IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Decoy Technology in Fog Computing

Arwinder Singh[1], Abhishek Gautam[2], Hemant Kumar[3], Er. C.K. Raina[4]

CSE Department, Adesh Institute of Technology, Gharuan, Punjab, India[1,2,3]

HOD, CSE Department, Adesh Institute of Technology, Gharuan, Punjab, India[4]

Abstract: Fog Computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. The motivation of Fog computing lies in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. In this paper, we proposed a system for securing data stored in the cloud using decoy technology. In this we monitor data access in the cloud and detect abnormal data access. When unauthorised access is detected that users, activity will be tracked in log details table. Based on the activities performed by unauthorized user. Admin can have blocked or delete that user. When a new user enters into this System, he has to register first. After successfully registered, that user will get a key through mail. And during login, if the user enters wrong password continuously more than three times, he will get access and his activity will be tracked on log details table in the database. And after this, whatever activities he is doing that also will be tracked in the log table. If he downloads any file, he won't get original file. Instead of that he will get decoy file. If a user entered correct password and he will get access. If that user wants to download any file, and he entered wrong key more than three times, in first three cases in the action column invalid will be entered and in the fourth case wrong key and that user will get decoy file. In every case, it Now will execute user behaviour algorithm. When a user edit password, he enters wrong key more than three times, then user will get message that password updated successfully. But in actual case it is not updating.

Keywords: FOG computing, Cloud computing, Decoy, Cisco, edge of network, Cloud Security.

I. INTRODUCTION

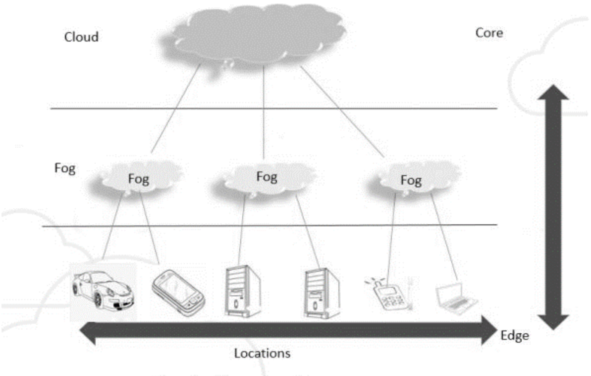
The term "fog computing" or "edge computing" means that rather than hosting and working from a centralized cloud, fog systems operate on network ends. It is a term for placing some processes and resources at the edge of the cloud, instead of establishing channels for cloud storage and utilization.

Fog computing tackles an important problem in cloud computing, namely, reducing the need for bandwidth by not sending every bit of information over cloud channels, and instead aggregating it at certain access points. This type of distributed strategy lowers costs and improves efficiencies. More interestingly, it's one approach to dealing with the emerging concept of Internet of Things (Iot).

Fog computing extends the cloud computing paradigm to the edge of the network to address applications and services that do not fit the paradigm of the cloud due to technical and infrastructure limitation including:

- Applications that require very low and predictable latency
- Geographically distributed application
- Fast mobile applications
- Large-scale distributed control systems

In fog computing data collected by sensors are not sent to cloud server instead it is sent to devices like network edge or set top box, routers, access point for processing thus by reducing the traffic due to low bandwidth as shown in Figure 1.1. Fog computing improves the Quality of service and also reduces latency.



Three level hierarchy in fog computing

Small computing works are locally processed and responses are sent back to the end users without the use of cloud. So, fog computing is emerging as a better option than cloud computing for smaller computing works. Fog computing plays an important role by reducing the traffic of data to the cloud. Since fog system is placed near to the data sources computation and communication are not delayed. The need for Fog Computing can be felt from the example of a jet engine. Whenever the jet engine is connected to the internet, half an hour running time of the jet engine creates 10 TB of data. This huge data itself will create a big traffic in the bandwidth which cannot be neglected. So, comes the importance of fog computing. Fog computing is complementary to cloud. Certain features of fog computing differentiate it from cloud, Fog

DOI10.17148/IJARCCE.2017.63188

Computing is used for real time interactions but cannot totally replace cloud computing as it is preferred for high end batch processing. As the name suggests cloud system is placed at a distant whereas the fog system is placed locally near to the end user.

