Secure Fog Computing System using Emoticon Technique

Harish Kumar, Sampada Shinde, Pratvina Talele
MIT College of Engineering, Pune

***Abstract*—**Fog computing is a distributed computing infrastructure in whichsome application services are provided at the edge of the network in smart devices(IoT devices) and some applications are handled in cloud. Fog computing operates on network ends instead of working entirely from a centralized cloud. It facilitates the operation of storage, compute, analysis and other services between edge devices mostly IoT devices and cloud computing data centres. The main objective of Fog computing is to process the data close to the edge devices .The problem that occurs in Fog is confidentiality and security of data . To overcome this problem, we have proposed the Dual-Encryption to data using Emoticon Technique which is combination of Cryptography and Steganography. In this method, first data is encrypted and then encrypted data is hidden with the cover text like emoticons. So Dual-Encryption enhances data security and reliability. Even if the covered text is accessed by unauthorized person, only encrypted data of original data can be viewed not the actual data.

*****

I. INTRODUCTION

Fog computing is a new technology which extends cloud computing towards the edge of Network [2]. Fog computing machines provide services with reduced latency and improved Quality of Service. In cloud computing concept, all the data produced from the users/edge devices will be directly stored into the cloud and this data is analysed by warehouses for analytical purpose. But in fog computing, the users will be notified about what the actions are needed to be taken on the data and stored it into the cloud.In the fog computing process, applications comes to the data not the data to the applications [1]. Fog computing enables a new set of applications and services also it acts as an interface between the cloud and the fog particularly for data management and analytics.

A. Fog Computing

The Fog acts as an interface between edge devices (IoT) and the cloud which provides necessary extra functionalities for application-specific processing like filtering, extracting and aggregation before transmitting the data to the cloud.

Fog computing is a highly virtualized platform that provides compute, storage, analysis and networking services between edge devices [2]. Fog computing has lots of advantages like widespread geographical distribution of data, information about the physical location of a device to another application or user, requires less time(low latency), heterogeneity, mobility support, the predominant role of wireless access, the strong presence of streaming and real-time applications, the orchestration of large scale control systems, hierarchical networking, and computing structures.

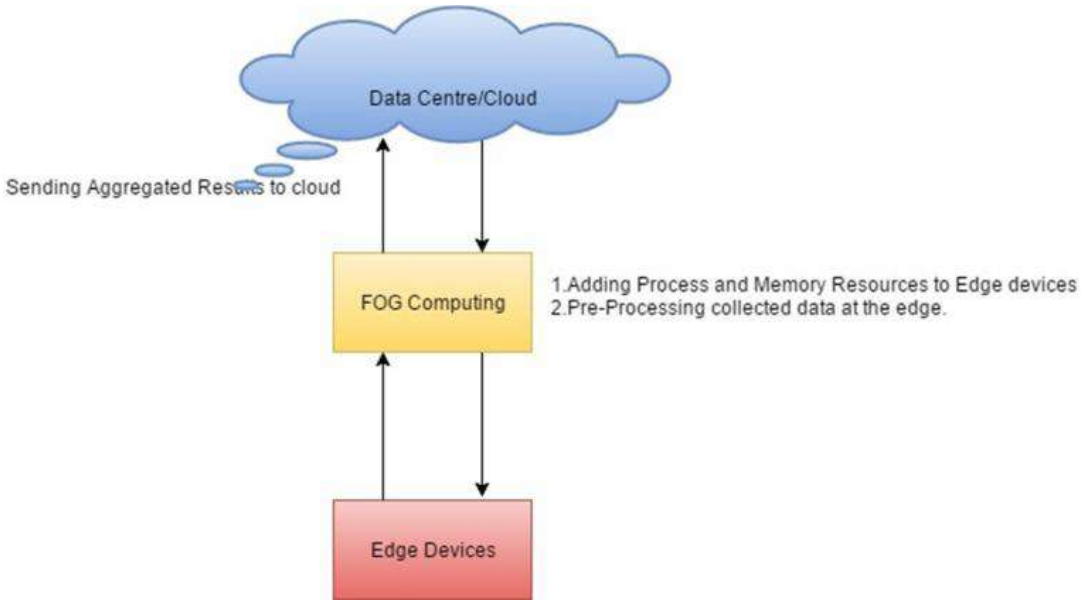

Fig. 1.Fog Computing as an interface between edge devices and cloud

B. Fog Engines

Fog-engine provides real time data analytic as well as facilitates edge devices (IoT) to communicate with each other and with the cloud. Fog-engine can be modified according to the application and agile to heterogeneous platform that is integrated to an IoT device [2]. It allows data processing in the cloud and in the distributed grid of connected IoT devices located at the network edge. It expedite for offloading data and interacting with the cloud as a gateway [2].

