Global Scientific JOURNALS

GSJ: Volume 7, Issue 4, April 2019, Online: ISSN 2320-9186
www.globalscientificjournal.com

DECOY TECHNOLOGY IN FOG COMPUTING

Theresa Catherine Rangel
Country: Pakistan
Email: rangeltheresa@hotmail.com

ABSTRACT

Initially we all were dependent on a computer to be physically present for storage and processing. No device could process information. Then cloud computing came into existence, where all computation was performed in the cloud.. But then the issue came for small processing, it took long to fetch data from the cloud and in cases when internet has some issue due to weather or any such reasons, it could take an extremely long time, which would result in a crash, which creates a major break in to it. This has security issues, where hackers can easily break it and manage to get themselves in. Hence a new technique Fog computing came into play, this reduces the computing and latency, because it runs most of its computation on Edge i.e. the user device itself. To ensure more security in case the device is in wrong hands or the account credentials have been obtained illegally, fog computing uses Decoy technology, where if any unusual activity it raises an alert , which in correspondence it will show the unauthorized user the data, but it will not be the original data, it will be manipulated garbage data which if the user is unaware will presume its original, so while the user is accessing the system, they are being tracked and all process is logged till they can be identified!

Keywords *Cloud computing, Fog computing, Edge, Data security, Decoy technology, Decoy Information, Data deduplication, User profiling, Digitilized, Storage, Sequence Learning*

1. INTRODUCTION

Distributed computing is an administrations give over the web, and these administration its not just programming administration it might be equipment benefit that implies to both software as well as hardware. A standout amongst the most critical administration that given by cloud specialist co-op is storage room, the customer is assured that security is implemented and it is guaranteed that nobody can get to their information and view it particularly when there is imperative data lying , Data robbbery attempts are enhanced if the hacker may be an insider. This is one of the elevated amounts of risk to a distributed computing system of Cloud Security, most customers accessing Cloud processing know this risk. [1]

The negligence of straightforwardness into a system, not to mention command over every loophole, the Cloud supplier's verification and validation itself, approval, and review controls just compounds these risk.

Simple passwords might be obtained by a noxious insider of the Cloud specialist organization or could be that the clients' private keys may be stolen, and this could be how their secret information may be extricated. Subsequent to taking a client's authentication credentials, the pernicious insider gains admittance to all client private data, while the system has no methods for identifying this unapproved access. Research in Cloud security is still in way, some resulting research has concentrated on methods for counteracting unapproved and ill-conceived access to information by creating complex access control and encryption components which comes in fog computing.

A. Data Security

Security is the core aspect which every user accessing the web is looking for. Everyone wants to be assured that their data will not fall in the wrong hands. Security is a central thought when arranging, structuring, executing , and dealing with a system foundation[2]. Not withstanding the regular issues that new system and gadget advances cause, including contrary qualities and progressing bolster issues, non-secure connections can uncover an association's system movement and assets to unapproved access. Such people may obtain information and adventure network based assets, including Internet get to, fax servers, and circle stockpiling, which if hacked can crash a whole system, render administrations inaccessible, and conceivably subject the association to lawful liabilities. [3]

B. Data Deduplication

As the meaning of the word itself; deduplication - elimination of duplicate data. The concept of deduplication is used in cloud computing, due to the issue of users saving the exact same data multiple times as it tends to be difficult to remember what was saved and many a times calling the data to confirm if it was already inserted can be hurdle-some hence to reduce the storage utilized by a single user, deduplication is performed. There are many tehcniques to ensure that only redundant data is deleted. This also raises a security threat, no doubt convergent encryption is implemented at a high scale, this methodology does not entertain extrmeely large data, due to the number of encryption keys that will get created. [4]