2. LITERATURE SURVEY

2.1. EXISTINGCLOUD COMPUTINGSYSTEM

First, Cloud Computing has provided many Opportunities for enterprises by offering their customers a range of computing services. Current "Pay-as-you-go" cloud computing model becomes an efficient alternative to owning and managing private data centres for Customers facing Web Applications.

Fig 2.1 Cloud Computing System

Disadvantages: -

- Existing data protection mechanisms such as encryption was failed in securing the data from the attackers.
- It does not verify whether the user was authorized or not.
- Cloud computing security does not focus on ways of secure the data from unauthorized access.

2.2. THREATS IN CLOUD:

1. Data breaches – This led to the loss of personal data and credit card information of about 110 million people, it was one of the theft during processing and storage of data.
2. Data loss – Data loss occurs when the disk drive dies without any backup created by the cloud owner. It occurs when the encrypted key is unavailable with the owner.
3. Account or service traffic hijacking – Account can be hacked if the login credentials are lost.
4. Insecure API's – Application Programming Interface controls the third party and verifies the user.
5. Denial of service – This occurs when millions of users request of same service and the hackers take this.
6. Malicious insiders – This occurs when a person close to us knows our login credentials.
7. Abuse of cloud services – By using many cloud server's hacker can crack the encryption in very less time.
8. Insufficient due diligence- Without knowing the advantages and disadvantages of the cloud many businesses and firms jump into cloud thus leading to data loss
9. Shared technology – This occurs when the information is shared by the many sites.

2.3. NEED OF FOG COMPUTING

Fog Computing enables a new breed of applications and services, and that there is a fruitful interplay between the Cloud and the Fog, particularly when it comes to data management and analytics. Fog Computing extends the Cloud Computing paradigm to the edge of the network. While Fog and Cloud use the same resources (networking, compute, and storage), and share many of the same mechanisms and attributes (virtualization, multi-tenancy) The Fog vision was conceived to address applications and services that do not fit well the paradigm of the Cloud.

They include:

- ✓ Applications that require very low and predictable latency the Cloud frees the user from many implementation details, including the precise knowledge of where the computation or storage takes place. This freedom from choice, welcome in many circumstances becomes a liability when latency is at premium (gaming, video conferencing).
- ✓ Geo-distributed applications (pipeline monitoring, sensor networks to monitor the environment). • Fast mobile applications (smart connected vehicle, connected rail).
- ✓ Large-scale distributed control systems (smart grid, connected rail, smart traffic light systems).

2.4. PROPOSED FOG COMPUTING SYSTEM

Unlike traditional data centers, Fog devices are geographically distributed over heterogeneous platforms, spanning multiple management domains. Cisco is interested in innovative proposals that facilitate service mobility across platforms, and technologies that preserve end-user and content security and privacy across domains

