A Review Paper on Providing Security in Cloud Computing Using User Behavior Profiling and Decoy Technology

[1]Syed Asiya, [2]N.Veda, [3]B.Maheshwari
[1]Assistant Professor, [2,3]Students
Department of Computer Science & Engineering
Balaji Institute of Technology & Sciences, Narsampet, India.

Abstract:
The new advancements in the field of data innovation offered the general population pleasure, solaces, and accommodation; however there are numerous security-related issues. One of them is secret word record. Secret phrase documents have a great deal of security issue that has influenced a huge number of clients and also numerous organizations. The Cloud is the bunch of a PC associated with store data. Cloud computing makes achievable for numerous clients to, share normal processing assets, and to access and store their own and business data. Substantial information put away on cloud so, executing security turn out to be extremely vital on the customer side. Existing calculation bombed once key is lost by proprietor. User behavior profiling and decoy technology give an alternate method to anchor information on a server which is progressively effective and secure. There are numerous calculations on client conduct profiling and imitation innovation however nobody can discover the issue is that proficiently conveying the fake document in such a way the gatecrasher not ready to perceive the contrast between the authentic and fake record, when the mysterious conduct of the client recognized. Proposed a system which consists of user behavior profiling and decoy technology.

Keywords: Cloud Computing, Fog Computing, Decoy Technology, User Behavior Profiling

I. Introduction

Cloud computing comprises of a mutual pool of assets shared among clients per membership premise. The way PC put away data and individual information can cause new information security challenges. In the present world situation each association utilizing distributed computing to ensure their information and to utilize the administrations like Iaas, Paas, Saas. Encryption system, that we use today so as to ensure the information over the cloud are not sufficiently reasonable to stop the unapproved access to authentic client information. In this manner, we proposed a framework in which we going to utilize the two procedures together for example client conduct profiling and bait innovation. Into this framework at whatever point a gatecrasher endeavors to get to the information of the certified client, we consequently produce a bait document with a similar name and scrambling content record in such a way it looks authentic as the focused on record and gives the equivalent to the interloper. we consequently create a fake document with a similar name and scrambling content record in such a way it looks authentic as the focused on record and gives the equivalent to the gatecrasher.

II. Literature Survey

As we have many solutions on user behavior profiling and decoy technology but no solution addresses the problem of efficiently delivering the decoy file in such a way the intruder not able to recognize the difference between the genuine and decoy file, once the anonymous behavior of the user identified. The existing system was not worked on anonymous behavior. The data stored on cloud need security for stored data. The way information and personal data stored in system can infect new data security challenges. Encryption mechanism, that we use today's in order to protect the data over the cloud is not fair enough to stop the unauthorized access to genuine user data. The previous database system deployed in local network can be accessed locally. As the use of internet is increasing because of new computing technology, the users can access the database from any point of view which leads to a problem of security. Existing security mechanisms fails to secure data from attackers. Encryption mechanism doesn't verify the identity of the intruders, instead of that, they focus only on the key provided by the users at the time of accessing the available resources which may or may not provide by the authenticated user.

III. User Behavior Profiling

Proposed a totally new system all together secure the information over the cloud utilizing the user behavior profiling and another hostile decoy technology. We observed the information access over the cloud and attempt to recognize the strange access design over the cloud. Into this framework at whatever point a gatecrasher endeavors to get to the information of the real client, we naturally produce a fake record with a similar name and scrambling content document in such a way it looks real as the focused on record and gives the equivalent to the interloper. Profiling method connected hear to show how, when, and how much measure of data access by the client over the cloud. Such typical conduct of the client is persistently observed to decide if strange access to a client's data is happening.

Delineated conduct based security for the most

Part utilized by cops in misrepresentation identification. Bait innovation is utilized in path By approving, regardless of whether the information get to is approved or unapproved when strange conduct is identified.

Mistaking the aggressor for a counterfeit measure of distraction data, which is given by the imitation documents, the conduct of the client is being distinguished as unknown utilizing user behavior profiling technology. The Generated File should we with the end goal that the substance of the first document and bait record are totally extraordinary and difficult to recognizable.

