ISSN 2395-1621

Implementation of Security and Privacy on Fog Computing using Decoy Technique

[#1]Yogesh K Nath, [#2]Rupesh R Bhairat, [#3]Ajit N Ghagare,
[#4]Prof. Geeta Atkar

[1]nathyogesh03@gmail.com
[2]rupeshbhairat@gmail.com
[3]ajitnghagare919@gmail.com
[4]geeta.atkar@raisoni.net

[#1234]Department of Computer
G.H.R.C.E.M, Wagholi, Pune.

ABSTRACT

Now days, Cloud network is less secure or protect the data on cloud from the data theft attacks, mostly insider attacks. A large and secure of professional and personal data is stored on Cloud server. Cloud network storage is being used in different industrial sectors. In this sector of the abundant advantages of storing data on cloud, Security still remains a major problem which needs to be conquered. Computers system is used to access the data on Cloud, with the new communication and computing network create new data security challenges. The subsisting methods of protecting secure and important data on cloud have failed in preventing data theft attacks. An altered approach is carried out for securing the data, in addition to the previous standard encryption mechanisms. The users using the Cloud are monitored and their access patterns are recorded. All Users have a unique profile which is monitored and updated to the server. When an unwanted activity such as unauthorized permission access or random and untargeted search for data is detected which is not likely to be of the real user, a disinformation attack is launched. The any user or person who is trying to access the own data is made to answer the security questions. A large amount of Decoy data is provided or available to the attacker which in turn protects the user's real data.

ARTICLE INFO

Article History

Received: 26th May 2017

Received in revised form :

26th May 2017

Accepted: 28th May 2017

Published online :

29th May 2017

Keywords: Cloud Computing, User Behavior Profiling, Decoy documents.

I. INTRODUCTION

Now days, Cloud is very essential need of all organization and firms. Global Cloud store very large-big amount of data of organizations and company so they can access data from any location in world by only internet connection you have your side. Cloud has provided as well as some challenges of securing valid data in cloud. Problems of hacking and misuse of cloud can lead to misuse and access of personal data and organization's important data. Mostly hacker is insider to the organization or person with negative thoughts and bad intention. The online twitter incident issue example where the personal and important information is hacked and launched on the incorporate unauthorized website. In this incident the hacker attack on the, accounts of users were hacked including the account of U.S. President Barack Obama. So we prevent this data theft attacks in cloud computing, we are providing and introducing new technique called fog computing. In this methodology, we are introducing the combination of two technologies: User Behavior Profiling and Decoy Information Technology. Using User Behavior profiling technology, we detect authorized person and unauthorized person. If the person is authorized then it sends the original file to the user but if the person is unauthorized then it sends the bogus files to the user. Unauthorized person doesn't know that files are bogus files we create the fake file. To secure the real data of the user from misuse we can use decoy file technology.

II. LITERATURE SURVEY

The existing system is less secure to detect the unauthorized users and can be easily hacked by anyone professional in hacking field. We facility of security questions has been provided to the existing system then also the available system is very poor system and less secure. Anyone who has got unauthorized access to cloud can search for files and data. The system is not able to identify whether the user is

legitimate or not. If the person is authorized and illegitimate then also this system sends the original information to the user. Therefore existing system is not secure. Encryption methodology is provided to existing system but cloud server and valid data is not secure by only encryption.

"Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", this paper explains monitor data and provides data security from unauthorized intruders and confusing the attacker and unauthorized users about the real data.
Advantages:
1-User Behavior Profiling
2-Decoy Information technology

"Software decoys for insider threat", in this paper author, discussed a technique that confuses the insider and attacker also used obfuscation which helps to secure data by hiding it and making it decoy information for insider.
Advantages:
Author developed a technique that was a software decoy for securing cloud data.

"Reliability in the Provides Three tier architecture Utility Computing Era: Towards Reliable Fog Computing", in this paper author providers feasibility to real time objects where the user can perform the operation on cloud computing.
Advantages:
Three tier architecture for Fog Computing is used.

"Improving Websites Performance using Edge Servers in Fog Computing Architecture", this paper provide various methods are combined and used with unique knowledge to improve the performance of rendering a web page.
Advantages:
This proposed system reducing the size of web objects, minimizing and blocking HTTP requests, and reorganizing the web page.