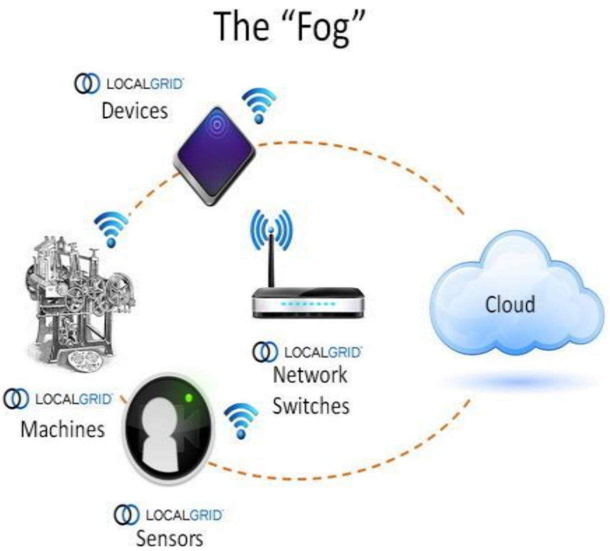


Fig 2.2 Fog Computing System

Advantages: -

- Fog can be distinguished from Cloud by its proximity to end-users.
- The dense geographical distribution and its support for mobility.
- It provides low latency, location awareness, and improves quality-of-services (Qos) and real time applications.

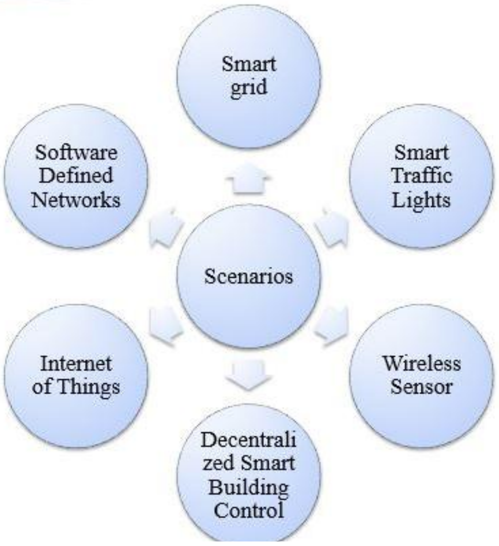


Fig. 2.3. Advantages

2.5. ARCHITECTURE.

Fog computing extends the cloud-based Internet by introducing an intermediate layer between mobile devices or the end user device and cloud, aiming at the smooth,low-latency service delivery from the cloud to smart device. This accordingly leads to a three hierarchy Mobile-Fog-Cloud architecture.

The intermediate Fog layer is composed of geo-distributed Fog servers which are deployed at the edge of networks, e.g., parks, bus terminals, shopping centres, etc. Each Fog server is a highly-virtualized computing system, similar to a lightweight cloud server, and is equipped with the on-board large- volume data storage, compute and wireless communication facility.

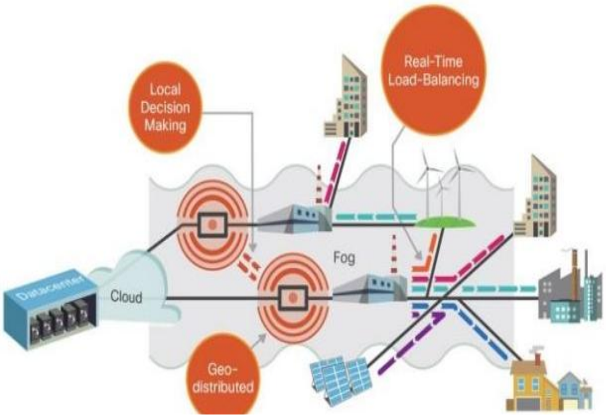


Fig. 3.1 Architecture

The role of Fog servers is to bridge the mobile users and cloud. On one hand, Fog servers directly communicate with the mobile users through single-hop wireless connections using the off-the-shelf wireless interfaces, such as Wi-Fi, Bluetooth. With the on-board compute facility and precached contents, they can independently provide pre-defined service applications to mobile users without assistances from cloud or Internet. On the other hand, the Fog servers can be connected to the cloud so as to leverage the rich functions and application tools of the cloud. To summarize, the purpose of Fog computing is to place a handful of compute, storage and communication resources in the proximity of mobile users, and therefore to serve mobile users with the local short-distance high-rate connections. This overcomes the drawback of cloud which is far to mobile users with elongated service delays. Therefore, the fog is interpreted as the cloud close to the ground.