A. System Architecture:

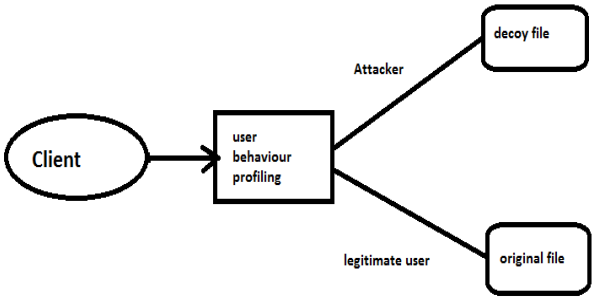

Figure A: System Architecture

User: Login, Register, Search file, Download file Intruder: Behave wrong by entering the wrong password

Get decoy file Admin: View Users, View hackers downloaded file.

When Client sends any file can be a chance of sending the file by attacker and legitimate user. So this can be solved by decoy technology and user behavior profiling.

B. Algorithm of Mathematical Model:

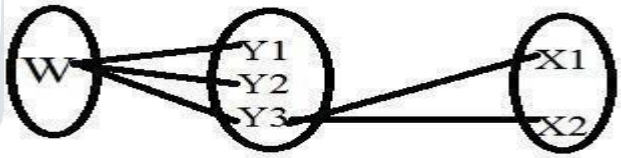

Figure B: Mathematical model

Let, Z be the System Such that, Z= {W, X, Y, success, failure} Where, W= Login details, X= Decoy file, Y=Identifying user behavior and Download\decoy file Input=Enter invalid login details. Function: Y1=Verify User Login details. Y2=Find anonymous activity Y3=If User behavior is illegal to download decoy file

Output:

X1=Success Case-1(If the user is in normal condition then it will get original file and if anonymous will get decoy file) X2=Failure Case-2(Large database can lead to more time consumption to retrieve the information) 2.Hardware failure 3. Software failure

IV. Conclusion:

With the expansion of information, burglary assaults the security of clients private information over the cloud is turning into a significant issue for cloud specialist organizations. For which, Fog Computing is a system which helps in anticipating and checking the conduct of the client and giving security to the client's information. The proposed system was initially created utilizing encryption calculation however we have additionally actualized it with the client conduct profiling calculation alongside powerfully produced imitation document idea. The proposed system scramble the information of the record that is programmer won't perceive a distinction between the first document and mixed document.

V. References:

[1] Ahamed, B. B., & Ramkumar, T. (2015). Deduce User Search Progression with Feedback Session. Advances in Systems Science and Applications, 15(4), 366-383.

[2] Prevention Of Malicious Insider In The Cloud Using Decoy Documents by S. Muqtyar Ahmed, P. Namratha, C. Nagesh. Cloud Security: Attacks and Current Defenses Gehana Booth, Andrew Soknacki, and Anil Somayaji.

[3] Overview of Attacks on Cloud Computing by Ajay Singh, Dr. Maneesh Shrivastava.

[4] D.Jamil and H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[5] K. Zunnurhain and S. Vrbsky, Security Attacks and Solutions in Clouds, 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.

[6] Sivaram, M., Yuvaraj, D., Porkodi,V., & Manikandan,V.(2018). Emergent News Event Detection from Facebook Using Clustering. Journal of Advance Research in Dynamical & Control Systems, Vol.10,07-special issue,PP1941-1947.

[7] 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".

[8] Fog Computing: Mitigating Insider Data Theft Attacks in The Cloud.

[9] M. Van Dijk and A. Juels, On the impossibility of cryptography alone for privacy- preserving cloud computing, in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec10. Berkeley, CA, USA: USENIX Association, 2010, pp. 18.

[10] M, Sivaram, et al. "Securing the Sensor Networks Along With Secured Routing Protocols for Data Transfer in Wireless Sensor Networks." Journal of Emerging Technologies and Innovative Research, vol. 5, no. 10, Oct. 2018, pp. 316–321., doi:http://doi.one/10.1729/Journal.18612.

[11] Ahamed, B. B., & Yuvaraj, D. (2018, October). Framework for Faction of Data in Social Network Using Link Based Mining Process. In International Conference on Intelligent Computing & Optimization (pp. 300-309). Springer, Cham.

Authors Bibliography:

1. **Syed Asiya, Assistant** professor at Balaji Institute of Technology & Science , Laknepally, Narsampet. Interested research areas are data mining, internet of things, cloud computing.
2. **N. Veda,** Student of Balaji Institute of Technology & Science , Laknepally, Narsampet. Interested research areas are data mining, internet of things, cloud computing, Artificial Intelligence
3. **B. Maheshwari,** Student of Balaji Institute of Technology & Science , Laknepally, Narsampet. Interested research areas are data mining, internet of things, cloud computing, big data.