Implementation of Fog Computing for Enhancing Security of Cloud

[1]Prasad Dharmadhikari, [2]Mandar Dunde, [3]Arpit Bhatnagar, [4]Abhishek Singh

Computer Engineering
NBN Sinhgad School of Engineering Pune, India

***Abstract*: Fog computing is a platform that extends cloud computing model and services to the edge of network. Cloud computing is emerging as upcoming solution which all organizations in the world aim to apply for its every day computing tasks because of its simplicity compared over On-Premise systems. But Cloud computing also comes with issues such as security, user authentication, privacy and access control. These issues inspire researchers to work on providing security solution for cloud to ensure secure cloud computing. This Paper entitles the implementation of fog computing as security provider for cloud and also proposes a new and cost-effective user authentication scheme which is designed at fog-level where an end user based authentication mechanism has been integrated to verify identity of end user to access the cloud which will increase the privacy in cloud environments.**

***Index Terms*: Cloud computing, Fog computing, Authentication, Security, Privacy**

I. Introduction

Cisco has presented another innovation named Cloud computing to the world upon their earlier Fog Computing innovation. Fog is the center layer between the source and target. The aim of the fog is to improve the data performance which will be uploaded to the cloud for information processing, analysis and storage. Fog Computing empowers another type of applications and services, and that there is a productive exchange between the Cloud and the Fog, especially with regards to data management and analytics. Fog Computing extends the Cloud Computing to the edge of the network. To overcome threats, fog computing helps in checking and identifying the unapproved access. Fog nodes provides feature of location access.

II. Literature Survey

1. Madsen.H and Albeanu.G : Introduced the difficul- ties looked by current figuring ideal models and examined how Fog processing stages are possible with cloud and are dependable for genuine tasks. Fog computing is, for the most part, accomplished for the need of the topographical appropriation of assets as opposed to having a unified one. Multi-Level tier is followed in Fog figuring stages. In the first tire, there is a machine to machine correspondence and the higher levels manage perception and detailing. The higher level is represented by the Cloud. They said that building Fog processing tasks are challenging.

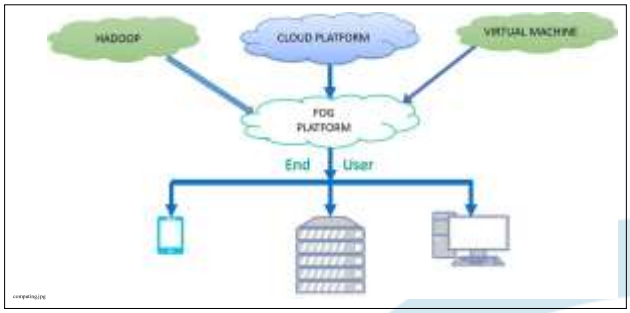
2. Z. Jiang et al.: Talked about Fog processing and further utilized it for improving the website's efficiency with the assistance of edge servers. They said that developing architecture of Fog Computing is exceedingly virtualized. They displayed their thought that the Fog servers screen the queries made by the clients and track each query by utilizing the client's IP address or MAC address.

3. Sabahi, F.: Referenced dangers and reaction to cloud computing. He displayed an examination of the advantages and dangers of traded off security and protection. In this paper, he has summarized quality and accessibility related issues of cloud resources given by the trusted third party. He examined the most widely recognized assaults these days are Distributed Denial of Service attacks. The answer for these assaults can be, cloud innovation offering the advantage of adaptability, with the capacity to give assets quickly as important to keep away from site shut down. Thinking about every one of these prerequisites, this model is made which incorporates two primary advances: first is to make clients and produce examples of their diverse access practices, the subsequent stage is observing the client access designs.

4. Salvatore J. Stoflio et al.: Presented another innovation known as Fog computing. They implemented security by using fake data technology. They clarified two techniques, for example, Client conduct profiling and Decoy. In User conduct profiling they inspected how, when and how many measures of data a supporter is getting to. They filtered their supporter's action to look at for any variation from the norm in the information get to nature of the subscriber. The second procedure is an imitation wherein data which is fake or we can say extortion i.e., honey pots, honey files, and so on are

used to confound the breacher by representing the information in such a way that it appears real.

III. System Architecture



IV. System Workflow

The system concentrates to provide straightforward, less complex, more secured solution which makes the Veri- fication easy to manage and make access to the ser- vice simple to the end client. The solution is based on unique Application ID which will be sent on user's mail id which user provides at the time of registra- tion. Application ID is created at the time of registration. The system works through following steps:

- If user don't have an account , then first register to create an account. Otherwise directly sign in to the account.
- After registration the information of user is stored in cloud database. And the account has been created.
- After registration, personal details and bank details along with unique application ID are sent on user's mail ID.
- If an authorised user enters valid credentials to sign in to his/her account username, password and unique application ID, then he/she will be redirected to original server and account has been successfully logged in.
- If user enters invalid credentials, then he/she will be redirected to the fog server and must follow the three levels of security as follows:
  - **Enter application ID :** If user enters valid appli- cation ID then he/she will be redirected to original server and account has been successfully logged in. Otherwise user will be redirected to next level.
  - **Image Captcha :** image captcha is a type of challange-response test used in computing to deter- mine whether or not the user is human.
  - **Security Questions :** User has to answer these questions and responses should match with the an- swers which were entered by user itself at the time of registration.
- If User fails to complete any one of above the levels then he/she is permenantly blocked and the access to complete system is revoked by the administrator.
- Next time when user tries to freshly login to the system, as the user is blocked, the user needs to contact the system administrator.