C. *User Behaviour Profiling*

The concept of monitoring the users daily behaviour; So incase of any abnormal activity for example a login from an unknown ip, an ad that the user always cancels etc. can help the system determine that it is not the authorized user, but in fact a fraud who has gotten their hands on the credentials of the user. this monitoring needs to be persistently checked to decide if an irregular access to ones data is being attempted. This technique for security is usually utilized in application to identify extortion [5]. Such behaviour would normally incorporate a large volume of data, where great number of archives are ordinarily perused regularly [6]. We screen for irregular hunt practices that display deviations from the client gauge; the relationship of pursuit conduct inconsistency discovery with snare based imitation documents ought to give more grounded proof of abnormal activity, and subsequently enhance a detector's precision.[4] [7] [8]

D. *Decoy Technology*

Decoy as in the name indicates to give false, or imitation of original but technically fake, is the technology used to make hackers believe they have accessed a users original data so that they can stop trying to attempt on harming eligible user data. Decoy technology is the innovation which is giving the fake data to the unapproved client or the aggressor. Fake advancements, or the producing the futile information records on the interest of the framework to perform an assault against the assailant. Utilizing this system the first data gets changed in a format which depicts as legitimate but data present in is bogus; with the goal that the ex-filtering of the record or data is winds up outlandish. This innovation might be coordinated with client conduct proling to anchor a person information in the Cloud. At a point where an unusual access to the cloud is noticed, decoy data is returned by the Cloud and conveyed in a manner to depict as totally genuine and original. The authenticated client, who is the proprietor of the data, would be able to promptly distinguish when imitated data is being displayed, and consequently could modify the Cloud's reactions through an assortment means, for example, questions to illuminate the Cloud security framework that it has erroneously recognized an unapproved access. For the situation where the entrance is effectively identied as an unapproved get to, the Cloud security framework would convey unbounded measures of false data to the foe, along these lines anchoring the user's genuine information from unapproved exposure.[3] [4]

2. THREATS IN CLOUD:

1) Data breaches This led to the loss of personal data and credit card information of about 110 million people, it was one of the theft during processing and storage of data. [9]
2) Data loss Data loss occurs when the disk drive dies without any backup created by the cloud owner. It occurs when the encrypted key is unavailable with the owner.[10]
3) Account or service traffic hijacking Account can be hacked if the login credentials are lost.[10]
4) Insecure APIs Application Programming Interface controls the third party and verifies the user. [9]
5) Denial of service This occurs when millions of users request of same service and the hackers take this.[10]
6) Malicious insiders This occurs when a person close to us knows our login credentials.[9][10]
7) Abuse of cloud services By using many cloud servers hacker can crack the encryption in very less time. [9]
8) Insufficient due diligence- Without knowing the advantages and disadvantages of the cloud many businesses and firms jump into cloud thus leading to data loss [2][10]
9) Shared technology This occurs when the information is shared by the many sites.[10]

3. DISADVANTAGES OF PREVIOUS SYSTEM:

1) Anybody can get to the information he can decode it in the event that he know the calculation[10]
2) Nobody knows when and exactly what time the assault may occur.[1][10]
3) By applying encryption procedure to the information we can't accomplish entire security to secret information.[1] [10]
4) It is troublesome to recognize which customer was attacked.[1][10]
5) We can't recognize which record was hacked.[10]
6) Last but not least it could be a hacker who has the credentials of an authenticated user i.e. could be an inside job, hence cannot say if a user was even hacked. [1][10]

4. SIGNIFICANCE OF FOG COMPUTING

Today, most of our data is uploaded to the internet or in another words cloud. We depend on the internet to store and compute our data, from documents to register a person right up to a countries defence codes, all depend on the cloud. Saving and manipulating data at cloud level requires a lot of processing speed hence CISCO introduced Fog computing or also known as fogging.

Fogging is a computing infrastructure that is decentralized in which data, its computation and storage are distributed logically and efficiently between the data source and the cloud.

