International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 9 100- 102

A Survey on Fog Computing: Services, Data and Security

Palash Hinglaspurkar
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
Palashhinglaspurkar10@gmail.com

Bhanuprasad Harinkhede
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
bgharinkhede@gmail.com

Ankit Meshram
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
meshram.ankit@gmail.com

Jayesh Patel
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
Jayeshpatel1994@gmail.com

Sagar Fale
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
Sagarfale8@gmail.com

Prof. Shailesh Kurzadkar
Computer Sci. & Engineering
Nagpur Institute of Technology
Nagpur, India
skurzadkar@gmail.com

***Abstract*—..** Cloud computing can be used as a delivery platform which is a promising way for storing user data and provides a secure access to personal and business information. It involves prevention form risks like data theft and various other attacks. Cyber criminals can access the documents which can results in misuse of data and also interpretation of highly confidential data for illegal purposes. For securing user data from cyber attacks a new paradigm called fog computing can be used. This technique can monitor the user activity to identify the legitimacy and prevent from any unauthorised user access. Fog computing is a computing technique that extends cloud computing to the edge by providing Security in the cloud environment.. In fog computing , new security and privacy challenges are to be faced that are inherited from cloud computing. Mainly fog computing is used to reduce the burden on cloud by gathering workloads, services, applications and huge data to near network edge. In this paper we have discussed this paradigm for preventing misuse of user data and securing information, challenges and corresponding solutions in a brief manner.

Keywords*-*cloud computing; Fog computing; Decoy technology; Data security and Insider theft attacks, security, privacy.

*****

I. INTRODUCTION

In last few years cloud computing gained huge popularity from corporate world to real time applications.

Information can be access any time and from anywhere only because of cloud computing. Cloud computing provides various advantages to its end-user such as cost efficiency, Backup and Recovery, Easy Access to Information, Quick Deployment, Automatic Software Integration but there are some disadvantages also related with cloud like Security Issues related with database, Limited control and flexibility.

Fog computing is proposed to enable computing directly at the edge of the network, which can deliver new security services especially for the future of cloud. For example, commercial cloud are providing data.

It is a highly virtualized platform that provides computation, storage, and networking services between end devices and traditional cloud servers.

II. RELATED WORK

Sayali Raje et al [2] have proposed that, the Fog that are; 1.Mobility, 2.Location awareness, 3.Low latency, 4.Huge number of nodes, 5. Extensive geographical distribution, 6.Various real time applications and we explore the advantages and motivation of Fog computing, and analyze its applications for IOT in conference paper.

Divya Shrungar et al [1] have proposed that the fog computing and the security related issues are not overcome yet.In our research paper we are proposing the user profiling technique with some new facilities, that include the image captcha process, that specifies wheather the user is human hacker or machine hacker. Also we are implementing the psychometric test after the image capcha process is cracked. Here we will introduce the façade technology that will redirected aurthorised user to the original server and unaurthorised or hacker to the fog server.

III. Cloud Computing

There are two basic working models of cloud such as Service Models and Deployment Models.

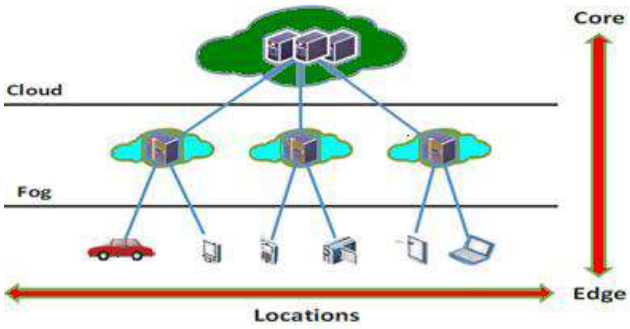
1.1.1 Service Models Service Models are the reference models on the basis of these models we can choose cloud provider. According to your need you can choose cloud services. These can be categorized into three basic service models as listed below: Software as a Service (SaaS) : This model provide the facility to the user to pay for any application or service to access anywhere any time from the cloud. This model uses third party vendor. All applications are delivered through and managed by a third-party vendor and whose interface is access on the user side Platform as a Service (PaaS) : This model provide the facility to the user to pay for the access to the platforms, allow them to deploy their own applications and software in the cloud. Infrastructure as a Service (IaaS) : This model provide the

facility to the user to manage and control the systems in terms of the applications , operating systems, network connectivity and storage but there is no need to control the cloud infrastructure. There are various other service models like XaaS, i.e., anything as a Service. This can be Business as a Service, Database as a Service, Network as a Service, Strategy as a Service or Identity as a Service.

1.1.2 Deployment Models the deployment models have been identified according to needs of the services and users of the clouds in specific ways with the different characteristics of the four different models. Private Cloud: This cloud infrastructure has been deployed, operated and is maintained by a particular organization and not shared with other organizations. Community Cloud: This cloud infrastructure is shared with a number of organizations with similar requirements and interests. Public Cloud: This cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This model provides an on-demand solution Payment is made on a per use basis. Hybrid Cloud: This cloud infrastructure is combination of clouds of any type. This can be a combination of public and private clouds or public or community cloud according to the need of services and applications required by the end user.

