International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 14-19

Analysis of Behavior Profiling Algorithm to Detect Usage Anomalies in Fog Computing

S.Virushabadoss[1], Dr.C.Bhuvaneswari[2]
[1](*Dept. of Computer Science, Adhiparasakthi College of Arts and Science / Thiruvalluvar University, India*)
[2](*Department of Computer Science, Thiruvalluvar University Model College of Arts and Science / India*)

Abstract: *Fog computing is the term coined by Cisco which is cloud computing extent and decentralized computing infrastructure in which several data were stored and subjected for computation. But the new computational theories have brought up the data security challenges against several security mechanisms in cloud. For instance, if an unauthorized activity is detected in a network, then to deceive the attacker we send large amounts of decoy information. This protects the real user's data. In Fog networks a user behavior gets changed when a system given a set of commands sequentially and it is easy to monitor the evolving nature of a user. This paper discusses the behavior profiling algorithm technique to overcome those issues in fog systems. The work carried out in this paper deals with selection of the best statistical metrics for identifying rouge nodes and it could be applied to any networks where user behavior seems to be anonymous by their sequence of actions.*

Keywords: *Behavior Profiling, Cloud Computing, Data Security, Decoy System, Fog Computing.*

I. Introduction

Fog networking is a collection of different things or devices which supports IOT techniques. Using this extension of cloud technique, larger to smaller organizations protects their data and as well as use that when they are in need. In this real world, the challenge often faced by administrator is their security over the huge databases. Internet of things systems for Industrial and commercial networks are not complicated but designing them is pretty much. Whenever the communication between local networks or through IP address in global internet, then the detection of anomalies were quite challenging, especially in cloud. Since, the existing techniques supports the certain security features but not allowing the unauthorized access detection and its resistance over valid data distribution, then it's time to implement certain strategies to address security issues. Fog networks communicate through access points, base stations, set-top boxes and such things (IOT) required mobility and geo-location access support and minimum latency. Because of that, it opens threat from all sides. The proposed fog computing mechanism facilitates security features to data which allows the detection of invalid access. Hence it prevents to enable valid data distribution over the networks. Cloud, Fog and devices give a three tier service delivery architecture which supports wide range of applications, say, augmented reality, big data analytics and content delivery in web applications. As fog computing is still in its earlier stage, it needs a clear and effective work on security and privacy might provide advanced security to the data stored in the cloud.

This paper is organized as several sections: Section 2 represents the survey on user behavior pattern for security in networks. Section 3 provides a related works on behavior profiling and existing classification systems. Section 4 describes the security implemented in cloud with fog systems and Section 5 gives the algorithm to provide decoy information according to user behavior pattern classification. Section 6 contains concluding remarks.

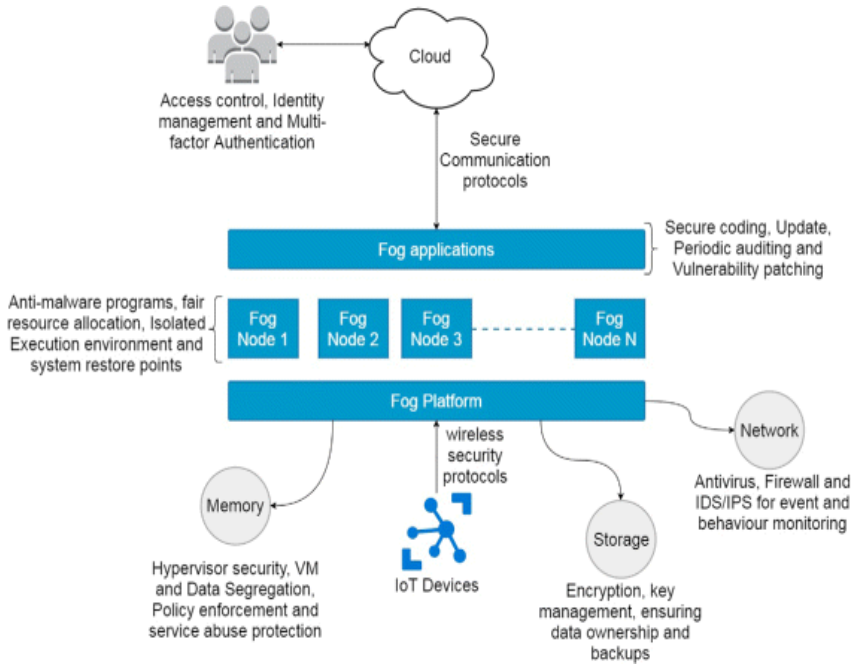

Fig.1 FOG Infrastructure Architecture

II. Literature Survey

According to the research paper entitled "Top threat to cloud computing" published by University of Derby [1], all major concerns including Google, Microsoft, Amazon etc. using cloud services since it has many advantages such as increased usages of hardware resources, reduction in costs, scalability and feasible in deployment. Hence the increasing rate of customers who gets on with cloud services such as Dropbox, Facebook, Linked in and I Cloud become inevitable.