The Internet makes most of our life easy; though one concern remains at hand i.e. its security. As mentioned, Fog computing is extended from cloud computing, which is utilized at edge i.e. our device level, our main concern is that any person may easily be able to guess the password or hack through to obtain our data, or possibility of uploading a virus to destroy any significant data. To ensure this concern is reduced to as minimal as possible, a technology is in place called decoy technology. As the name describes, it implements decoys as in similar to the truth but fake information which only the actual user would be able to identify its authenticity. In addition to log these details of any unauthorized user, even though emails are generated of abnormal activities but keeping in mind the fact that the authorized user personal id may have also been compromised. Hence Decoy technology procedure of depicting that the information displayed is legitimate whereas the actual user will be able to identify that the authenticity of the data and can correspond to the admin in charge of system of this issue, and via log details maintained it can help track the unauthorized user.
The main significance of Fog computing is not only its computing at edge (device end) in addition the ideology of using decoy data has not only impressed the computing world but also ensures security for sensitive data while not having to carry it around physically but utilizing the cloud to store the data.

5. LITERATUREREVIEW

Increment in use of PC and web expands information as per the research article published by Das, Kumar R., & Ravishankar (2018). Capacity of information in the ordinary framework is unthinkable nowadays. Lack of storage space plays a major role for individuals to move to register on the cloud. Cloud processing has many essential features which benefits every field of users such as; adaptability, versatility, portability, elasticity etc. One major issue which is still present is the security of data on the cloud. Even though endeavors are taken in the security of the cloud yet at the same time it contains provisions which are confining individuals to utilize the Cloud to store their data. Fog computing is the expansion of the cloud processing to the device or edge of system. Fog computing expands the capacity, systems administration and processing office of cloud figuring. Security in information is enhanced step by step however some information get puts away as volume of the information likewise builds. Anchoring information by utilizing different conduct parameters and distraction information innovation keep up secrecy of information. This paper proposes a methodology of utilizing fog processing for anchoring the information with proficient calculations and conduct examination on substantial information. [11]

Virushabadoss & Bhuvaneswari (n.d.), in their research article, describe and define fog computing as the term authored by Cisco which explain the degree of processing done bu cloud and its decentralized registering framework in which a few information were put away and oppressed for calculation. Be that as it may, the new computational hypotheses have raised the information security challenges against a few security systems in cloud. For example, on the off chance that an unapproved action is distinguished in a system, to misdirect the assailant we send a lot of imitation data. This secures the genuine client's information. In Fog organizes a client conduct gets changed when a framework given an arrangement of directions successively and it is anything but difficult to screen the developing idea of a client. This paper examines the conduct profiling calculation strategy to defeat those issues in fog frameworks. The work did in this paper manages determination of the best factual measurements for distinguishing rouge hubs and it could be connected to any systems where client conduct is by all accounts mysterious by their grouping of activities. [12]

Lucky Nkosi, Paul Tarwireyi and Matthew O Adigun performed a survey on different cloud computing difficulties proposed by early researches for the improvement of Cloud computing to enhance its usage. Various methodologies were studied and to enhance the security by developing efficient and effective manner for the fog not to be victim of misuse or attacker for cloud computing.[13]

In their research Shreya Waghmare, Shruti Ahire, Himali Fegade, Pratiksha Darekar developed a system to monitor data stored by users and how it could provides security of data from malicious intruders by detecting behaviour of user by the analysis of the characteristics of the users data hence protecting original data by providing encrypted data using Hadoop framework. [14]

Blesson Varghese, Nan Wang, Dimitrios S. Nikolopoulos and Raj Kumar Buyya write for the protection and security of Fog computing in mist of registering severe measure concerns are with the end goal to defend the information amid handling. Use of versatility, equipment assets,lessened cost, simple arrangement are a few territories of preferred standpoint of the cloud framework. Facilitating different clients and information stockpiling to the cloud condition has critical hazards. Security worry around the movement of data. Malignant programming might be introduced by programmers on the hub of the mist figuring. On the off chance that transitory information should be put away in this hub, additionally protection issue alongside security challenges should be tended to. Defenselessness can likewise expands security and protection issues in mist registering. To defeat from the issue imitation information idea and disinformation assault against malevolent insiders to the distributed computing. [15]

