Fog Computing: Security and Role in Internet of Things (IOT)

Selwyn Paul. J
Assistant Professor,
Dept. of Computer Science,
St. Joseph's College (Autonomous),
Bangalore.

C. N. Prasad
Assistant Professor,
Dept. of Computer Science,
St. Joseph's College (Autonomous),
Bangalore.

Ravi Kumar. D
Scholar,
Dept. of Computer Science,
St. Joseph's College
(Autonomous),
Bangalore.

***Abstract*-- Fog computing is paradigm which is extended the version of Cloud computing paradigm. Cloud computing is a network based environment; it is used as a delivery platform for sharing data and provides a secure access to personal and business information. But it involves in risk like Data theft attack is one of the security challenge in the Cloud computing. data theft attacks by this, intruders can take a look into documents which can be highly confidential data for illegal purposes .To overcome this problem new pattern called Fog computing can be used . This technique can monitor the user activity to identify the legitimacy and prevent from any unauthorised user access .similar to cloud; Fog provides data compute, storage and application services to end users.**

Keyword: Internet of Things (IoT), Cloud computing, Fog computing, Decoy technology, Data security

I. INTRODUCTION

Nowadays Cloud computing is achieving popularity because of its ease of usage and storage which is provided to users for personal and business purposes is increasing its demand. Software companies and other agencies are shifting more towards cloud computing environment. To achieve better operational efficiency in many organizations and small or medium agencies is using Cloud environment for managing their data. Cloud Computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (**SOA**). Cloud Computing provides an easy way for accessing, managing and computation of user data, but it also has some severe security risks. Data theft attacks are amplified if the attacker is a malicious insider. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance [1].

The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed .The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents hosted on Google's infrastructure as Google Docs .The damage was significant both for Twitter and for its customers[2]. Many researches took place in cloud computing securing for preventing unauthorized and illegal access to data, by developing encryption mechanism. This mechanism failed from protecting data. To overcome problem of preventing data theft attacks new technology called Fog computing, it is a paradigm which monitors the data and help in detaching unauthorized access. As in cloud, Fog computing also provides data computing, storage, and application services to end users. According to architecture fog is situated below the cloud at the ground level. The difference is Fog provides proximity to its end users and also supports mobility. Set up box or access point are used as end devices to host services at the network, these end devices are also termed as edge network. The main task of fog is to deliver data and place it closer to the user who is positioned at a location which at the edge of network. Here edge refers to different nodes to which the end user is connected and it is also called edge computing.

II. OVERVIEW OF FOG COMPUTING

The term Fog computing has been embraced by Cisco that refers to extending paradigm of cloud computing to Edge Computing or fogging. It is a highly virtualized platform that provides computation, storage, and networking services between end devices and traditional cloud servers

Cisco introduced its fog computing vision in January 2014 as a way of bringing cloud computing capabilities to the edge of the network and as a result, closer to the rapidly growing number of connected devices and applications that consume cloud services and generate massive amounts of data.

By handling these services that make up the Internet of Things (**IoT**) at the network edge, data can in many cases be processed more efficiently.

III. FEATURES OF FOG COMPUTNG

Some of the features of fogging are mentioned below:

1. Edge location, location alertness.
2. Wide range of geographical distribution.
3. Very large number of available nodes.
4. Mobility maintenance
5. Real-time communications
6. Majority of wireless access.
7. Heterogenitic nature.

IV. ADVANTAGES & DISADVANTAGES

Advantages are as follows:

1. Fog application decreases the amount of data to be moved, distance that data must move and the network traffic, thus limiting cost of transmission, latency and improving the quality of services (QoS) [2].
2. Eliminates the core computing environment, there after reducing a major block and a point of failure.
3. Improves the security, as data's are encoded as it is moved towards the network edge.
4. Ability to virtualize, henceforth extending the scalability.
5. Consumes less amount of band width.

Disadvantages include:
Introduces certain demerits on the selections of technology platforms,web applications or other services.

V. APPLICATIONS

Fog computing based systems are becoming an important class of **IoT.**

Augmented Reality (AR)
Augment reality applications are popular on smart phone, tablet and smart glasses by overlaying an informative view on the real world. AR applications usually need high computation power to process video streaming and high bandwidth for data transmission. For example, a normal AR application needs to process real time video frame using computer vision algorithm and at the same time process other inputs such as voice, sensor and finally output timely informational content on displays. A processing delay of more than tens of milliseconds will ruin the user experience and leads to negative user feedback. AR system supported by fog computing can maximize throughput and reduce latency in both processing and transmission.