2.6. CLOUD VS FOG COMPUTING

Cloud vs Fog computing		
Requirements	**Cloud Computing**	**Fog Computing**
Latency	high	low
Delay jitter	High	Very low
Location of server nodes	Within internet	At the edge of local n/w
Distance between the client and server	Multiple hops	One hop
Security	Undefined	Can be defined
Attack on data in router	High probability	Very Less probability
Location awareness	No	Yes
Geographical distribution	Centralized	Distributed
No. of server nodes	Few	Very large
Support for Mobility	Limited	Supported
Real time interactions	Supported	Supported
Type of last mile connectivity	Leased line	Wireless

2.7. Simple implementation of Fog Computing

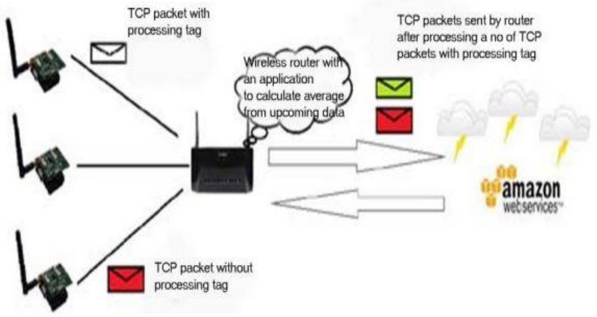

TCP packet with processing tag
Wireless router with an application to calculate average from upcoming data
TCP packets sent by router after processing a no of TCP packets with processing tag
amazon webservices
TCP packet without processing tag

Fig 3.1

DOI10.17148/IJARCCE.2017.63188

Figure shows a setup where many wireless sensor nodes keep uploading their day to day temperature reading to the cloud.

A node which wants to send only an average of its operational data to the cloud tags its packets, these packets are processed by the intermediate wireless router, the wireless router after processing uploads the data to the cloud. Untagged packets are sent directly to the cloud without any intermediate processing.

The sensors (Arduino boards) tags the temperature data packets.

On receiving the temperature data packets the raspberry pi (The Fog Network device) stores the temperature data and does a time series prediction on the data, the predicted data is then sent to the cloud, so that the cloud can display it on a webpage.

2.8. CHARACTERISTICS OF FOG COMPUTING

Defining characteristics of the Fog Computing are:

- Proximity to end-users, its
- Dense geographical distribution
- Support for mobility.

Fog reduces service latency, and improves QoS (Quality of Service), resulting in superior user-experience. Fog Computing supports emerging Internet of Everything (IoE) applications that demand real-time/predictable latency (industrial automation, transportation, networks of sensors and actuators). Fog paradigm is well positioned for real time Big Data and real time analytics, it supports densely distributed data collection points, hence adding a fourth axis to the often-mentioned Big Data dimensions (volume, variety, and velocity).

Unlike traditional data centres, Fog devices are geographically distributed over heterogeneous platforms, spanning multiple management domains. That means data can be processed locally in smart devices rather than being sent to the cloud for processing.

2.8.1. Fog Players:Providers and Users

It is not easy to determine at this early stage how the different Fog Computing players will align. Based on the nature of the major services and applications, however, we anticipate that:

- Subscriber models will play a major role in the Fog (Infotainment in Connected Vehicle, Smart Grid, Smart Cities, Health Care, etc.)
- The Fog will give rise to new forms of competition and cooperation between providers angling to provide global services. New incumbents will enter the arena as users and providers, including utilities, car manufacturers, public administrations and transportation agencies.

2.9. APPLICATIONS OF FOG COMPUTING

We elaborate on the role of Fog computing in the following motivating scenarios. The advantages of Fog computing satisfy the requirements of applications in these scenarios.

2.9.1. Smart Traffic Lights and Connected Vehicles:

Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles. Intelligent lighting turns on once a sensor identifies movement and switches off as traffic passes. Neighbouring smart lights serving as Fogdevices coordinate to create green traffic wave and send warning signals to approaching vehicles. Wireless access points like Wi-Fi, 3G, road-side units and smart traffic lights are deployed along the roads. Vehicles-to Vehicle, vehicle to access points, and access points to access points interactions enrich the application of this scenario.