According to the research paper written by R. Kulkarni, Waghmare, D. Chaudhary & P. Kulkarni (2018) 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 phrase record. Secret word records have a considerable measure of security issue that has influenced a large number of clients as well the same number of organizations. The Cloud is the bunch of a PC associated with store data. Cloud Computing makes plausible for different clients to, share normal computing assets, and to access and store their own furthermore, business data. In cloud computing client put away information on the server side also on customer side. Expansive information put away on cloud So actualizing security turn out to be extremely fundamental on the customer side. Existing calculation bombed once key is lost by proprietor. Client conduct profiling and decoy innovation give an alternate method to anchor information on a server which is more productive and secure. There are numerous calculations on client conduct profiling and decoy innovation in any case, nobody can discover the issue is that productively conveying the decoy document in such a way the gatecrasher not ready to perceive the contrast between the honest to goodness and decoy document, when the unknown conduct of the client recognized. Proposed a framework in which we going to utilize the two systems together i.e. client conduct profiling and decoy innovation. [16]

Cloud Computing is working to ensure that it can shield information on the cloud from information robbery assault. An enormous measure of individual and expert information is put away on cloud. Information burglary assault is one of the security challenge in the cloud computing. According to Saste, Madhwai, Lokhande & Chothe (2014) the methodology used by them is to safeguard information in the cloud. Cloud computing use diverse type of security, information security, stockpiling security, application security, organized security etc. The current component like encryption can't keep the genuine information from being hacked. So rather than encryption, they propose ways to deal with secure or ensure insider information does not fall into the wrong hands by utilizing decoy innovation that they call as Fog computing. The research authors check information access in the cloud and distinguish strange information to design in case system identifies irregular traffic. At the point when the non eligible clients attempt to get to the the data if system identifies this it utilizes test question (security questions), if an assailant enters an incorrect response for security question they give sham data to illicit client this ensure against the abuse of the client's real information, and whereas if client enters the right response for inquiry will get right data. The genuine client know whether any programmer endeavor to robbery and assault his private document, and furthermore know how much endeavor programmer hack each record at which time and information. [17]

K. Goar (March, 2018)research article elucidates that fog computing could be a world view that expands cloud computing which turned into a reality that made-up the strategy for fresh out of the plastic model for computing. Moreover, fog computing gives system administrations complete time to terminals inside the network. The inward data taking assaults in that a client of a framework misguidedly presents in light of the fact that the personality of partner other real client which is an emerging new test to the administration provider wherever cloud benefit provider probably won't have the capacity to guard the data. In this way, to anchor the critical client's delicate information type the guilty party inside the cloud. In this exploration paper he is proposing an exceptionally particular methodology with the help of hostile decoy information innovation, that is utilized for affirming regardless of whether the information get to is allowed wherever anomalous data is identified and subsequently confounding the wrongdoer with the phony information. [18]

In this contemporary age, Cloud Computing plays exceptionally essential job in the online world. In the words of Kalaskar, Ratkanthwar, P. Jagadale & B. Jagadale (2016), in their research article, they write that, Cloud computing gives us fundamentally extraordinary methods for utilizing computers to get to our own business data processed. These new ways emerges some new challenges in the security of cloud. Old strategies like information encryption have flopped in averting information robbery where the culprits are insider to the cloud supplier. We are proposing another methodology where information is anchored by hostile decoy innovation. We can use screen diverse parameters of information access in cloud to distinguish information to get designs. At the point when unapproved information get to is suspected and afterward checked by utilizing test questions, we send vast measure of decoy data to assailant. This decoy data counteracts abuse of client's genuine information.[6]

Mukherjee ,Shu, Kumar, Maglara, Ferrag and Choudhury define the noxious Insider to the cloud; Malicious insiders assault is one of the server assault to the distributed computing which has information burglary assault by vindictive insider to the cloud supplier. Absence of verification from the cloud specialist co-op causes information robbery. Client information can be get gotten to effectively by malevolent insiders to the cloud, however the assault originated from the cloud specialist organization end clients don't recognize the unapproved get to.[19]

6. IMPLEMENTATION

The proposed system detect intrusion by using behaviour analysis, On detection of intruders decoy data is provided to the user.

