Security and Privacy Issues of FOG Computing: A Survey

SHLOK ROY [1], ANKITA JIYANI[2]
[1, 2] *Department of Computer Science and Engineering, Poornima College of engineering*

Abstract -- As with the increase in modernization everything is being getting cloud based. From a some firms to multinational organization everyone is using cloud for storage and management of their data that can be use further to create, distribute, storage manage analysis or for supporting decision making through a centralized computing infrastructure. FOG Computing is an extension of cloud computing that deals with the decentralized computing infrastructure. In fog computing the data in distributed among various logical places between cloud and data source. As the data in decentralized which results in security issues for the storage and usage of data. This paper deals with various kinds of security and privacy issue in context of fog computing that will be helpful for securing the data in cloud in a efficient manner.

Index Terms - FOG Computing, Access Control

I. INTRODUCTION

Cloud Computing is branch of new developing advance computer science that provides if provide provides shared configurations among the system resources and a high level services that easily monitored and maintained without any excess extra efforts over the internet. Cloud Computing is an useful technology used by organization at a very high level but it too comes with security issues as the data is in cloud and the service provider can easily access it anytime. There is also a third party that to have the rights to access as well as use the data on cloud. The various solutions to the privacy include user's choice of data storage and many policy and legislation. FOG Computing is also known by fogging or fog networking. Fog computing is a decentralized computing infrastructure .It deals with the data, storage, compute and applications are distributed depending upon the logic .It is at the most logical and efficient place between cloud and the data source. Fog computing is an extended version of Cloud computing. The main motive of developing fog computing is to improve the efficiency and to overcome the loop holes of cloud computing. Fog computing reduces the amount of data transfer to cloud for processing, analysis, and storage of data. It is also used for security and compliance reasons.

II. HOW FOG COMPUTING WORK

Data generated and collected through various devices and seniors doesn't have their own computing or storage resource to apply various kinds of analytical or machine learning tasks on the data collected by them they require some additional resources. There requirement is being fulfilled by cloud servers as they do have the power to do all these tasks, these servers are too far away to far away to process these data give a real time response. In addition this which have all the end points connected and sends the raw data to the cloud over the internet. This may have some privacy, security and legal issues especially when they are dealing with sensitive data subjects. In fog environment, the processing of these tasks takes place in data hub on a smart device or by smart router or gateway which results in reduction of amount of data processing to the cloud.

III. ADVANTAGES AND DISADVANTAGES OF FOG COMPUTING

Advantage	Disadvantage
1. Reduces amount of data to be sent on cloud.	1. Physical location takes away from the anytime, anywhere, any data benefit of the cloud.
2. Conserve network bandwidth.	2. Security issue: IP address spoofing, man-in-the-middle attacks

3.Improve system response	3.Privacy issues
4.Support mobility	4.Availabilty/Cost of log equipment/hardware
5. Improve security issue by keeping data close to the edge.	5. Trust and authentication concern
6.Minimizes network and internet latency	6.Wireless network security concerns

IV. LITERATURE REVIEW

The present system provides only the single authentication which is not much secure and can easily be hacked by hackers[1].The system does not provide any additional security like security questions for more security. The hackers can easily get into the cloud and search for the files that available [2].State-of-the-art applications are typically deployed on top of cloud services which offers the illusion of infinite resources, elastic scalability, and a simple pay –per-use billing model[1].Future application domains such as the Internet of Things, autonomous driving, or future 5G mobile apps, however require low latency access which is typically achieved by moving computation towards the edge of the network[1]. Fog computing is a promising computing paradigm that extends cloud computing to the edge of network [2].Similar to cloud computing but with distinct characteristics, fog computing faces new security and privacy challenges besides those inherited from cloud computing [2].

Threats in cloud

1. Data breaches – It leads to the loss of credit card information and personal information's of around 110 million users, it was a theft that has been occurred during processing and storing data.

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.

3. Account or service traffic hijacking – Account can be hacked if the login credentials are lost.

4. Insecure API's – Application Programming Interface controls the third party and verifies the user.

5. Denial of service – This occurs when millions of user request of same service and the hackers take this.

6. Malicious insiders – This occurs when a person close to us knows our login credentials.

7. Abuse of cloud services – By using many cloud servers hacker can crack the encryption in very less time.

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 [1].