Smart Grid.
Energy load balancing applications may run on network edge devices, such as smart meters and micro grids. Based on energy demand, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind. Fog collectors at the edge process the data generated by grid sensors and devices, and issue control commands to the actuators. They also filter the data to be consumed locally, and send the rest to the higher tiers for visualization, real-time reports and transactional analytics [3].

Decentralized Smart Building Control.
The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements. Sensors will use distributed decision making and activation at Fog devices to react to data. The system components may then work together to lower the temperature inject fresh air or open windows.

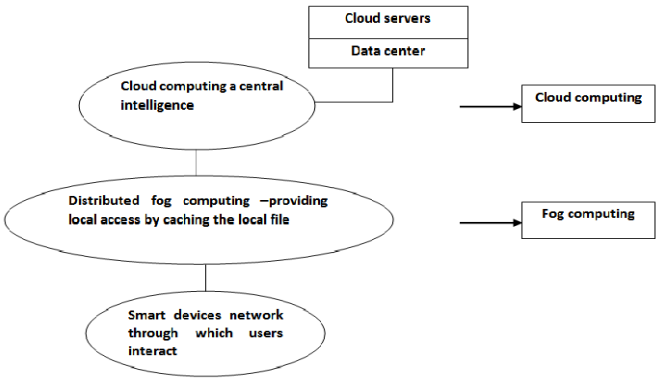
Smart Traffic Lights.
Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic.

Real-time video analytics.
Largely-deployed camera sensors in city or along the road are important component of smart city and smart connected vehicle to support surveillance, management etc. Fog computing can provide resource of computation and storage to store captured video streams, transcode and process video frame for tasks such as object recognition, object tracking and data mining etc. After that we can just send out notification, events, description or video summary to end users, central servers or databases. With the help of fog, we can achieve real-time processing and feedback of high-volume video streaming and scalability of service on low-bandwidth output data. Privacy-preserving techniques can also be applied at the fog side, to ease the concern of personal privacy leakage in public surveillance systems [4].

Smart Train maintenance.
Smart Sensors on self-maintaining trains monitor train components. If they detect any manor problem or trouble, they send an automatic message to the train operator mentioning that so and so component is in trouble, trains location , next station so stop train at the next station for emergency maintenance.

Connected Vehicles (CV) The Connected Vehicle distribution displays a rich setup of connectivity and interactions: cars to cars, cars to access points (Wi-Fi, 3G, smart traffic lights), and access points to access points [2].

VI. ARCHITECTURE OF FOG COMPUTING.



In the architecture of fog computing, we are explaining, how cloud is involved in central intelligence along with cloud servers and data center.

It includes various components and sub components of cloud and fog that builds the structure of the system. This architecture can be classified into two sections:

- Front end
- Back end

The front end and back end is interlinked to each other via virtual network or the internet. Besides, there are other components like Middleware, Cloud Resources etc., that is included in the Cloud computing architecture.

Front end provides interface for the client, customer or the user. It includes the client's computer system or network that is used for accessing the fog system. Different Computing system has different user interfaces. For email programs, the support is given from web browsers like Chrome, and Internet Explorer etc. On the other hand, for other systems there are unique applications shared between the client and the service provider.

Back end is the side used by the service provider. It includes various servers, computers, data storage systems, virtual machines etc, that builds together the fog of computing services. This system can include different types of computer programs. Each application in this system is managed by its own dedicated server. The back end side has some responsibilities to fulfil towards the client [5].

- To provide security mechanisms, traffic control and protocols.
- To employ protocols that connects networked computers for communication.

Protocol

One central cloud server is used to manage the entire fog Computing system. This server is responsible for monitoring the traffic and makes sure each process is run without any interrupt. This process is followed with a fixed set of rules called Protocols. Also, unique software called Middleware is used to perform the processes. Middleware connects networked computers to each other.

Whereas fog Computing is having an access of caching technique with the help file structure along with the network interaction between the users and smart sensors.