A. ***System Architecture***

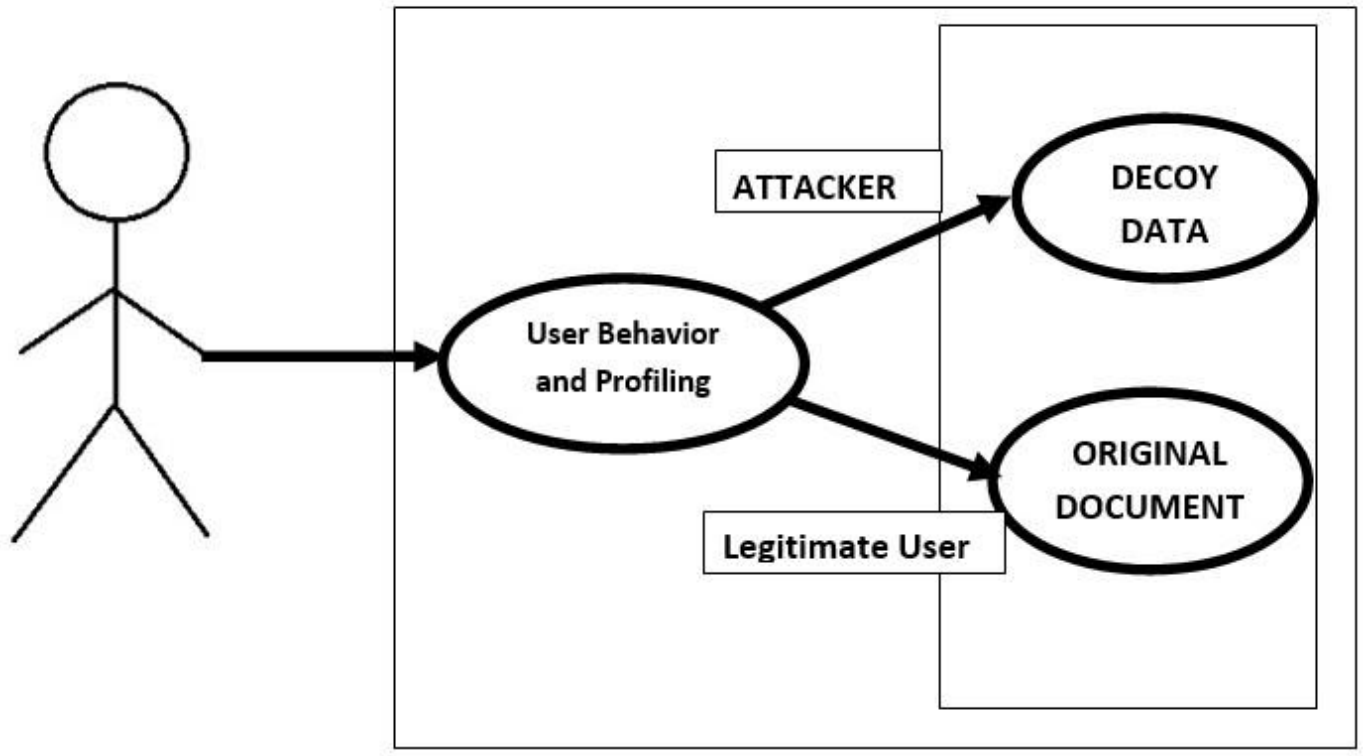

Fig. 1. SystemArchitecture

As depicted in the model, the security component that can counteract inside an information burglary. This is accomplished by propelling disinformation assaults. This is a preventive measure that guarantees shirking of insider assaults. The security system makes utilization of two ideas known as profiling and decoy data. Clients who access the cloud to see their own information and furthermore perform information elements are required to have some particular examples of utilization. Such clients are known due to their behaviour pattern.