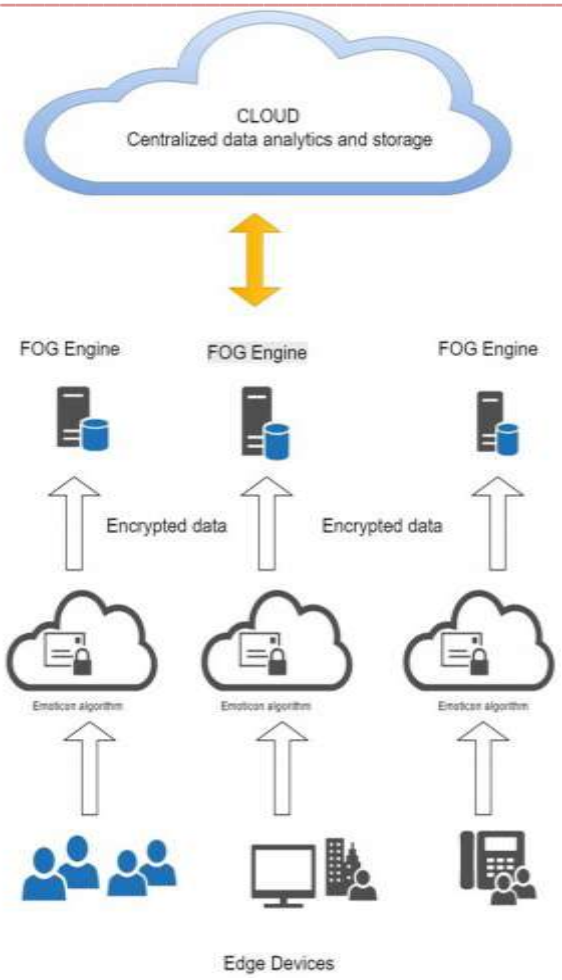

Fig. 2.Fog Engine in Cloud Based Computing System

C. *Data Security*

In Fog computing, there are many security issues and even the encryption of data is not safe method [1].Security and privacy should be maintained in every layer while designing Fog computing system [3]. Data theft attacks is major issue in fog computing. If an unauthorized person is an insider then the chances of data being misused are more. We have to provide high level of data security in Fog computing system.

II. LITERATURE SURVEY

A. *Big Data*

Big data refers to the substantial amounts of unstructured, semi structured or structured data that flows continuously through and around consortium, including text, video, data from sensors, and transactional records [2]. Big data analytics describes the process of performing complex analytical tasks on data that typically includes grouping, aggregation, or iterative processes [2].Data which is generated from Internet of Things or edge devices will grow exponentially as the number of connected nodes increases.

Figure.3 provides an overview of a flow of data analytics in Fog engine. The first step is to perform collection of data from edge devices or Internet of Things. Data cleaning is the next step which is used to reduce the data size by removing redundant information which enhances data analytics and processing speed. Data cleaning also detects and corrects errors and any inconsistencies from data to improve its quality of service[2].Data is analysed depending upon users request or query and based on the results many decisions or interpretation could be performed.

