THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

A Proposed Architecture of Iot-Fog-Computing Oncyber Security system and big-Data Analytics

Inzimam Ul Hassan, Swati*, Mehak, Upinderkaur

Lovely faculty of Technology and Sciences

Lovely professional university, Phagwara, Punjab

inzimamulhassan@gmail.com, rampalswati@gmail.com,

mehakkatnoria93@gmail.com, upinderkaur45@gmail.com

Abstract*—In particular, the cloud computing that represents a revolution in Internet of Things (IoT), with its hype today, the service providers are facing various drawbacks like cyber threats, mobility support lacking and location-distribution.Fog-enabled IoT is a new paradigm that expands the architecture of cloud computing by providing services and resources on the edge of the network and also integrates with the Internet of Things. Fog/Edge computing has been proposed for tending to a portion of downsides, as at the edge of the networks it empowers the computing assets and offers big-data examination instead of transmitting them to the Cloud at local bases. A Cloud-like framework has been characterized for the Fog which is having comparative capacities, including software, platform and infrastructure-based-services. The distribution of Fog applications faces different security issues identified with virtualisation, monitoring of network, information assurance and assault identification. The communication of three layers i.e. Fog, IoT and cloudfor adequately executing large information examination and digital security applications has been explained in the given paperwhich recommends a foundational IoT-Fog-Cloud engineering. It likewise surveys security barriers, arrangements and future research headings in the design.*

Keywords:-Cyber-attacks, Internet of Things, Fog/Edge Computing, Authentication, AES,Challenges, Solutions, Message Queuing Telemetry Transport

Introduction

Web has assumed essential job today. Everything around us associated with internet with computerized personality. With the improvement of Internet Innovation, Internet of Things has gotten more significant piece of day by day human life.The Internet of Things has developed to digitize our day by day undertakings in different frameworks, for instance, smart homes, keen urban areas, smart industrial facilities and smart medicinal services [1].

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Long as Cloud frameworks offer high computational foundation, control, data bandwidth, software, stages and capacity, IoT applications coordinate with Cloud frameworks crosswise over system frameworks [2], [3]. IoT frameworks fuse the transmission of sign of sensors, actuators and administrations, which require high preparing resources for executing big -data investigation and cyber security applications. Regardless they experience the ill effects of the disadvantages of adaptability, where different set of information sources are gathered and investigated from the three layers of IoT, Fog and Cloud frameworks [1], [4], [5].

Cloud frameworks, in types of software, stages and infrastructure, would address the difficulties of adaptability and operability by giving administrations to clients and organizations[1], [6]. As it may, Cloud frameworks experience the ill effects of absence of mobility support, inactivity, awareness of locations and geo-distribution. The Fog/Edge standards have been anticipated to handle negative marks of Cloud-based systems which empower big-data investigation at the edge of the network [4]. The technology termed as 'Fog Computing' was authored by a company named OpenFog Consortium [1], [5]. It is an architecture which expands the principle elements of the Cloud to give services at the edge of a network system, and is a very virtualised design of the reserve pool. The Fog provides a decentralized foundation, where information is audited and examined between the customers and Cloud server centres. For impressively supporting data management systems, well-situated to smear real-time and big-data analytic techniques.

IoT consists of three issues.In the first place, heterogeneity is discussed in the aspects of different sensing, processing and storage components. Traditionally, only computers are linked to the Internet. Today, heterogeneous things around here with a digital identity are linked to the Internet.Second, scalability is the key solution for handling explosive growth in the IoT ecosystem. When you deploy the IoT system, remember the current and future needs of the system. Due to lacking scalability, IoT will not be accommodating future expansion.Develop a system for ease of expansion, Demand device durability, and Align network and device longevity are three key points for insuring scalability in IoT.Third, Under Interoperability, the various number of heterogeneous devices are working together to achieve a high level of goal in the IoT ecosystem. It is therefore the most essential need for IoT devices to interact with each other. For example,a laptop with WiFi enabled facilities cannot be automatically connected to a mobile phone with the Bluetooth enabled facility [20]. Because of various security related issues, the full-fledged security solutions are hard to implement under IoT environment.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Research studies under [4]–[9] suggested that Fog innovation shall be structured later on to provide an improved and reliable structure for taking care of the eternally increment of organizedutilizations and services.The writers in [1], [6], [9]-[11] has been recommended enormous techniques to deploy access control, security solutions, firewall, authentication and IDPS (Intrusion Detection and Prevention System) at layer named Fog.

A Universal IoT-Fog-Cloud architecture has been proposed in this paper to improve the implementationbased on analytics of big-data and applications of cyber security. Security related challenges, threats in security, existing results in security and further research guidelines has been also discussed here.