This ordinary conduct of clients is profiled in the principal stage. At that point imitation data is kept in document framework other than tossing various society equations. The insider attack by large don't have the conduct of eligible client. Hence they are pulled in to utilize imitation data. As the bait data isn't the genuine information there is no issue when programmer utilizes it or takes it. In any case, the navigational examples of the malignant insider can be contrasted and the navigational examples of authentic clients. The anomalous conduct must be suspected.

The genuine client of cloud acts typically and his exercises coordinate the general profile of any such clients. At the point when imitation data, for example, fake data, nectar records and bait archives are brought into the document framework, at that point the route of certified clients will be same as they endeavor to utilize the legitimate substance of their own.

In any case, when attackers attempt to utilize the framework, they are unquestionably pulled in towards fake data. The distraction innovation is extremely valuable as it deludes noxious insiders. Whenever the fake innovation is utilized against a client profile, it is saved as to know the associated conduct with clients and that way it is conceivable to anticipate insider information burglary assaults.

The model application makes utilization of the two methodologies together to distinguish insider information robbery assaults. At the point when an insider hacker attempts to utilize Cloud for information elements, he gets pulled in to sham data which seems delicate and valuable to programmers. Thus the proposed application beguiles vindictive clients to carry on that way and maintain a strategic distance from insider burglary assault. The exploratory outcomes uncovered that the blend of both the procedures, for example, client profile administration and furthermore the bait innovation could yield best outcomes. The accompanying segment demonstrates the usage of the model application.

7. ALGORITHM

The concept of providing fake record is that the hacker does not instigate more request to crack the users personal information. In addition keeping in mind the hacker has already obtained the eligible user credentials and is in the system, this type of

security is still a wider issue in todays day. [19] . Following are a few points which the basic algorithm covers while trying to secure a user personal information form being leaked.

A. Pattern Generation

Occasions are caught and put away in the log, the following step is to perform design age that shapes the profile of the client dependent on the arrangement of occasions executed by the client. With the end goal to precisely decide the standards of conduct of the clients, the personal conduct standard of the client is profiled by preparing every client on how they are required to carry on in the framework when given genuine access. Deciding if a client is a malevolent client or not without having a predefined standard of conduct is troublesome. We are not asserting that profiling the standard of conduct of the client is the main answer for the issue of moderating pernicious insiders, yet we are accentuating that profiling client standard of conduct gives a method for managing with the issue of insider dangers.

B. Detect Anomaly

Behaviour of a user is saved during the initial alloted time period. When the user logs in then their behaviour is compared to the past behaviour. On the off chance that the client conduct is surpassing the edge esteem or a limit, the remote client is suspected to be peculiarity, they are presented with decoy data. On the off chance that the present client conduct is as the past conduct, the client is permitted to work on the actual data. [1]

C. Suspicion Detected

If the current client's conduct appears to be suspicious, at that point the client is requested to give answers to arbitrarily chosen mystery questions. On the off chance that the client neglects to give rectify answers to a specific breaking points or edge, the client is given fake records. In the event that the client gave remedy answers as far as possible, the client is treated as should be expected client. Sub subsection . [1] [19]

D. Pattern Matching

The end goal to identify the client standard of conduct, we utilize the consecutive example mining system. Consecutive standard coordinating methodology utilizes a mining system to recognize designs, by looking at the current produced design with the one put away in the client profile to see if the personal conduct standard is still predictable with the past personal conduct standard. In the event that the personal conduct standard put away in the client profile isn't the equivalent with the current example we accept that there is a likelihood that a client is a malignant client or there will be consequences if the personal conduct standard is steady with the one put away in the client profile, we accept that the client is the authenticated client. [13]

E. Generating Decoy data

The key test in producing decoy data is that it ought to seem reasonable and in-discernable fromatted. The main objective is for imitation solicitations to convey indistinguishable properties from the real client information and make the server to carry on similarly. We expect that genuine and bait calculation on an application reproduction is the equivalent as long as, given a genuine and a relating distraction ask for, comparative or indistinguishable code execution ways are pursued. As of now, we don't put any setting related requirements (e.g., a progression of legitimate convention messages or application asks for that a client would be probably not going to perform in a particular request) as we expect that an aggressor would not endeavor to recognize distractions in such way. Be that as it may, our methodology can be stretched out to incorporate more imitation assessment heuristics. Formats are utilized to produce random stages in the adequate esteem space for the parameters or substance of a given message type.