ULTEO: Ulteo is a commercial open source VDI, with the security and backing of a commercial enterprise. Their objective is to deliver non-proprietary platforms built on innovation, independence and an open architecture. It offers the most cost efficient application delivery platform to the market today, with Ulteo Virtual Desktop Community Edition at free of cost and Ulteo Premium Edition giving administrators the ability to deliver applications. OVD is more of a graphical terminal server that manages desktop sessions and delivers them to a variety of endpoints on the network, whereas a genuine VDI solution is based on virtualization technology and allocates virtual machines with an enterprise desktop operating system, generated from a blueprint, to the clients as required [1].

DROPS: Division and Replication of Data in the Cloud for Optimal Performance and Security. This technology divides a file in to five segments and sends a copy to the cloud nodes. Every node stores only a single segment of a particular data of a file such that no real information revealed even when the attacks carried over successfully.

SPLUNK: It is a user behavior solution to find unknown threats and behaviors across users, end devices and various applications. Their machine learning algorithms focuses on external attacks, internal threats and produce supporting evidences through security operation center (SOC) and also it presents security analysis with important points visually which helps in investigating anonymous behavior. The Splunk enterprise security for data correlation supports on data scoping and automatic responses by bi-directional integration with UEBA.

III. Existing System

Every layer in the fog computing system should be addressed with necessary security features and here are some existing security models.

3. TRUST AND AUTHENTICATION

Generally cloud data centers are owned by cloud service providers but for fog computing services it could be different parties due to the choices available on deployment.

- One way to build fog networks with the infrastructures of wireless carriers which have the control on gateways and provide authentication. Another way of building fog networks by the cloud service providers by expanding their services to the edge of the network.
- When the private cloud turn in to fog by the end users to lower the cost of ownership and lease the spare resources on the cloud, the trust and authentication over the fog network arises.

3.1 Trust Model: There are some issues need to be addressed in the reputation based systems. For instance, how to achieve distinct identity and treatment on intentional and accidental usages and attaining redemption of reputation? In a research paper [2] author proposed a reputation model for resource selection with its reliability in peer-to-peer networks using an algorithm known as distributed polling. Some of the trust models based on unique hardware might provide trust utilities in fog computing applications such as Secure Element, Trusted Execution Environment or Trusted Platform Module. The Trust model [3] yields success in e-commerce, peer-to-peer, user reviews and social networks.

3.2 Fake nodes in Fog: A big threat to the user data in a network communication are fake nodes. Most of its problems are difficult to address, especially in fog system. Problems such as complex trust situation calls for different trust management schemes and maintaining a blacklist of unauthorized nodes were hard since problems on dynamic creating, deleting of virtual machine instances. And also author Han [4] proposed the measurement method to avoid connecting rouge access point.

IV. Data Security With Fog System

Until now the major challenge in fog computing is providing desired security over confidential information and its level of assurance to people. Especially problem which concern in securing user data such that no other user can gain access. Whenever a user connects to the internet then the storage of files, documents and media in remote places takes place based on different cloud services and different proposals exists for that.

In order to secure the data in cloud, there has been many approaches like standard encryption methods, standard access to controls were made. But all were failed from time to time for various reasons like lack of security procedures, error codes, insider attacks, wrong implementations, failed to envision on creative and effective attacks and misconfigured services. Although providing a trustworthy cloud computing environment is major objective, it's really tough to prevent such attacks in real time, so we can limit the damage of stolen data by decreasing the value of that information to the attacker through preventive disinformation attack [5].

Using decoy information as a database for validating the alerts raised by monitoring system carried out by sensors and generating the decoys during that time might improve the efficiency and accuracy of the security in network systems [8].

