: A literature review on its value for consumers and retailers," *Journal of Retailing and Consumer Services*, vol. 21, pp. 1001-1012, 2014.

[5] M. Weiner, M. Jorgovanovic, A. Sahai, and B. Nikolié, "Design of a low-latency, high-reliability wireless communication system for control applications," in *Communications (ICC), 2014 IEEE International Conference on*, 2014, pp. 3829-3835.

[6] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, pp. 854-864, 2016.

[7] A. Hasan and K. Qureshi, "Internet of Things Device Authentication Scheme Using Hardware Serialization," in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, 2018, pp. 109-114.

[8] P. Nelson. (Dec, 2016). *Just one autonomous car will use 4,000 GB of data/day*. Available: https://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html

[9] K. N. Qureshi, F. Bashir, and A. H. Abdullah, "Distance and signal quality aware next hop selection routing protocol for vehicular ad hoc networks," *Neural Computing and Applications*, pp. 1-14, 2019.

[10] J. Schultz. (2017). *The Amount of Data Created Each Day on the Internet in 2017*. Available: https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/

[11] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, pp. 34-42, 2017.

[12] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the Suitability of Fog Computing in the Context of Internet of Things," *IEEE Transactions on Cloud Computing*, vol. 6, pp. 46-59, 2018.

[13] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293-19304, 2017.

[14] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*, 2014, pp. 1-8.

[15] B. N. Ekanayake, M. N. Halgamuge, and A. Syed, "Security and Privacy Issues of Fog Computing for the Internet of Things (IoT)," in *Cognitive Computing for Big Data Systems Over IoT*, ed: Springer, 2018, pp. 139-174.

[16] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, pp. 2991-3005, 2016.

[17] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012, pp. 13-16.

[18] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, pp. 2787-2805, 2010.

[19] K. N. Qureshi, A. H. Abdullah, O. Kaiwartya, F. Ullah, S. Iqbal, and A. Altameem, "Weighted link quality and forward progress coupled with modified RTS/CTS for beaconless packet forwarding protocol (B-PFP) in VANETs," *Telecommunication Systems*, pp. 1-16, 2016.

[20] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16-27, 2018.

[21] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International conference on wireless algorithms, systems, and applications*, 2015, pp. 685-695.

[22] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*, ed: Springer, 2018, pp. 103-130.

[23] M. H. Ibrahim, "Octopus: An Edge-fog Mutual Authentication Scheme," *IJ Network Security*, vol. 18, pp. 1089-1101, 2016.

[24] E. Topalovic, B. Saeta, L.-S. Huang, C. Jackson, and D. Boneh, "Towards short-lived certificates," *Web 2.0 Security and Privacy*, 2012.