For example, if the message is a HTTP GET ask for conveying the "Stick" parameter with a space of four numeric characters ([0-9]f4g) the system would create all changes [20]. On the other hand, for a "seek word" parameter with a space characterized by a lexicon of the English dialect we would create a suitable number of distractions or enough practical baits to fulfill a given share. The framework at that point assesses all created baits against the genuine client contribution from a preparation set utilizing the heuristics specified previously. Distraction messages that show comparable or indistinguishable application server conduct are kept, while the rest are disposed of. As powerful paired instrumentation is computationally costly, we make a period space exchange off and store the created fakes for sometime later instead of do continuous age and assessment.[7]

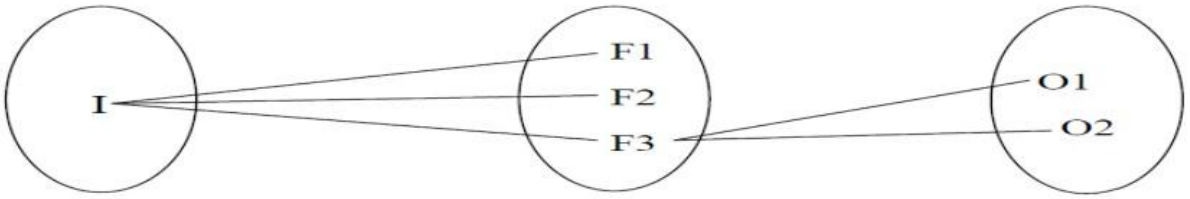

Fig. 2. Mathematical Model

8. MATHEMATICAL MODEL

The following model depicts the process in a set formation, to easily understand how the system is to implement the business flow. [21] [22]

Let, S be the System Such that,
A= {I, O, F, success, failure} Where,
I= Login details
O= Decoy file
F =Detecting user behavior and Download decoy file

Input:
I=Enter invalid login details.

Function:
F1=Check user login details [22]
F2= find Anonymous activity
F3= if user behavior is illegal to download decoy file

Output:
O1=Success Case
The user is behaving normally it will get original file and if anonymous will get decoy file
O2=Failure Case

1) A huge database can lead to more time consuming to get the information.
2) Hardware failure.
3) Software failure

CONCLUSION

Increase in industry confidential data being saved on the cloud and accessed via Fog computing i.e. usage of computing at node (device), the security of data became a serious issue, for which implementation of security for fog computing which constitutes of a combination of User profiling and decoy data. User profiling instigates monitoring and prediction of user behaviour, after interpreting any abnormal pattern decoy data which can be dynamically generated for attackers; Sequence learning plays an important role in User Profile characterization as the system maps user behaviour to specific patterns so it can distinguish between legitimate and fake users. The idea is to scramble the original data in a manner which a hacker would not be able to distinguish, so it can mislead the attacker into thinking they have obtained the original data; to limit the chances of data being retrieved by illegitimate users by using this attack of preventive disinformation.

ACKNOWLEDGEMENT

I would like to express my sincerest gratification to my teachers, for all their guidance and patience in addition to all the facilities they provided during the entire creation of this research, which has allowed me to grow in learning as well as being able to present this topic. Their encouragement and motivation is highly appreciated. Above all I would like to thank my family for guiding me in this time.