2.9.2. Wireless Sensor and Actuator Networks:

Traditional wireless sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors. In this scenario, actuators serving as Fog devices can control the measurement process itself, the stability and the oscillatory behaviours by creating a closed-loop system. For example, in the scenario of self-maintaining trains, sensor monitoring on a train's ball-bearing can detect heat levels, allowing applications to send an automatic alert to the train operator to stop the train at next station for emergency maintenance and avoid potential derailment. In lifesaving air vents scenario, sensors on vents monitor air conditions flowing in and out of mines and automatically change air-flow if conditions become dangerous to miners

2.9.3. IoT and Cyber-physical systems (CPSs):

Fog computing based systems are becoming an important class of IoT and CPSs. Based on the traditional information carriers including Internet and telecommunication network, IoT is a network that can interconnect ordinary physical objects with identified address. CPSs feature a tight combination of the system's computational and physical elements. CPSs also coordinate the integration of computer and information centric physical and engineered systems.

IoT and CPSs promise to transform our world with new relationships between computer-based control and communication systems, engineered systems and physical reality. Fog computing in this scenario is built on the concepts of embedded systems in which software programs and computers are embedded in devices for reasons other than computation alone. Examples of the devices include toys, cars, medical devices and machinery. The goal is to integrate the abstractions and precision of software and networking with the dynamics, uncertainty and noise in the physical environment. Using the emerging knowledge, principles and methods of CPSs, we will be

DOI10.17148/IJARCCE.2017.63188

able to develop new generations of intelligent medical devices and systems,'smart' highways, buildings, factories, agricultural and robotic systems.

3. PROBLEM STATEMENT

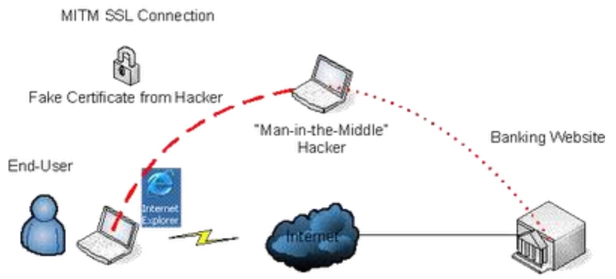
- Analyse the security issues in the fog computing
- We propose a distinct approach to secure cloud known as Fog Computing.
- We use decoy information and user behaviour profiling to secure data on Cloud.

4. SECURITY ISSUES

The main security issues are authentication at different levels of gateways as well as (in case of smart grids) at the smart meters installed in the consumer's home. Each smartmeter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses.

4.1. MAN-IN –MIDDLE-ATTACK

In this subsection, we take man- in-the-middle attack as an example to expose the security problems in Fog computing. In this attack, gateways serving as Fog devices may be compromised or replaced by fake ones.



Man-in-the-middle attack has potential to become a typical attack in Fog computing. In this attack, gateways serving as Fog devices (refer to Figure 6.1) may be compromised or replaced by fake ones.

Examples are KFC or Star Bar customers connecting to malicious access points which provide deceptive SSID as public legitimate ones.

Solution: -Most of the effective defences against MITM can be found only on router or server-side. You won't be having any dedicated control over the security of your transaction. Instead, you can use a strong encryption between the client and the server. In this case server authenticates client's request by presenting a digital certificate, and then only connection could be established. Another method to prevent such MITM attacks is, to never connect to open Wi-Fi routers directly. If you wish to so, you can use a browser plug-in such as HTTPS Everywhere or ForceTLS. These plug-ins will help you establishing a secure connection whenever the option is available.