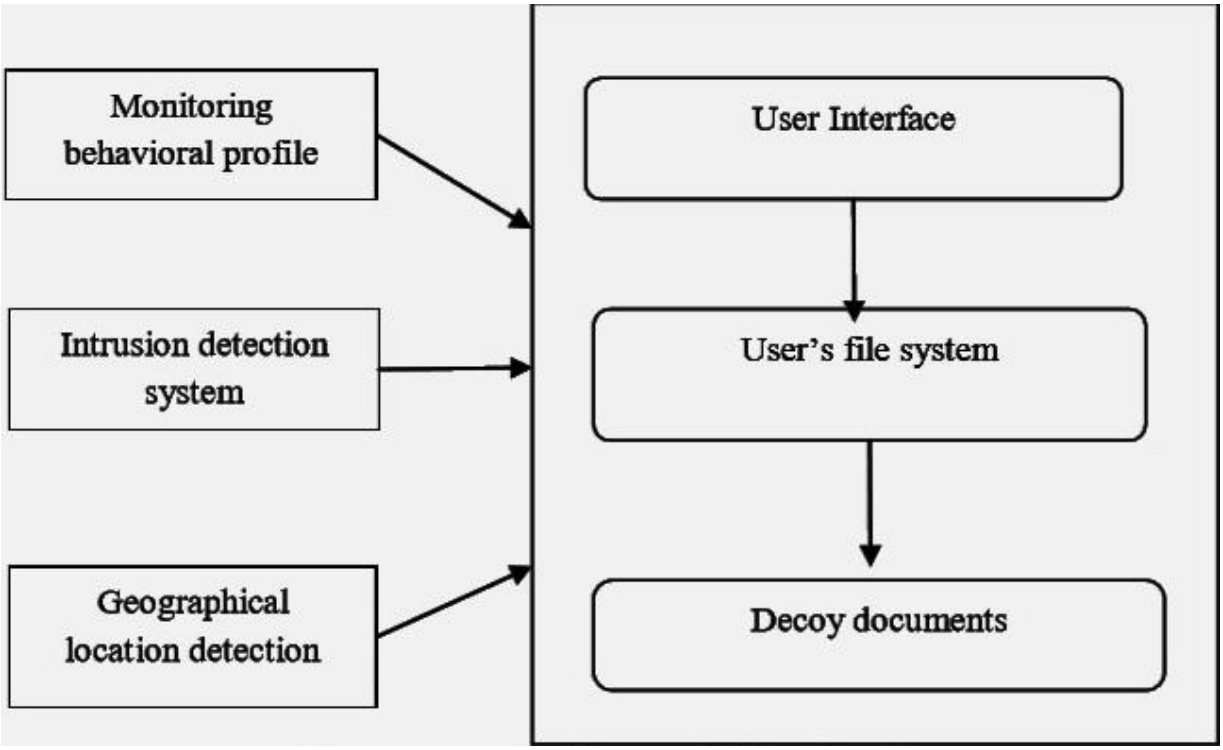
With a fully developed fog computing architecture, customers and solution providers across industries can develop, manage, and run software applications directly on industrial networked devices. This includes hardened routers, switches, and IP video cameras [6].

VII. SECURING CLOUDS USING FOG.

There are various ways to use cloud services to save or store files, documents and media in remote services that can be accessed whenever user connect to the Internet. The main problem in cloud is to maintain security for user data. There are various methods to secure remote data in cloud using standard access control and encryption methods. But these mechanism lead to failed from time to time. We can achieve this through a "preventive" decoy (disinformation) attack. We can secure Cloud services by implementing given additional security features [7][8].

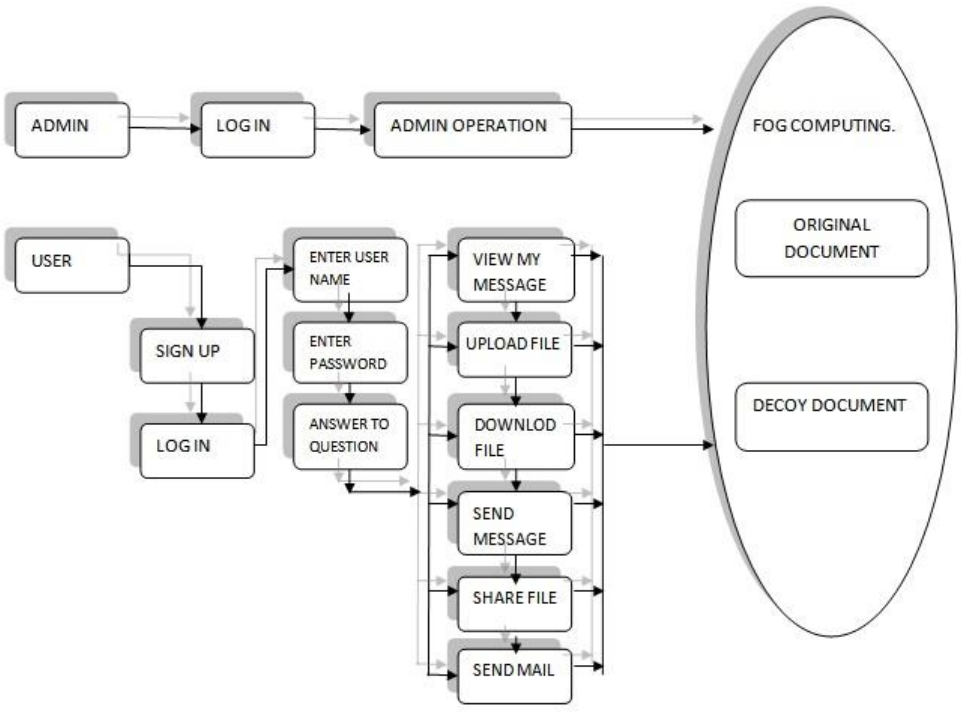
Decoy Technology.