Literature Review

Liu et.al has presented some cloud computing framework and furthermore breaks down cloud computing security issue. He proposed that solitary security can't be utilized to tackle the cloud security issue subsequently, numerous conventional and some new methodologies are required to utilize together to give the whole security in cloud [21].

Aderemiet.al have discussed security vulnerabilities falling under cloud computing and the possibilities that could be taken to perform homomorphic encryption, and mooted an encryption layer on the top of the encrypted data in the cloud[22].

Simarjeet Kaur et.al, contemplated the various information encryption systems that have been created by analysts throughout some last year's[23]. It is ensured that critically important information is protected here at all times by the use of such secure techniques in cloud applications.

Sang et.al[16] anticipated a framework for Fog, which is a context-aware framework. The designed framework bolsters various edge technologies, includes Wi-Fi, Bluetooth and LTE capabilities with the support to Software Defined Networks (SDN) and virtualization tools.It is additionally proposed to convey Airborne Fog frameworks, where air gadgets alike drones could be executed like Fog nodes to facilitate different implementations and a variety of facilities to the end-users [17].

[24] have been discussed about that,in fog computing platform and EU's devices an Authentication is a crucial requirement. Insecure authentication, as foremost security concern under Fog computing has been identified.

Azam et.al[13] has been proposed a methodwhich connects a smart communication and already processed data module for Cloud-IoT networks. To diminish the computational

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

overhead at the Cloud side, the given technique has been taken a combination of smart gateway with Fog computing technique.

R.Nikam, et.al[25], instigated a novel approach called "Cloud Storage Security using Multi-Factor Authentication", To provide security to organizational data from intruders. This paper advises CP-ABE (Ciphertext-Policy – Attribute-Based Encryption and Multi-Factor Authentication (MFA) guarantees the sharing of data between peer organization to keep identity unspecified. Static username and passwords are also used to ensure initial level authentication followed by OTP based on Token (TOTP Algorithm) generator technique that is taken as authorizations for users.

FOG Computing Systems

Fog system description

Fog computing is a decentralized computing framework wherein information, compute, storage and applications are found somewhere close to the information source and the cloud.The Fog worldview was firstlyanticipated by an organization named Cisco to turn into an architecture of Cloud frameworks which gives computation, storage and correspondence benefit between Cloud servers and customer systems [1], [5], [10]. The computation and data processing facilities has been activated by fog at the edge of the network. Which defines that it is a complimenting layer to the cloud computing system and also offers physical design of distributed architecture. In short it could be said that it is impossible to use fog computing without cloud computing.

In 2016 under OpenFog Conglomerate, an Open Machine to Machine (OpenM2M) architecture is suggested to create link between IoT devices and Fog and other services [14].Under other [15] fog computing design has been proposed, which have designed various application interfaces to enable access through virtual machine for collecting important data at Fog nodes.

IoT-Fog-Cloud's Systemic Architecture

Fog computing is introduced to manage the restriction of Cloud Computing. For supporting Internet of Things Fog Computing came under lemon light. Fog computing hubs can process the information with highest priority that should be tended to right away. The Fog hubs are the nearest to IoT gadgets and procedure high prime concern.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

The information produced by IoT devices have little emphases can be coordinated to cloud server for further examination and preparing.

In Fig-1, a systemic design has been proposed for showing communication of Fog, IoT and cloud layers, Where Smart cities and Smart factories have been taken as example. Message Queuing Telemetry Transport (MQTT) is connected to industrial IoT actuators for publishing topics like measuring temperature and humidity. [1] Given architecture in Fig-1 allowing monitor, capture, filter, examine and exchange of data, which would save time and access recourses to deploy and run Bigdata analytics with security applications in cyber.

On the other hand, Distributed architecture of fog could be used to enhance computational resources for big-data analytics at the edge of network infrastructure. The network elements like access points, router, hub, switches and set-top-boxes could be used to enhance the services.

