ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Approach to Data Theft Prevention Technique on Clouds using Fog Computing

Rajesh Anand

Assistant Professor, P.G. Department of Computer Sciences, Hindu College, Amritsar, India

ABSTRACT : Cloud Computing is a network based environment that focuses on sharing computations or resources. In cloud customers only pay for what they use and have not to pay for local resources which they need such as storage or infrastructure. So this is the main advantage of cloud computing and main reason for gaining popularity in today's world. Threats against computer networks continue to multiply, but existing security solutions are persistently unable to keep pace with these challenges. To overcome the problem of security we are introducing the new technique which is called as Fog Computing.

Fog Computing is not a replacement of cloud it is just extends the cloud computing by providing security in the cloud environment. With Fog services we are able to enhance the cloud experience by isolating user's data that need to live on the edge. The main aim of fog computing is to place the data close to the end user. Fog Computing places processes and resources at the edge of the cloud. Often on the network devices. While data remains stored in the cloud. This leads to faster processing times and fewer resources consumed. Traditional Cloud computing on the other hand concentrates all applications and data in the cloud.

In this paper i propose a new paradigm for securing data, computational resources in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. Decoys are capable of detecting malicious activities, such as insider and masquerade attacks, that are beyond the scope of traditional security measures. 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. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment.

KEYWORDS*:* Cloud, Cloud Computing, Decoys, Fog Computing.

I. INTRODUCTION

Organizations across the globe are using cloud computing technology to protect their data and to use the cloud resources as and when they need. Cloud Computing provides us a means by which we can access the applications as utilities, over the internet. It allows us to create, configure, and customize the business applications online. The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. Cloud is a subscription based service. Cloud computing is a shared pool of resources. 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. While most Cloud computing customers are well-aware of this threat, they are left only with trusting the service provider when it comes to protecting their data. The lack of transparency into, let alone control over, the Cloud provider's authentication, authorization, and audit controls only exacerbates this threat. Encryption mechanisms not protect the data in the cloud from unauthorized access. As we know that the traditional database system are usually deployed in closed environment where user can access the system only through a restricted network or internet. With the fast growth of World Wide Web user can access virtually any database for which they have proper access right from anywhere in the world. By registering into cloud the users are ready to get the resources from cloud providers and the organization can access their data from anywhere and at any

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

time when they need. But comfortless comes with certain type of risk like security and privacy. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. To overcome by this problem we are using a new technique called as fog computing. Fog computing provides security in cloud environment in a greater extend to get the benefit of this technique a user need to get registered with the fog. once the user is ready by filling up the sign up form he will get the messages or email that he is ready to take the services from fog computing.

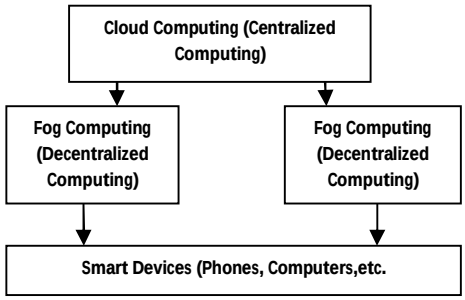


Fig. 1 Cloud Computing &Fog Computing

II. EXISTING SYSTEM

Existing data protection mechanisms such as encryption was failed in securing the data from the attackers. Clouds do not verify whether the user was authorized or not. Cloud computing security does not focus on ways of secure the data from unauthorized access. So, hacker gains access the documents. In year 2010 and 2011 Cloud computing security was developed against attackers. As a consequence, worldwide sale of security software rose by 7.75% in 2011. Yet in spite of the heightened scrutiny that practices have been under, computer crimes continue to flourish, finding of hackers in the cloud. Additionally, traditional security techniques offer no defense against “insider” to protect data in the cloud.