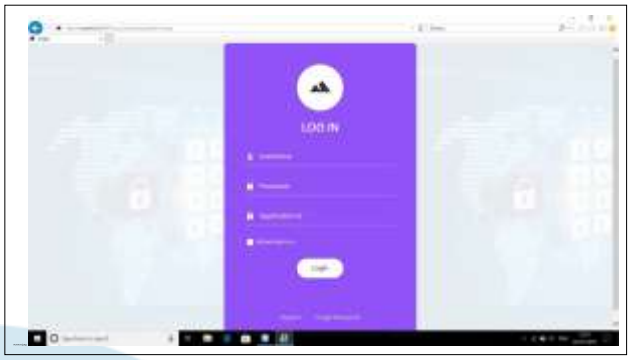


Fig. 1. Login screen

Fig. 2. Registration Page

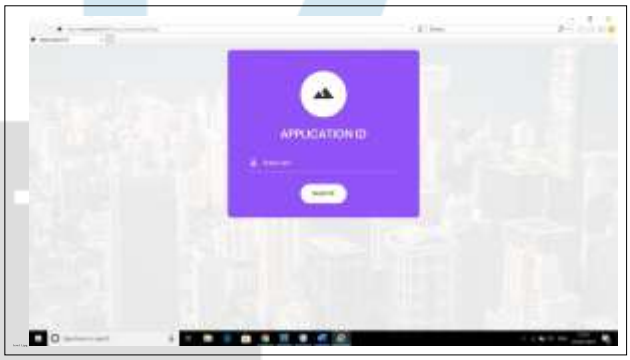


Fig. 3. Security Level 1

Fig. 4. Security Level 2

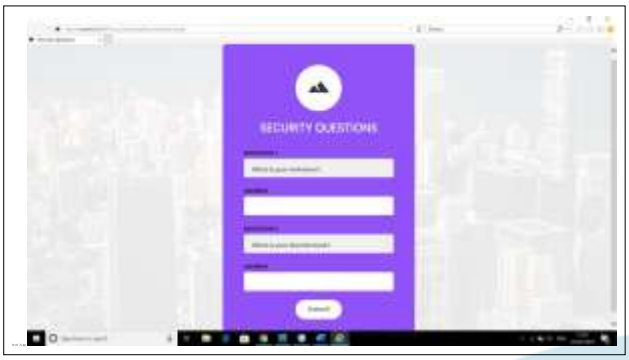


Fig. 5. Security Level 3

Fig. 6. Successful Login

Fig. 7. Transactions interface

Fig. 8. Blocked User

V. Security in Fog Computing

There are different approaches to utilize cloud services to save or store files documents and media in remote services that can be accessed to at whatever point the client connected with the web. The principal issue in the cloud is to keep up security for client's information such that it ensures just validated clients and nobody else accesses that information. The issue of giving security to secret data is a core security issue, that it doesn't provide a level of assurance many people want. There are different techniques to verify remote information in the cloud using standard access control and encryption strategies.It is great to state that all the standard methodologies used for giving security have been concluded to fail occasionally for a variety of reasons, including faulty implementation, buggy code, insider assaults, misconfigured services, and the innovative development of advanced assaults not imagined by the implementers of security methodologies. Building a protected and dependable cloud computing environment isn't sufficient, in light of the fact that assaults on information continue to occur, and when they do, and data gets lost, there is no real way to get it back. There is a need to get answers for such issues.In this paper, we present a way to deal with verifying individual and business information in the Cloud. We propose monitoring information access patterns by profiling client behavior to decide whether and when a malignant insider illegally accesses to somebody's files in a Cloud. Fake records put away in the Cloud alongside the client's genuine information additionally serve as sensors to identify unauthorized access. When unapproved information access or introduction is suspected, and later checked, with test questions, for example, we immerse the malignant an insider with decoy data so as to dilute the client's genuine information. Such preventive assaults that depend on decoy technology could give unprecedented levels of security in the Cloud and in social networks.

VI. Conclusion

In Fog Computing we are showing another methodology for tackling the issue of insider information theft assaults in a cloud utilizing powerfully produced distractive files and furthermore saving capacity required for keeping up fake documents in the cloud. So by utilizing decoy method in Fog can limit insider assaults in cloud.

References

[1]Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.

[2]Zhu, Jiang,Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture, Service Oriented System Engineering (SOSE), IEEE. 2013.

[3]Sabahi, F. Cloud computing security threats and responses, In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on 2011,pp. 245-249.

[4]Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[5]Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.

[6] Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp. 13-16.

[7] Claycomb, W. R., Nicoll, A. Insider Threats to Cloud Computing: Directions for New Research Challenges, In Computer Software and Applications Conference (COMPSAC),IEEE 36th Annual, July, pp. 387- 394, 2012.

[8] Park, Y., Stolfo, S. J. Software decoys for insider threat, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, May, pp. 93-94, 2013.