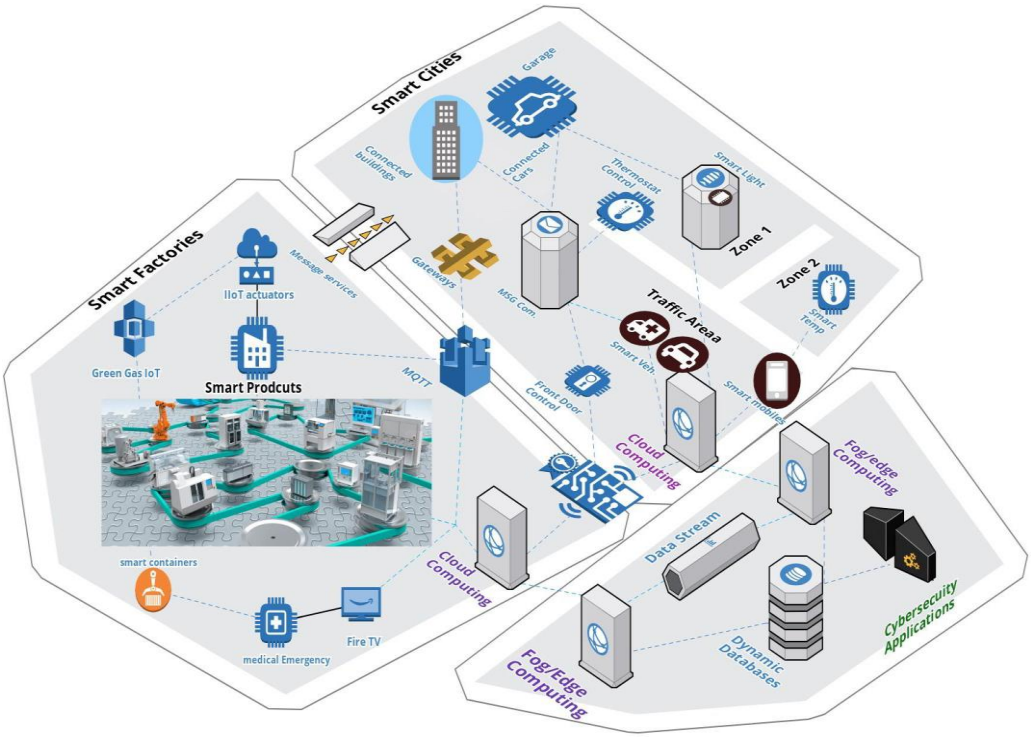

Fig1-Fog computing architecture and Cloud-IoT interaction

IOT, FOG AND CLOUD SYSTEM'S APPLICATIONS

Fog computing benefits can used for different cloud and IoT based applications [18]. How the fog applications can be implemented for real time and at large scale is explained as below:

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

- SDN(Software Defined Networks): is a type of a network infrastructure that could be used by fog to bring about and handle control over the SDN communication layers. A tech named control unit has been executed to the server which is centralized and SDN nodes specified communication path [18].
- Smart Grid: has meters and microgrids fabricated at the edge of the technology of network to balance load of services. The smart grids have been supported by the fog to generate data from IOT designed network for storing data and other data mining applications.
- Wireless Sensor network: are used to trail and sense variety of IoT based applications. The actuators are used to handle the network physically. The actuators can easily manage the performance while they accessed as fog appliances.

CYBER SECURITY BASED CHALLENGES

Meanwhile the devices based on Fog and IoT devices are connected with cloud, the network could be damaged by many cyber security threats. The reason behind these attacks and threat are unsecured locations which are protected, open architecture which leads to loop-holes and vulnerabilities [19]. Various security issues in Fog are given below:

a) While fog nodes are leaving and joining the network, which makes it difficult to maintain security, authentication and privacy.
b) While fog nodes are leaving the fog layer of the network it's tough to reserve privacy by EU's.
c) Trace users with the help of cloud service provider is also difficult.
d) Provide sufficient and strong authentication to the infrastructure is also being difficult.
e) Fog system is facing various advanced persistent threats like botnets and ransomware which are inherited from IoT and cloud-based system.
f) Fog nodes are handling data in large amount which makes it easy to compromise by the attackers. Many difficulties occur while asserting, integrate and to maintain privacy.
g) Various privacy issues also occur while dealing with concealing confidential data. It should be mandatory to hide details of sensitive data while making privacy preserving techniques.

SOLUTIONS TO MAINTAIN SECURITY AND FUTURE SCOPE

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Number of security solutions cane be taken to handle above privacy issues like firewalls, encryption, authentication, authorization and access control. Intrusion detection and prevention system can also be installed to handle different security and privacy challenges. It could also decrease complexity in authentication.

a) *Access control* mechanism installation may help to facilitate authentication and authorization to end users and at workstations guarantied. A policy-based control has been proposed in Fog for protecting cooperation in between heterogenous sources.
b) With the installation of *Intrusion Detection System (IDS)* all the suspicious events could be recognized easily, it also makes audit records of all the events which occur at Fog layer. All the suspicious events and attacks could be easily recognized by analysing network traffic.
c) To protect user information *Privacy and Encryption* based techniques have been used, under which it makes hard to secure data for IoT, Fog and Cloud based system. For cloud many solutions have been offered like smart grid and wireless networks. This technique might be implemented for protecting data from tampering. Privacy techniques also need research in future to secure sensitive information and the reason behind this is network nodes distribution on high demand.

CONCLUSION

In given paper, an architecture of IoT, Cloud and Fog layer has been reviewed for effective and secure communication. The layers of given architecture generate different number of data sources, cloud layers used for processing, where data is computed and stored at centralised set of locations. Because of mobility in network the security became a biggest challenge. Many security challenges under Fog has been reviewed here and which possible precautions can be taken are also discussed. In Addition, the paper has also reviewed about existing IoT and Cloud open architecture under security issues. There are various security problems still exist which could be removed while taking future research direction and can also improve previous security techniques.

