Handling Attacks by Implementation of FOG Computing  
Ashwini Barik\textsuperscript{1} Amit Dighe\textsuperscript{3} Akshay Pawar\textsuperscript{3} Prasad Yewale\textsuperscript{4}  
\textsuperscript{1,2,3,4}Department of Information Technology  
G.H. Raisoni Institute of Engineering and Technology, Pune

Abstract—“This is move first, Cloud first world and, Everything is becoming digital and software driven”, the statement was first issued by Mr. Satya Nadella when he was appointed CEO of Microsoft. As being stated to be true It is definitely a cloud driven world. Where you mange most of your resources by incorporating with the cloud. But having a cloud or being a part of cloud also involves how you access the resources from cloud. How transparent your cloud in accessing the resources is also play an important role in adding valuation to it. Existing data security mechanisms such as encryption, entrusted third party auditor have failed in preventing masquerade attacks, especially those by an insider to the cloud provider. We propose a different method for securing data in the cloud using decoy or bogus files. We keep track of file access in the cloud and detect anomalous data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user’s real data.

Key words: FOG Computing, Disinformation Attack, Cloud

I. INTRODUCTION
Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. This strategy provides a “fog” of misinformation to protect your sensitive, real information in the cloud. Fog computing refers to the creation of bogus, “decoy” information placed in the cloud along with otherwise true information to hide what is true from what is bogus. We recognize following three needs in order to secure the data in cloud, so that more efficient corrective methods can be employed.(1) First, The problem of providing security to confidential information remains a core.(2) Second, The lack of transparency into has led to more worser and severe data theft attacks.(3) Twitter incident is one example of a data theft attack from the Cloud, where account of US president Mr. Barack Obama was illegally hacked.(4)(5) Third, Monitoring cloud activity and detecting data access changes regularly is not possible. Masquerade attacks are characterized by an adversary stealing a legitimate user's credentials and using them to impersonate the victim and perform malicious activities, such as stealing information. Prior work on masquerade attack detection has focused on pro_ding legitimate user behaviour and detecting abnormal behavior indicative of a masquerade attack.

While this sort of attack was launched by an outsider, stealing a customer’s admin passwords is much easier if initiated by a malicious insider. After stealing a customer’s password and private key, the malicious insider gets access to all customer data, while the customer has no means of detecting this illegitimate access.

Much research in Cloud computing security has focused on ways of preventing unauthorized access to data by developing sophisticated access control and encryption mechanisms is still precarious. However data compromise still a thorn in neck for any legitimate user. It has shown that fully established encryption, often hailed as an alternative to such threats, is not a suffice enough to protect sensitive data when used alone (7).

We propose a completely different method to secure the cloud using decoy methodology, which we have come to term it as Fog computing. We use this technology to launch misleading attacks against malicious insiders, forestalling them from distinguishing the absolute sensitive customer data from pseudo worthless data. In this paper, we propose two ways of using Fog computing to prevent attacks (1) User behavior profiling (2) Decoy technology. The technology that complements our project besides these is the machine learning part, which is implemented using naïve bayes classifier.

II. ARMORING CLOUDS WITH FOG
Numerous recommendations for cloud-based services describe ways to store documents, files, and media in a remote service that may be accessed wherever a user may connect to the Internet. A particularly irking part before such services are broadly accepted concerns guarantees for securing a user’s data in a manner where that guarantees only that user and no other person can gain access to that data.

The problem of providing confidentiality to the information one access remains a core security problem that, to date has not provided the levels of assurance most people desire. Many proposals have been made in order to secure remote data in the Cloud by applying encryption mechanism and standard access control mechanisms. It is fair to say all of the standard approaches have been demonstrated to fail from time to time for a variety of reasons such as malicious insider attacks, mis-configured services, faulty implementations, caboose code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures (8). Building a noteworthy cloud computing environment is not enough, because accidents bound to happen, and when they do, and information gets misplaced, there is no way to get it back. One needs to prepare for such accidents. The following figure shows the proposed diagram of system.
that user is malicious one then it will hide true user’s real files.

For implementing the user behavior profiling we use the data mining algorithm. Data mining algorithm we used for comparing the user behavior profiling of real user and malicious user. For this we use the Naive Bayes classifier algorithm.

In simple terms, a naive Bayes classifier assumes that the presence or absence of a particular characteristics of a class is unrelated to the presence or absence of any other feature, given the class variable. For example, a fruit may be contemplated to be an apple if it is red, round, and about 4” in diameter. Even if these features rely on each other or upon the existence of the other characteristics, a naive Bayes classifier contemplates all of these properties to independently contribute to the probability that this fruit is an apple.

An advantage of the naive Bayes classifier is that it only requires a small amount of training data can be used to estimate the parameters (means and variances of the variables) crucial for classification. Because independent variables are speculated, only the variances of the variables for each class need to be determined and not the entire covariance matrix.

(2) Decoys:
A decoy document is a machine generated document containing content to entice an insider into stealing bogus information. Decoys have a number of properties. They should be believable (so an attacker will consider the document to be real), conspicuous (so an attacker can easily find the decoy), enticing (so that the decoy is attractive and is likely to be opened by the attacker), differentiable by the real user (so the real user knows what is real and what is not) and non-interfering (so that the real user won't accidentally misuse the bogus information contained within the decoy). A legitimate user's private information is better protected if there are a large collection of decoys available to confuse an attacker.

Decoy information, such as decoy documents, honeypots, honeypots, and various other bogus information can be reproduced on demand and serve as a means of detecting anomalous access to information and to adulterate the thief's ex-filtrated information. Serving decoys will flabbergast and perplex an antagonist into believing they have ex-filtrated useful information, when they have not. This technology may be amalgamated with user behavior profiling technology to secure a user’s information in the Cloud. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely appropriate and normal.

Admin in our system uploads the decoy files such as fake data that are randomly created. If the user is predicted that it is abnormal or masqueraded it will hide all real user files and it will only show decoy files uploaded by the admin.

We in our system are using SHA-1 algorithm to calculate digital signature of decoy files and encrypting the passwords of various users. If user click on any file, first it will calculate the digital signature of that file and compare it with digital signature files of decoy database. If it is
matched then it ask for OTP. If it is not matched then requested file is downloaded.

OTP( One Time Password ) is a random string generated by a server using a random string generator function which is sent to the user by email or SMS.

III. RESULT AND CONCLUSION
Hence we implemented security to the cloud database by profiling user behaviour to determine if and when a malicious insider illegitimately accesses someone’s documents in a Cloud service by implementing naïve-bayes classifier algorithm . We Implement Decoy technology stored in the Cloud alongside the user’s real data also serve as sensors to detect unauthorized access. Once illegitimate data access or exposure is identified, and later verified, with challenge questions for instance, we deluge the malicious insider with bogus information in order to dilute the user’s real data. Such preventive attacks that rely on deceptiveness technology, could provide uncommon levels of safety measures in the Cloud and in social networks.

ACKNOWLEDGMENT
We would like to thank Ms. Rekha Jadhav, Department of Information Technology, GHRIET, Pune for their valuable comments and guidance.

REFERENCE