V. Proposed System

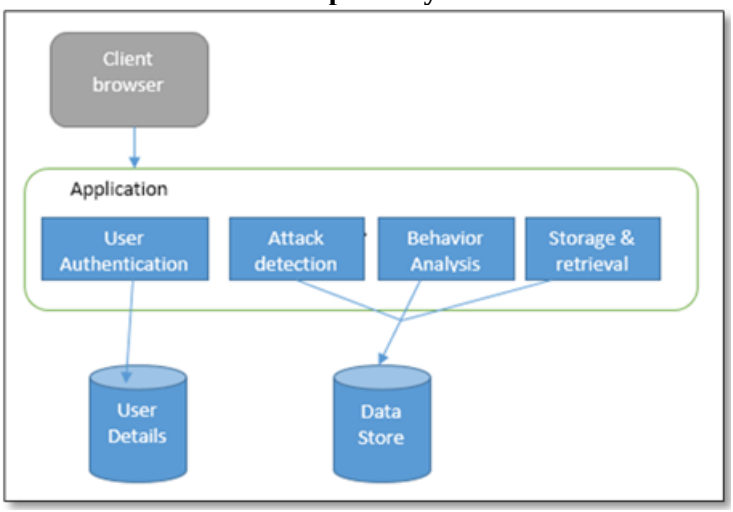

Fig. 2 System Architecture

5. Behavior Profiling Mechanism:

It is a technique used to find how much a user accessed their information in the web and also used in the commercial sites to detect the fraudulent and track the unusual behavior of a user. Building such a model in fog systems has been really effective since a normal means of access in a cloud service has been continuously

checked to identify the any abnormal behavior access to a users' information. This process might include volumetric information on how documents were treated.

The above diagram shows an entire model on user profiling mechanism and decoy technique. It mainly deals with the user's behavior system and checks for user's legitimacy. If systems find any unauthorized activity then it sends disinformation data and keeps real data safe of a user.

Closure on User Behavior Profiling:

1. Look for an unusual behavior among users.
2. Monitor that user's behavior profile with their information such as username, password specified, and user key etc., [6].
3. Tracing of login passwords.
4. During document access, the user key specified is tracked along with the type of operation i.e., valid or invalid.
5. Classify profile as valid or invalid using the following mathematical operation: P (4) = count (invalid operations/operations),

If the result of P is above a threshold parameter then the profile is categorized as invalid and the user is redirected to the decoy module [6].

Advantages of placing decoy files in database are:

1. The detection of unauthorized access.
2. The confusing the attacker with duplicate or wrong data.
3. Sending bogus files.

Algorithm:

Let A be the superset of all sets.

A ≡ {input, output, operations, success, failure} Where, Input is set of parameters provided as input to system.

Input ≡ {U, Z, DS, F} U is set of users. It is infinite set of users, U ≡ {U1, U2, U3……UN}

Z is set of servers. It is finite set of servers, Z ≡ {Z1}

DP is set of dataset parameters.

DP ≡ {P1, P2, P3, P4, P5}

P1 ≡ Session Time, P2 ≡ Duration, P3 ≡ File upload count, P4 ≡ File Download count, P5≡ Blacklist count

F is set of files. It is Infinite set of files, F ≡ {F1, F2, F3……, FN}

Output is set of results.

Operations are set of functions.

Operations ≡ {Op1, Op2, Op3, Op4, Op5, Op6, Op7, Op8, Op9}

Operations are for Request received, Load user profile, apply mining & calculate current request parameter, if invalid user then send the Decoy/Bogus data, Fetch file, Calculate digital signature, Compare with decoy file digitally, If similar, Alert admin, Update log, Blacklist respectively.

If desired input generated then its SUCCESS else it generate FAILURE message.

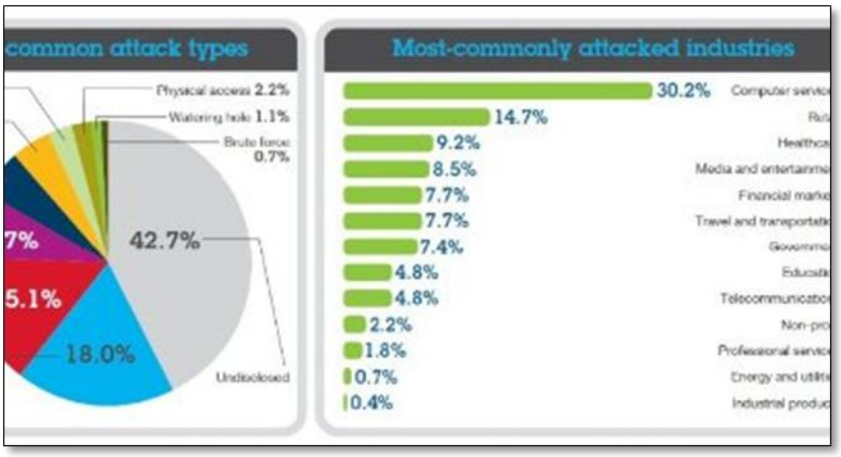

Fig. 3 Common attack types

Results:

As far as the results are concerned, implementing these techniques in QRADAR yields 90% of positive results [Fig.3] The following sample screenshots of qradar [Fig.4] displays the suspicious content browsing along with its source addresses and bandwidth. [Fig.5] brings the recent and severe offenses with its source and destination addresses with its category type processed by QRADAR. After identifying the illegitimate access, the decoy information's send to the attacker in order to prevent the real user's data.