4.2. DECOY SYSTEM

Decoy data, such as decoy documents, honey pots and other bogus information can be generated on demand and used for detecting unauthorized access to information and to poison the thief's ex-filtrated information. Serving decoys will confuse an attacker into believing they have ex-filtrated useful information, when they have not. This technology may be integrated with user behaviour profiling technology to secure a user's data in the Cloud. Whenever abnormal and unauthorized access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way that it appears completely normal and legitimate. The legitimate user, who is the owner of the information, would readily identify when decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has incorrectly detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver unbounded amounts of bogus information to the attacker, thus securing the user's true data from can be implemented by given two additional security features:

1. Validating whether data access is authorized when abnormal information access is detected
2. Confusing the attacker with bogus information that is by providing decoy documents

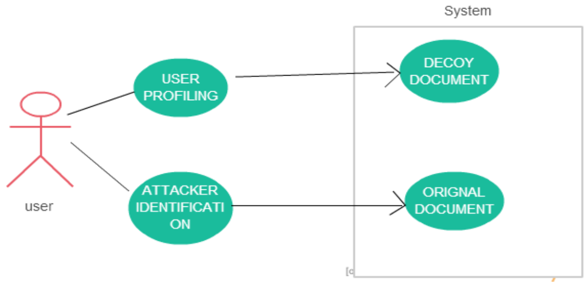


Fig Decoy System

5. PROPOSED METHOD

- We use decoy information and user behaviour profiling to secure data on Cloud.
- The proposed mechanism facilitates security features to data and thereby allows for detection of invalid access.
- It provides prevention to enable valid distribution of data.

5.1. Methodology

There are two main modules:

- User: User can have the following functionalities:

1. Login
2. Edit password
3. Upload files
4. View files and Download
5. Search files
6. Key Recovery.

▪ Admin:Admin can have the following functionalities:

1. Upload decoy-Admin can upload decoy files
2. Manage files
3. Manage users-Can block and delete user based on the activities.
4. User logs-Maintains log details of all users

5.2. Modules:

1. **User Authentication:** The user is facilitated here to authenticate and thus, ensure that only valid users can access the application. But, it also tracks the user login operation and accordingly redirects the user to the decoy application.

2. **Admin Module:** This module facilitates the admin to manage users, the data stored and the invalid activities occurring within the application. Thus, this user will be responsible for tracking the application functionalities. A set of valid access rules will also be defined by the admin for identification of invalid users.

3. **File Access Module:** This module will enable to track whether the search operations executed by the user follow a valid set of operations or not. Accordingly, the system will decide whether the user should be redirected to the decoy environment.

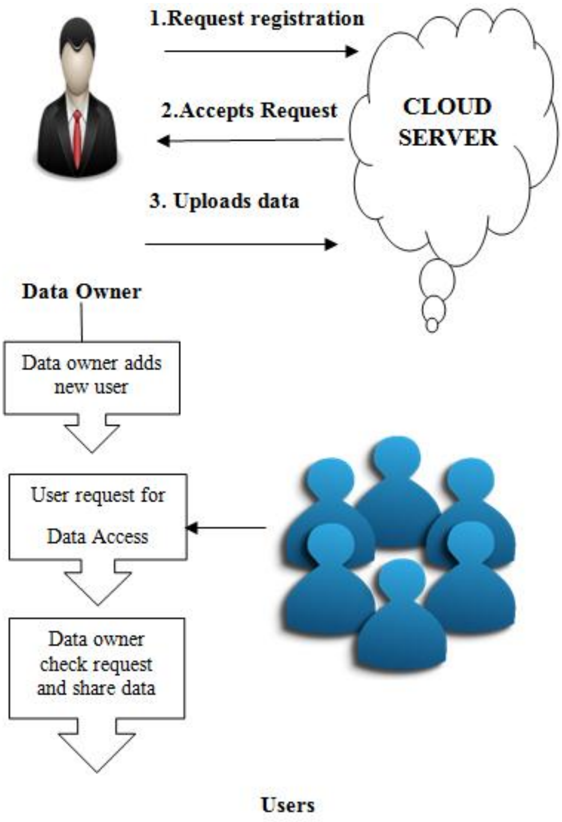
4. **Data Access Module:** The data available for user access will be authenticated using a separate user key specified by the application to the user during registration. Based on the validity of this user key the system will redirect the user to the Decoy Module for tracking and prevent invalid distribution of data.