REFERENCES

[1] S. A. A. A. Alsaidi, "Protect Sensitive Data in Public Cloud from an Theft Attack and detect Abnormal Client Behavior," *ijesc*, May 2014.
[2] Y. Yang, X. Zheng, and C. Tang, "Lightweight distributed secure data management system for health internet of things," *Journal of Network and Computer Applications*, Nov. 2016.
[3] V.Sriharsha Student, "Dynamic Decoy File Usage to Protect from malicious insider for data on public cloud," vol. 1, Oct. 2013.
[4] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Wenjing Lou, and Patrick P.C. Lee, "Secure Deduplication with Efficient and Reliable Convergent Key Management," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 25, June 2014.
[5] P.Jyothi, R.Anuradha, and Dr.Y.Vijayalata, "Minimizing Internal Data Theft in Cloud Through Disinformation Attacks," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, Sept. 2013.
[6] Gayatri Kalaskar, Purva Ratkanthwar, Prachi Jagadale, and Bhagyashri Jagadale, "FOG Computing: Preventing Insider Data Theft Attacks in Cloud Using User Behavior Profiling and Decoy Information Technology," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 32, Feb. 2016.
[7] Miss. Shafiyana Sayyad, Mr.Anil Bhandare, and Mr. Deepak Yelwande, "Fog Computing: Software decoys for insider threat," *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, vol. 2, Mar. 2015.
[8] G. Kurikala, K. G. Gupta, and A. Swapna, "Fog Computing: Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 2, no. 4, pp. 176–181, 2017.
[9] L. Yeh, P. Chiang, Y. Tsai, and J. Huang, "Cloudbased fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation," *IEEET transactions on Cloud Computing*, Oct. 2015.
[10] Botta Alessio, Antonio Pescape, Donato de Walter, and Valerio Persico, "Integration of Cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.
[11] U. P. Das, R. VijayaKumar, and B. R. Ravishankar, "Securing Data in Cloud using Disinformation Data in Fog Computing," *International Journal of Computer Science Trends and Technology (IJCST)*, June 2018.
[12] S. Virushabadoss and C. Bhuvaneswari, "Analysis of behavior profiling algorithm to detect usage anomalies in fog computing," *One Day National Conference On Internet Of Things - The Current Trend In Connected World*, 2018.
[13] Lucky Nkosi, Paul Tarwireyi, and Matthew O Adigun, "Insider Threat Detection Model for the Cloud," *IEEE*, 2013.
[14] Shreya Waghmare, Shruti Ahire, Himali Fegade, Pratiksha Darekar, "Securing Cloud using Fog Computing with Hadoop Framework," *International Journal of Science, Engineering and Technology An Open Access Journal, Shreya Waghmare et al*, vol. 5, no. 3, 2017.
[15] Blesson Varghese, Nan Wang, Dimitrios S. Nikolopoulos, and Raj Kumar Buyya, "Feasibility of Fog Computing," *arXiv preprint arXiv:1701.05451*, Jan. 2017.
[16] T. R. Kulkarni, V. Waghmare, D. Chaudhary, and P. Kulkarni, "Security Implementation in cloud computing using User Behavior Profiling and Decoy Technology," *World Journal of Technology, Engineering and Research*, 2018.
[17] Umesh K. Gaikwad and Shirish S. Sane, "Effective Classifier for User's Behavioral Profile Classification," *International Journal of Computer Science and Information Technologies,*, vol. 5 (3), 2014.
[18] V. K. Goar, "Different Approach to Secure Data with Fog Computing," *IJFRCSCE*, march 2018.
[19] M. Mukherjee et al. Rakesh Matam, Lei Shu, Vikas Kumar, Lenadros Maglara, Mohamed Amine Ferrag, and Nikumani Choudhury, "Security and Privacy in Fog Computing: Challenges," *Security and Privacy in Fog Computing: Challenges*, Oct. 2017.
[20] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "Cca-secure abe with outsourced decryption for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 730–738, 2018.
[21] KM Reena, Sunil Kumar Yadav, and Nikhil Kumar Bajaj, "Security Implementation in cloud computing Using User Behaviour Profiling and Decoy Technology," *International Conference on Inventive Communication and Computational Technologies*, 2017.
[22] T. H. L. Gao, Yang Xiang, Zhi Li, and Limin Sun, "Fog Computing: Focusing on Mobile Users at the Edge," *arXiv preprint arXiv:1502.01815*, Feb. 2015.