On demand machine generated document it contains the content to attack the attacker into stilling the bogus information. Decoy files or documents are trap files which not useful for the legitimate (owner) users but act as trap for illegitimate users (attacker).The file system has files and folders in which trap files are also placed to detect that the user is legitimate or an attacker. Decoy will confuse the attacker into believing they have ex-filtered useful document, when they are not. when an attacker will enter into the system the search behaviour will be random and if any trap is hit by that user then the pattern will change thus any change in usual behaviour of the user will be detected and but if the trap is hit by owner by mistake then by answering some secret challenge questions the owner can be checked. Further, the diagram of high level security architecture makes the procedure clear[8].



Component architecture of high level security

VIII. FOG COMPUTING.



Working of Fog Security

states the actual working of the fog computing .In two ways login is done in system that are admin login and user login .When admin login to the system there are again two steps to follow:

step1: Enter user name.
step2: Enter the password.

After successful login of admin he can perform all admin related tasks, but while downloading any file from fog he have to answer the security Question if he answer it

correctly then only original file can be download. In other case, when admin or user answer incorrectly to the security question then decoy document is provided to the fake user. Decoy technology work in the given manner if you have any word ,suppose "MADAM" in the document then some alphabets are replaced as M->A then the given word become "AADAA" which have no meaning. In some Case, if attacker getting to know that „M‟ is replaced by „A‟ in the given document and by applying reverse engineering he get result as "MMDMM"[10]. In any case he can't judge content of document.

When user login to the system he also have to follow the same procedure as admin. Operations like upload files/documents, download files/documents, view alerts, send message, read message, broadcast any message all these can be perform by the user. ALERT this stream provide the detail knowledge of attack done on their personal file/document with details like date, time, no of times the attacker trying to hack that file/document .Best thing of fog Computing is after each successful login the user get SMS on the mobile that „login successful‟. from this the user get alert when other else trying to gain access to his/her personal fog account and when attacker trying to download some files/documents then user also get SMS that contain attacker IP-address, attacker's server name, date, time details on his/her mobile so that become easy to catch attacker by tracing all these things[9].
In this way fog computing is more secure than the traditional cloud computing.

IX. CONCLUSION

In this paper, we have analysed Fog Computing and its real time applications .Fog computing has the ability to handle the data tsunami created by Internet of Things. Different approach for securing personal and business data in the cloud. We propose a system to prevent data access patterns by profiling user behaviour to establish if and when a wicked insider criminally accesses someone documents in the cloud services. The decoy technology allows the use to keep decoy information or dummy information in the file system to mislead insider data theft attackers. Use Fog computing for optimizing the website performance. We hope that by continuing this work using Fog Computing platforms can lead to improved defensive techniques and would contribute in increasing the level of security if user data on the cloud.

X. REFERENCE

[1] http://www.webopedia.com/TERM/F/fog-computing.html.
[2] https://www.erpublication.org/admin/vol_issue1/upload%20Image/IJETR031426.pdf
[3] http://www.ijarcsse.com/docs/papers/Volume_4/6_June2014/V4I6-0126.pdf
[4] http://esatjournals.net/ijret/2014v03/i09/IJRET20140309018.pdf
[5] http://www.goldmansachs.com/our-thinking/pages/iot-meets-clean-tech.html?cid=PS_02_64_07_00_01_15_01
[6] http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf
[7] http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf
[8] http://www.ieee-security.org/TC/SPW2012/proceedings/4740a125.pdf
[9] https://techradar.cisco.com/technology/fog-computing
[10] http://www.slideshare.net/nullhyd/decoy-documents