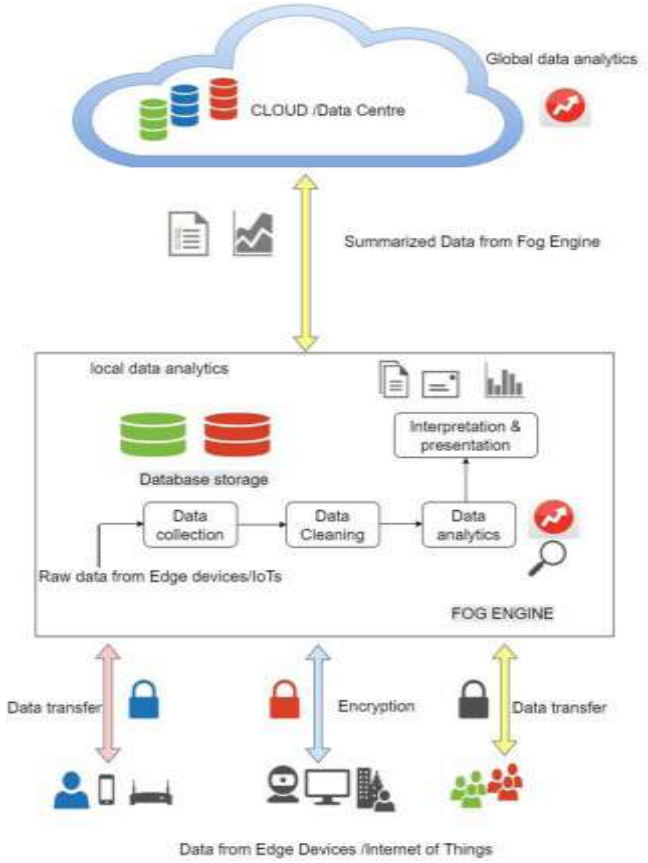

Fig. 3.Big Data Analytics in Fog Computing System

In Fog computing system, instead of sending all data received from edge devices or IoT to the cloud, only summarized result of a data is sent to the cloud. Fog engine receives all the data from edge devices or IoT, and it is responsible for performing local data analytics near the data source itself rather than sending it to cloud. Fog engine performs all the major functions of Big data. As the data is pre-processed, filtered and cleaned in the Fog engine itself before offloading the data to the cloud, the amount of data which is being carried is lower than the data produced by edge devices or IoT's. Fog engines provides a very limiting enumerating power and storage capacity as compared with cloud but Fog engine offers high level of fault tolerance and can be integrated with mobile IoT nodes or edge devices.

B. *Problem Statement*

Security is one of the major concerns because there are lots of sensitive data around us. It could be any company pricing details, or even it could be national secret. All thedata must be secured and should make sure that it has all necessary methods in it, which makes an attacker difficult to crack the key. This paper primarily concentrates on security and privacy of data as

key part. In the system of cloud, though secured data is sent to the fog from cloud, predicting the security threat in the fog such as man in the middle attacks, we would like to add a second layer of security within the level of fog.

C. *Existing Solution*

In fog at present AES encryption algorithm is considered as an exemplary Advanced Encryption Standard(AES) algorithm consisting data encryption in first phase and forwarding corresponding data to fog engine for further analysis in second while in third phase it offers decryption of encrypted data using fog engine to get valid data [1].

For encrypting the data AES algorithm requires more processing time along with complex security overhead. This algorithm is efficient but does not provide preservation and complex privacy of data

III. PROPOSED SOLUTION

To avoid the above problem a solution is introduced by putting forward Emoticons technique where two layer encryption is provided. In this approach, the emoticons which are generally used in chats, short message services and comments, are used as cover media to deliver the data in a hidden manner [4]. The emoticon is a type of icons or pictorial representation of text that interprets a user's perception and reflex in text mode as shown in Figure. 4. These are popularly used icons especially where there is a restriction on the number of characters.