Disadvantages in Existing System

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

III. PROPOSED SYSTEM

This paper proposes completely a new technique to secure user’s data in cloud using user behavior and decoy information technology called as Fog Computing. Decoys are constructs which contain data that appears valuable but is in fact fake. We use these techniques to provide data security in the cloud. Admin monitor data access in the cloud and detect abnormal data access patterns. In this technique when the unauthorized person try to access the data of the real user the system generates the fake documents in such a way that the unauthorized person was also not able to identify that the data is fake or real. It is identified thought a question which is entered by the real user at the time of filling the sign up form. If the answer of the questions are wrong it means the user is not the real user and the system provide the fake document else original documents will be provided by the system to the real user.

Benefits of Proposed System

- Fog can be distinguished from cloud by its proximity to end-users.
- The less frequently and the less distance that data has to travel, the more secure it is. Additionally, there are strict regulatory requirements about where data is stored and accessed.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

- The fake data is provided to the attackers to secure the real user.

IV. SECURING CLOUDS

There are various ways to use cloud services to 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's data in way that guarantees only authenticated users gain access to that data. The issue of providing security to confidential information is core security problem, that it does not provide level of assurance most people desire. There are various methods to secure remote data in cloud using standard access control and encryption methods. It is good to say that all the standard approaches used for providing security have been demonstrated to fail from time to time for a variety of reasons, including faulty implementations, buggy code, insider attacks, misconfigured services, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures. Building a secure and trustworthy cloud computing environment is not enough, because attacks on data continue to happen, and when they do, and information gets lost, there is no way to get it back. There is need to get solutions to such accidents. The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen data to the attacker. We can achieve this through a preventive, Decoy (disinformation) attack. We can secure Cloud services by implementing given additional security features like.

1. Intrusion Detection System
2. Decoy System
3. One time Password System
4. Block the Attacker

1. Intrusion Detection System

Today's enterprise is encountering two types of threats: cyber-attacks and insider threats. Once a cyber-attacker gains trusted access to an environment it is extremely difficult to distinguish his/her activity from a benign user. Insiders have an advantage because they have trusted access to an environment that traditional security solutions are not designed to combat. We can simulate illegitimate logins by taking a session and attributing it to an incorrect source. Behavioral profiling in the online world is a tough task. The suspected cyber criminal cannot be visually seen and/or analyzed for a long period, which is not the case in the physical world. This means that online behavioral profiling is based purely on a limited set of user actions collected by detection systems. That is why current detection systems have opted to analyze normal user behavior, define a normal user profile and then raise a red flag if an action outside of that "normal" profile occurs. User profiling is well known technique that can be applied as system already knows when, how much a user accesses information in the cloud. Such "normal user profile" can be continuously checked to determine whether abnormal access to a user's information is occurring. The current logged in user access behavior is compared with the past behavior of the user. If the user behavior is exceeding the threshold value or a limit, then the remote user is suspected to be anomaly. If the current user behavior is as the past behavior, the user is allowed to operate on the original data. If the current user's behavior seems anomalous, then the user is asked for randomly selected secret questions. If the user fails to provide correct answers for a certain limits or threshold, the user is provided with decoy files. If the user provided correct answers for a limit, the user is treated as normal user. This method of behavior security is commonly used in fraud detection applications.

2. Decoy System

Decoy data, such as decoy documents, honeypots and other false information can be generated on demand and used for detecting unauthorized access to information and to poison the thief's ex-filtrated information. Computers whose primary function is to attach the attention of malicious actors are often called "honeypots". Honeypots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against themselves. Indeed, these systems are created for the sole purpose of deceiving potential attackers. In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honey pots connects several honey pot systems on a subnet, it may be called a honey net. The use of trap based mechanisms as a means for detecting insider attacks is used in general.

Decoy Systems, also known as deception systems, honey-pots or tar-pits, are phony components setup to entice unauthorized users by presenting numerous system vulnerabilities, while attempting to restrict unauthorized access to network information systems. Honey Pot Systems are decoy servers or systems setup to gather information regarding an attacker or intruder into your system. It is important to remember that Honey Pots do not replace other traditional Internet security systems; they are an additional level or system. For each newly created folder or a file, corresponding decoy file will be maintained. The directory and file structure are same for both the decoy file system and the original file system. The information contained in the decoy file is not original.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

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 behavior 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 false information to the attacker, thus securing the user's true data from can be implemented by given two additional security features:

(a) Insuring whether data access is authorized when abnormal information access is detected, and
(b) Mystifying the attacker with false information that is by providing decoy documents.