5. **Decoy Module**: This module will facilitate the system to redirect invalid users to a dummy set of modules wherein invalid data will be distributed to the invalid user and the user activities will be notified to the admin. Thus, the system will not notify the invalid user about the detection of invalid activity and prevent.

6. IMPLEMENTATION & BEHAVIOUR

6.1. Flow of system

- When a new user enters into this System he has to register first. After successfully registration that user will get a key through mail.
- And during login if the user enters wrong password continuously more than three times he will get access and his activity will be tracked on log details table in the database and after this whatever activity he is doing that also will be tracked in the log table. If he downloads any file he won't get original file Instead of that he will get decoy file.
- If a user enters correct password, he will get access. If that user wants to download any file and he enters a wrong key more than three times. In first three cases, invalid entries will be entered in the action column. In the fourth case if wrong key is entered then that user will get decoy file. In every case, it will execute user behavior algorithm.



- When a user edit password, he enters wrong key more than three times, then editpwdwrong key will be entered and user will get message that password updated successfully. But in actual case it is not updating.

6.2. Process Model Used for the Project

A spiral model of software development and enhancement. This model is the iterative model which is used in implementation of this project. Each phase starts with a design goal and ends with a client reviewing the progress thus far project, with an eye toward the end goal of the project.

The steps for Spiral Model can be generalized as follows:

✓ The new system requirements are defined in as much details as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

✓ A preliminary design is created for the new system.

✓ A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

✓ A second prototype is evolved by a fourfold procedure:

▪ Evaluating the first prototype in terms of its strengths, weakness, and risks.

▪ Defining the requirements of the second prototype.

▪ Planning a designing the second prototype.

▪ Constructing and testing the second prototype.

- ✓ At the customer option, the entire project can be aborted if the risk is deemed too great. Risk factors might involve development cost overruns, operating-cost miscalculation, or any other factor that could, in the customer's judgment, result in a less-than-satisfactory final product.
- ✓ The existing prototype is evaluated in the same manner as was the previous prototype, and if necessary, another prototype is developed from it according to the fourfold procedure outlined above.
- ✓ The preceding steps are iterated until the customer is satisfied that the refined prototype represents the final product desired.
- ✓ The final system is constructed, based on the refined prototype.
- ✓ The final system is thoroughly evaluated and tested. Routine maintenance is carried on a continuing basis to prevent large scale failures and to minimize down time.

7. CONCLUSION

We present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service.
Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology could provide unprecedented levels of security in the Cloud and in social networks model.

REFERENCES

[1] http://www.cisco.com/web/about/ac50/ac207/crc_new/university/RFP/rfp13078.html
[2] http://www.howtogeek.com/185876/what-is-fog-computing/
[3] http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1365576
[4] http://a4academics.com
[5] https://en.wikipedia.org/wiki/Cloud_computing
[6] https://en.wikipedia.org/wiki/Fog_computing
[7] https://en.wikipedia.org/wiki/Internet_of_Things
[8] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, USA
[9] Ben-Salem M., and Stolfo Angelos D. Keromytis, "Fog computing: Mitigating Insider Data Theft Attacks in the Cloud," IEEE symposium on security and privacy workshop (SPW) 2012.
[10] Ben-Salem M., and Stolfo, "Decoy Document Deployment for Effective Masquerade Attack Detection," Computer Science Department, Columbia University, New York.
[11] F. Bonomi, "Connected vehicles, the internet of things, and fog computing," in The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011

DOI10.17148/IJARCCE.2017.63188