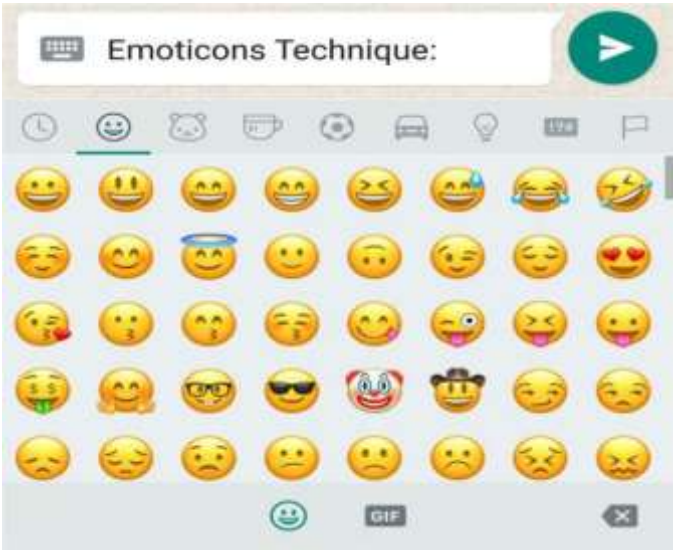

Fig. 4.Emoticons used for Encryption

Initially the data is collected by edge devices. Before transmitting the data to the Fog Engine, the data is encrypted using emoticon technique. In first phase, data is encrypted using Cryptography, where data is transmitted in particular form. And these encrypted data will be input to second phase of emoticon technique. In second phase, encrypted data is hidden behind the cover media that are the emoticons. Again these emoticons are put into cover text which finally generates stego text to be transmitted.

The receiver on the other end receives the stego text then first extracts the emoticons from the cover text and then maps the meaning of each emoticon to get the encrypted message. Then the authorized user can decrypt the message using their own private key to decrypt the message to finally get the actual data.

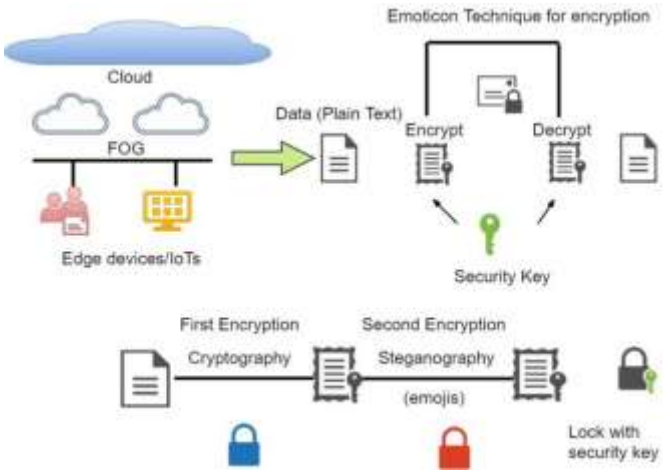

Fig. 5.System architecture using Emoticon Technique for Encryption

IV. ADVANTAGES AND LIMITATIONS

In this technique, first data is Encrypted and then hiding the encrypted data with the cover text like emoticons makes nearly impossible to access the data. So, even if the covered media is accessed by attacker, only encrypted data of original message can be viewed. Hence by adding encryption to already encrypted data ensures confidentiality of the communication and increases reliability.

The only limitation of proposed method is that, it requires lots of memory since encrypting the data using cover text (emoticons) requires additional memory.

V. CONCLUSION

This paper focuses on Data Security. We proposed Emoticon Technique for Encryption of Data in Fog Computing which is a combination of Cryptography and Steganography which is in progress. It adds a second layer of data security and provides high complex security of data.

VI. REFERENCES

[1] Akhilesh Vishwanath, RamyaPeruri, Jing (Selena) He, "Security in Fog Computing through Encryption", International Journal of Information Technology and Computer Science (IJITCS), Vol.8, No.5, pp.28-36, 2016. DOI: 10.5815/ijitcs.2016.05.03

[2] F. Mehdipour, B. Javadi and A. Mahanti, "FOG-Engine: Towards Big Data Analytics in the Fog," 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber

Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Auckland, 2016, pp. 640-646.

[3] Yi S., Qin Z., Li Q. (2015) Security and Privacy Issues of Fog Computing: A Survey. In: Xu K., Zhu H. (eds) Wireless Algorithms, Systems, and Applications. WASA 2015. Lecture Notes in Computer Science, vol 9204. Springer, Cham

[4] Miss. Madhura A. Bhoi, Miss. Barkha V. Budhwani, Miss. Poonam R. Dhayagode, Miss. Tahurafeeza J. Sayyed, Miss. PratvinaTalele, "Data Hiding using Emoticons", December 16,Volume 4 Issue 12 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 54 – 56