IV. FOG COMPUTING

Cloud computing carried out closer to the end users' networks is thus identified as fog computing. Fog computing is a creation of virtualized platform that is located between cloud and end user devices. Fog computing can provide better Quality of services in terms of delay and reduced data traffic over the internet etc. Keeping the Data close to the user, to eliminate the delays in data transfer fog allows keeping the data close to the user instead of store them in a far datacenters.



Great mobility: There is a very highly growth in the amount of data and devices. A fog system supports to handle this large data and information and provides a better and faster way to access, controle and analyze the data. Fog computing would be a great option to prevent the data in the proper manner or distinct information to pass to the overall network. This will reduces the delay.Fog computing concept can be applied in a number of areas where Internet of Things is present. It will play an important role in various applications in IOT.

A. *User Profiling Technique*

This is where we use user profiling technique in this technique we judge the behavior of the user. In this we are taking the information from the user, in which some of the field is mandatory. Then after for each user the unique id is generated, that is used at the time of user login.

At the end when the user is successfully registered into the system, then the user can login into our portal automatically the ip address of the user from where the user is currently login is stored in the admin's database.

B. *Authentication*

Authentication is an important issue for the security of fog computing since services are offered to massive-scale end users by front fog nodes. We have considered the main security issue of fog computing as the authentication at different levels of fog nodes. Existent authentication is not efficient and has less scalability. We have proposed a secure and user-friendly solution to the authentication problem in local wireless network, relying on a physical contact for pre-authentication in a location-limited channel.

We have proposed user profile behavior technique for the authentication. And some extra security services.

C. *Decoy Technology*

This is where decoy technology is used, which means confusing the attacker by placing trap files (that are fake files appearing real to the attacker) in the user's file system. The system is secure so whenever the attacker enters the system he will open the files to which the access is open and will search in a random manner, but here in the system only those files are left open to the users which are trap files. So when the attacker will open the trap file the abnormality in user behaviour will be detected. With Cusum change point will be detected.

D. *Figures and Tables*

Parameters	Cloud Computing	Fog Computing
Server nodes location	Within the Internet	At the edge of the local network
Awareness about location	No	Yes
Number of server nodes	Few	Very large
Security	Less secure, Undefined	More secure, Can be defined
Mobility	Limited support	Supported

Figure 1. Comparision of Cloud computing and Fog computing

*V.*CONCLUSION

This survey discusses security services of fog computing with similar concepts, gives representative applications which will promote fog computing, and mentions various aspects of issues we may encounter when design and implement fog computing systems. Besides, new opportunities and challenges in fog computing for related techniques are discussed and issues related, security and privacy are highlighted.

VI. FUTURE SCOPE

This fog computing application can be used in any kind of portal. For e.g. in banking, organizations, corporate world etc. It have been also be used in any cloud environment, too stored and load data into the cloud. It also played the vital role in the IOT in future.

VII. ACKNOWLEDGEMENT

This research paper is made possible with the help and support of my parents, teachers, family, friends, and all the people who guided me throughout my work. Especially, we. Would like to thank all the other professors of my department who have suggested me and helped me in writing this paper. Finally, we sincerely thank to our parents, family, and friends, who gave us emotional and financial support. Without the support of these kind people the product of this research paper would not be possible.

REFERENCES

[1] Divya shrungar et al.”Fog computing: Security in cloud envornment”Voloume- 5,Issue 8,Aug 2015

[2] Sayali Raje et al“cloud security using fog computing, ,2014,IRF International Conference

[3] 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.

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

[5] Iglesias J. A., Angelov P., Ledezma A., and Sanchis A., “Creating evolving user behavior profiles automatically” ,IEEE Trans. on Knowl. and Data Eng., May 2012, vol. 24, no. 5, pp. 854–867

[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] Park, Y., & Stolfo, S. J. “Software decoys for insider threat”, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, pp. 93-94.

[8] Montelibano, Joji, and Moore A. ,"Insider threat security reference architecture", In System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE, pp. 2412-2421.

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

[10] Grobauer, B., Walloschek, T., & Stocker, E. ,“Understanding cloud computing vulnerabilities”. Security & Privacy, IEEE, 2011, pp. 50-57

[11] Salem M. B. and Stolfo S. J. , “Decoy document deployment for effective masquerade attack detection”, in Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment, ser. DIMVA’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 35–54

[12] Rocha F. and Correia M., “Lucy in the sky without diamonds: Stealing confidential data in the cloud,” in Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops, ser. DSNW ’11. Washington, DC, USA: IEEE Computer Society, pp. 129– 134.

[13] Archer, Jerry,l. "Top threats to cloud computing v1. 0." Cloud Security Alliance ,2010.

[14] Marinos A. & Briscoe G., “Community Cloud Computing”, Heidelberg: Springer, 2009,pp. 472-484.

[15] Godoy D., “User profiling for web page filtering”, IEEE Internet Computing, Jul. 2005, vol. 9, no. 4, pp. 56–64.