III. PROPOSED WORK

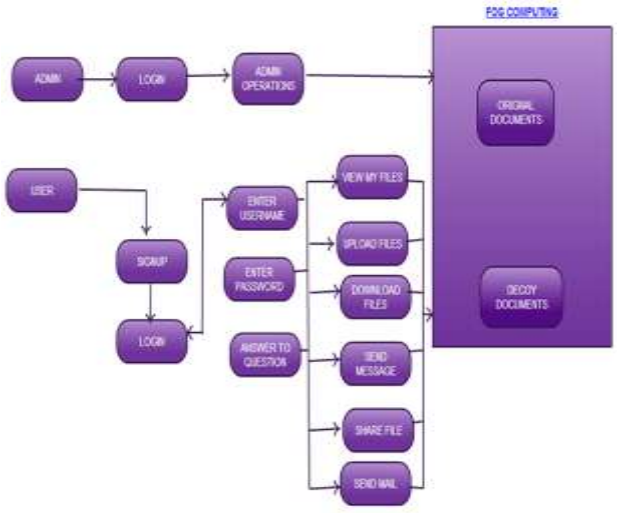

Fig 1. System architecture

We propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing. We implement the new technology to launch disinformation attacks against malicious insiders performing on cloud, preventing them from distinguishing the real sensitive customer data from fake worthless data. The system decoys, then, serve two purposes: (1) we check or validating whether data access is authorized when abnormal information access is detected, and (2) second one is confusing the attacker with bogus information.

Module Description:

1. **Cloud Computing.**
2. **User Behaviour Profiling:**
3. **Decoy documents.**

Cloud computing

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources we take the example, networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It divide into three type

1. Application as a service(AaS).
2. Infrastructure as a service(IaS).
3. Platform as a service(PaS).

Cloud computing exhibits the following key characteristics:

1.We improves with users' ability to re-provision technological infrastructure resources.

2. We also Cost is claimed, reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure.

3. Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

4. Multi resources access and costs across a large pool of users thus allowing for.

5. Centralization of infrastructure in locations with lower costs for within of time we can access resources (such as real estate, electricity, etc.)

6. We also analysis the Utilization and efficiency improvements for systems that are often only 10–20% utilized.

7. We also Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

8. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

9. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels.

10. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

User Behaviour Profiling:

We check data access on the cloud and detect abnormal data access patterns User behaviour profiling methods is a well best Technique that can be applied to the proposed system model. This technique analysis the how, when, and how much a user accesses their information in the Cloud server. Access 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behaviour based security is used to detect the fraud detection applications system. Such profiles would naturally include volumetric information, how many documents are typically read and how often. We also monitor for abnormal search behaviors that exhibit deviations from the user baseline the checking correct of search behavior anomaly detection. When we use trap-based decoy files should provide stronger evidence proof of the attacker, and therefore improve a detector's accuracy.

Decoy Documents:

We apply the different new approach for securing information of users in the cloud using offensive decoy technology. We analysis and monitor data access in the cloud and detect abnormal service data access patterns. We implement a disinformation attack by returning big amounts of decoy information data to the attacker. This technique protects against the misuse of the user's from real data. We used new technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:

(1) We Validating whether data access is authorized person when abnormal information access is detected, and

(2) We confusing to the attacker with bogus information.

IV. RESULT

V. CONCLUSION

We conclude that and analysis, with the increase of data theft attacks on cloud, the security of user data is becoming a serious issue for cloud service providers for which our proposed system fog computing is a paradigm which helps in monitoring the behavior of the user which activity they perform and providing security to the user data. Other techniques discussed in this study paper use fog computing for optimizing and analysis the website performance issue. We finalize that by continuing this proposed work using Fog Computing platforms can lead to highly very strong techniques and would contribute in increasing the level of security if user data on the cloud so the user have provide more security.

REFERENCES

1) Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data theft Attacks in Cloud" IEEE 2012

2) Ivan Stojmenovic, Sheng Wen, "The Fog Computing Paradigm: Scenarios andSecurity Issues" IEEE 2014

3) D. C. Saste, P. V. Madhwai, N. B. Lokhande, V. N. Chothe, "FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology", IJCTA, Sept-Oct 2014.

4) Thogaricheti Ashwini, Mrs. Anuradha.S.G, "Fog Computing to protect real and sensitivity information in Cloud", IJECSE,SSN 2277-1956/V4N1-19-29

5) Shanhe Yi, Cheng Li, Qun Li, "A Survey of Fog Computing: Concepts, Applications andIssues, ACM 2015

6) Viraj G. Mandlekar, VireshKumar Mahale, Sanket S.Sancheti, Maaz S. Rais, "Survey on Fog Computing Mitigating Data Theft Attacks in C loud", International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-2, Issue-6, November-2014

7) Yongkun Li, Member, IEEE, and John C. S. Lui, Fellow, IEEE, "Friends or Foes: Distributed and Randomized Algorithms to Determine DishonestRecommenders in OnlineSocial Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 10, OCTOBER 2014.