V. PROPOSED WORK

- We propose a distinct approach to secure cloud known as Fog Computing.
- We use decoy information and user behaviour profiling to secure data on Cloud.
- The proposed mechanism facilitates security features to data and thereby allows for detection of invalid access.

It provides prevention to enable valid distribution of data.

Algorithms Used

User behaviour Algorithm:

It will take user id as input.

1) Set THREASH = 0.5f; COUNT = 4, MIN_RECORDS = 5;
2) In an Array List we will Store Some actions.
   l.add("wrong key"); l.add("invalid");
   l.add("trialkey"); l.add("decoy");
   l.add("editpwdwrongkey");
   l.add("editpwdtrialkey");
   l.add("wrongpwd"); l.add("trialpwd");
3) Takes number of rows in the log details table for that user.

4) If the number of rows less than minimum records, returns validate.

5) Else Set invalid=0Takes action from the log details of that user, if it contain any operation mentioned in the array list invalid count will be incremented.

6) It will calculate Set value=0, row=0 Value = value + (((float) invalid) / ((float) COUNT));

7) find avg = (number of rows for that user in log details tab / 2) if value>=THREASH, increments row.

8) This will repeat for all rows .If rows > avg, returns invalid date. Else returns validate. In short, User behaviour algorithm returns the behaviour of that particular user based on the entries in log details table. if this returns invalidate then in the action column decoy will be entered. Suppose If the user entered correct password and he got access. At the time of downloading he entered correct key. Then User behaviour algorithm will execute. It will take number of invalid entries in the table and returns either validate or invalidate. If its return invalidate then during downloading he will get decoy file even if that user enter correct key. In every case this algorithm will execute. At the time of key recovery it will be verified using challenging questions.

VI. CONCLUSION

This paper discusses several security and privacy issues in the context of fog computing, which is a new computing technique which provide elastic resources at the edge of network to nearby end users. We have also discussed security issues such as secure data storage, secure computation and network security. We also highlight privacy issues in data privacy, usage privacy and location privacy, which may need new think to adopt new challenges and changes.

We present an approach for securing business data in the cloud. Once unauthorized access or exposure is suspected, and later verified, with challenges questions for that instance, then we inundate this malicious insider with bogus information in order to dilute the user's real data.

REFERENCES

[1] Jayshree Khandagalel , Deepak Fodse2, Poonam Sul3, Prita Patil, "FOG Computing"2016

[2]. David Bermbach1 , Frank Pallas1 , David Garc'1a P' erez2, Pierluigi Plebain3, ''A Research Perspective on Fog Computing",2017.

[3] Ben-Salem M., and Stolf Angelos D.Keromytis, "Fog computing: Mitigating Insider Data Theft Attack in the Cloud,"IEEE symposium on security and privacy workshop(SPW)2012

[4] C.Wei, Z.Fadlullah, N.kato, and I.Stojmenovic,"On optimally reducing power loss in micro-grids with power storage devices,"IEEE Journal of Selected Areas in Communications, 2014 to appear

[5] Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. WCMC 13 (2013)

[6] Dsouza, C., Ahn, G.J., Taguinod, M.: Policy-driven security management for fog computing: Preliminary framework and a case study. In: IRI. IEEE (2014)

[7] Dwork, C.: Differential privacy. In: Encyclopedia of Cryptography and Security. Springer (2011)

[8] ETSI: Mobile-edge computing. http://goo.gl/7NwTLE (2014)

[9] Gao, Z., Zhu, H., Liu, Y., Li, M., Cao, Z.: Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In: INFOCOM. IEEE (2013)

[10] Gennaro, R., Gentry, C., Parno, B.: Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: CRYPTO. Springer (2010)

[11] Gil Press: Idc: Top 10 technology predictions for 2015. http://goo.gl/zFujnE

[12] Ha, K., Chen, Z., Hu, W., Richter, W., Pillai, P., Satyanarayanan, M.: Towards wearable cognitive assistance. In: Mobisys. ACM (2014)