References

[1] S.Khan,S.Parkinson and Y.Qin, “Fog computing security: a review of current applications and security solutions”,*Journal of Cloud Computing*, vol. 6, no. 1, p. 19, Dec 2017.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[2] N.Moustafa, K.K.R.Choo,I.Radwan, and S.Camtepe, "Outlier dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog", IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 1975-1987, Jan 2019.

[3]A.V.Dastjerdi, H.Gupta, R.N.Calheiros, S.K.Ghoshand R.Buyya, "Fog computing: Principles, architectures, and applications",in internet of things, pp. 61-75, Jan 2016.

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

[5] G.Kurikala, K.G.Guptaand A.Swapna, "Fog computing: Implementation of security and privacy to comprehensive approach for avoiding knowledge thieving attack exploitation decoy technology", International Journal of Scientific Research in Computer science, Engineering and Information Technology, vol. 2, no. 4, pp. 176-181, Aug 2017.

[6] S.Yi, C.Liand Q.Li, "A survey of fog computing: concepts, applications and issues", in Proceedings of the 2015 Workshop on Mobile Big Data. ACM,pp. 37–42, Jun 2015.

[7] M.Chiang, S.Ha, I.Chih-Lin, F.Rissoand T. Zhang, "Clarifying fog computing and networking: 10 questions and answers", IEEE Communications Magazine, vol. 55, no. 4, pp. 18–20, Apr 2017.

[8] Y.Guan, J.Shao, G.Weiand M.Xie, "Data security and privacy in fog computing", IEEE Network, vol. 32, no. 5, pp. 106-111, Mar 2018.

[9] G.Premsankar, M.D.Francesco and T.Taleb, "Edge computing for the internet of things: A case study", IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1275-1284, Feb 2018.

[10] R.Roman, J.Lopezand M.Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges", Future Generation Computer Systems, vol. 78, pp. 680-698, Jan 2018.

[11] K.K.Choo, R.Lu, L.Chen and X.Yi, "A foggy research future: Advances and future opportunities in fog computing research", pp. 677-679, 2018.

[12] N.Moustafa, G.Misraand J.Slay, "Generalized outlier gaussian mixture technique based on automated association features for simulating and detecting web application attacks", IEEE Transactions on Sustainable Computing, Feb 2018.

[13] M.Aazam and E.N.Huh, "Fog computing and smart gateway based communication for cloud of things", in Future Internet of Things and Cloud (FiCloud), 2014 International Conference on. IEEE, pp. 464–470, Aug 2014.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[14]S.K.Datta, C.Bonnet and J.Haerri, "Fog computing architecture to enable consumer centric internet of things services", in Consumer Electronics (ISCE), 2015 IEEE International Symposium on. IEEE, pp. 1–2, Jun 2015.

[15] M.Zhanikeev, "A cloud 19 platform to facilitate cloud federation and fog computing", Computer, vol. 48, no. 5, pp. 80–83, May 2015.

[16] W.S.Chin, H.S.Kim,Y.J.Heoand J.W.Jang, "A context-based future network infrastructure for iot services", Procedia Computer Science, vol. 56, pp. 266–270, Jan 2015.

[17] S.Yi, C.Li and Q.Li, "A survey of fog computing: concepts, applications and issues", in Proceedings of the 2015 Workshop on Mobile Big Data. ACM, pp. 37–42, Jun 2015.

[18] "Etsi: Mobile-edge computing," 2014. [Online]. Available: http://goo.gl/7NwTLE

[19] H.Dubey, J.Yang, N.Constant, A.M.Amiri, Q.Yang and K.Makodiya, "Fog data: Enhancing telehealth big data through fog computing," in Proceedings of the ASE BigData&Socialinformatics 2015. ACM, pp. 14, Oct 2015.

[20]M.I.Hussain, "Internet of Things: Challenges and research opportunities", Special Issue ICAC 2016 of CSIT, 2016.

[21]Liu and Wentao. "Research on cloud computing security problem and strategy" In 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), IEEE, pp. 1216-1219, Apr 2012.

[22]Atayero,A.Aderemi,F.Oluwaseyi, " Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 10, pp. 546-552, 2011.

[23]S.Kaur "Cryptography and Encryption In CloudComputing" VSRD-International Journal of Computer Science and Information Technology, vol. 2, no. 3, pp. 242- 249,2012

[24]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, no. 10, pp. 2991-3005, Jul 2016.

[25]Nikam,Rushikesh and M.Potey, "Cloud Storage Security using Multi-Factor Authentication", International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-7, Dec 2016.