Fig. 4 Scores on Suspicious content browsing along with its source addresses and bandwidth.

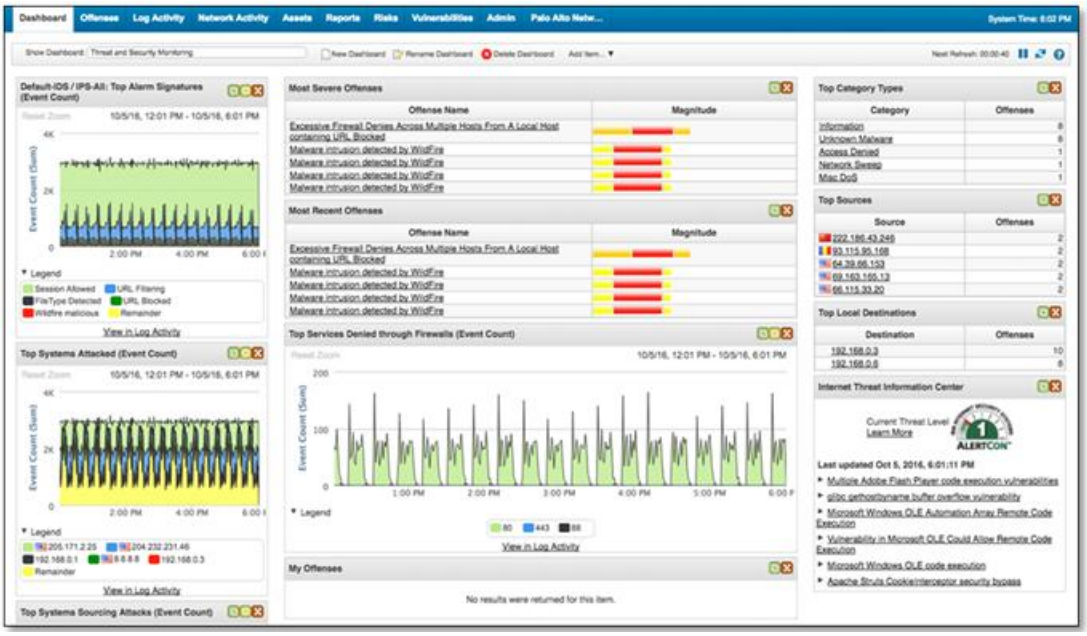

Fig. 5 Log Activities of recent and severe offenses with its source and destination addresses.

VI. Conclusion

One of the most difficult tasks of the data society is dealing with exponential growth of data overload. Especially when the data's were outsourced to third party might raise the concern over privacy and security. This paper analyzed the behavioral profiling algorithm which monitors the unauthorized data access in a network. It ensures that the navigate patterns were recorded and using best statistical products like Qradar yields the results mark up to 90% in detecting an anonymous behavior. The decoy information saved in the fog with the original data of a user could detect the illegitimate access and it also lookup for an insider who access real user's documents in a cloud service.

This process might be extended to mist computing where the clouds were bought near to the data centre where it's been created and accessing the information with protection on such networks become feasible by implementing user behavior algorithm.

References

[1]. Muhammed Kazim, Cloud Security Alliance, "*Top Threat to Cloud Computing V1.0*," University of Derby, March 2010.
[2]. Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, "*Fog Computing: Mitigating Insider Data theft Attacks in Cloud*".
[3]. Tom H. Longxiang Gao, Yang Xiang, Zhi Li, Limin Sun, "*Fog Computing: Focusing on Mobile Users at the Edge*", 6th Feb 2015.
[4]. Younghee Park, Salvatore J. Stolfo, "*Software Decoys for Insider Threat*", ACM.
[5]. Miss. Shafiyana Sayyad, Mr.Anil Bhandare, Mr. Deepak Yelwande, "*Fog Computing: Software decoys for insider threat*", Volume 2 issue 3 March 2015.
[6]. Gayatri Kalaskar, Purva Ratkanthwar, Prachi Jagadale, 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) – Volume 32 Number 7- February 2016.
[7]. Aatish B. Shah, Jai Kannan, Deep Utkal Shah, Prof. S.B.Ware, Prof. R.S.Badodekar, "*Fog Computing: Securing the cloud and preventing insider attacks in the cloud*."
[8]. Umesh K. Gaikwad, Shirish S. Sane, "*Effective Classifier for User's Behavioral Profile Classification*", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.