On applying above concepts to detect unauthorized data access to data stored on local file system by attackers who view of legitimate users after stealing their credenitials. Experiment results in a local file system setting show that combining both techniques can yield better detection result. This result suggests that this approach may work in Cloud environment, to make cloud system more transparent to the user as a local file system.

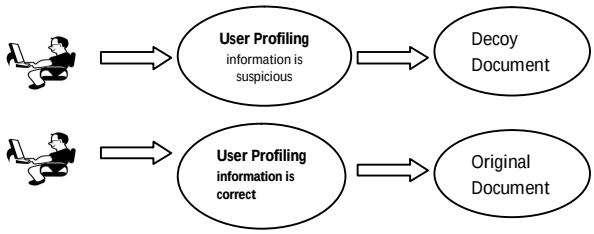


Fig -2: Decoy System

ADVANTATES OF USING PROPOSED STSTEM

- Confusion of the attacker to distinguish real from fake informaion.
- Deterrence effect plays a significant role in reventing masquerade activity by risk-averse attacker.
- Detection of masquerade activity but not the attacker.

3. One Time Password Security System

One Time Password security system can be applied at User Login Level to provide extra security so that only authorized user could be able to login only. The One Time Password system will generate a verification code which the user required to enter during registration. After this code will be confirmed by the Administrator and only
after his authorization the user registration will be done. Then the user could move further to access his application data. While uploading the innovative data will be sent to the Cloud Service Provider and a copy of it would be sent to the Administrator for authentication. After a simple yes/no message from the Administrator the innovative file will be processed further for division and encryption by the Cloud Service Provider. This will also reduce the overhead significantly. The rights to modify update or delete will only exist in with the owner of the data thereby ensuring an most select level of Security. Internally the Database administrator is also monitored by the Administrator in order to keep a check on any form of wicked activity. Data lost can also effectively retrieved using standby servers. Other specifications in the application include digital signatures.

4. Block the Attacker

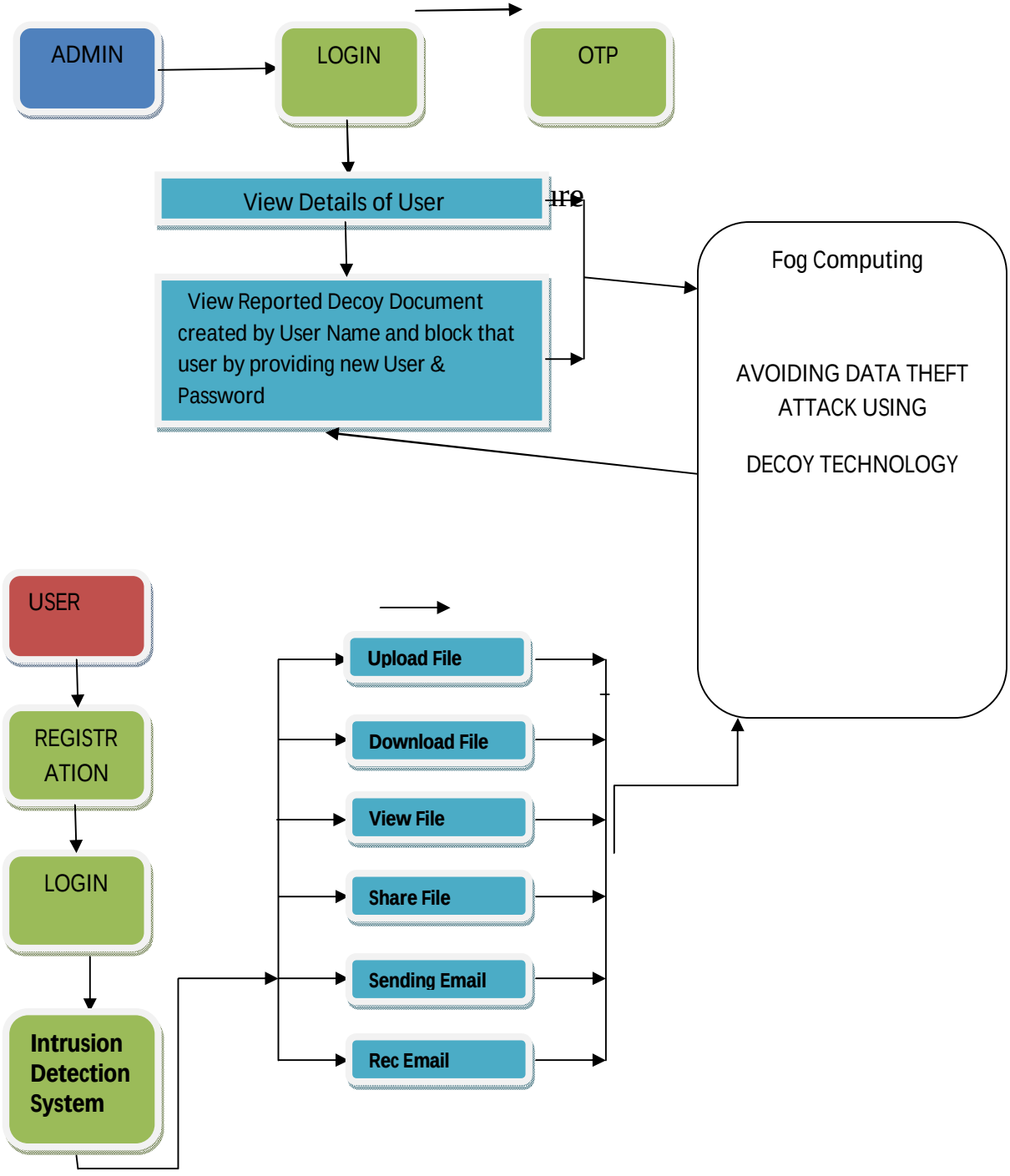
The Information of attacker from his user profile behavior or Intrusion Detection System we can directly block that user or we can ask a user to change security questions accordingly. All the record of the different user will maintained in the user profiling activities, so as soon as system detects any specious activities, it directly block that user in case, if any allowed user try to search any other widely stored files then according to our situation our system blocks that client, but during blocking system asks security questions to that user to avoid attacks.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016



Fog System Architecture

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

V. CONCLUSION

Data privacy is one of the biggest challenge in cloud computing by implemented different approaches for securing personal and business data in the cloud. We propose a system to prevent data access patterns by Intrusion Detection System/ behavior analysis, Decoy System, One time Password System and Block the Attacker 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. In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

REFERENCES

[1] C.Rieger, D.Gertman, and M.McQueen, "Resilient control systems: Next generation design research," in Proc. 2nd IEEE Conf. Human Syst.Interact., Catania, Italy, May 2009, pp. 632–636
[2] Madhusri.K,Navneet."Fog Computing: Detecting Malicious Attacks in a cloud international Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.
[3] Cloud Security Using Fog Computing Proceedings of IRF International Conference, 30th March-2014 http://iraj.in/up_proc/pdf/56-13963354905-7.pdf
[4] Cloud Security Alliance,' "Top Threat to Cloud Computing V1.o. "March 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[5] B.M. Bowen and S. Hershkop, "Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/," 2009.

BIOGRAPHY

Rajesh Anand is working as Assistant Professor in P.G. Department of Computer Science & Applications at Hindu College, Amritsar. He received Master of Computer Application (MCA) degree in 1991 from GNDU (Guru Nanak Dev University, Amritsar, Punjab, India. His areas of research interests are Computer Networks (wireless Networks), Stenography, Data Base Management System, web 2.0 etc.