International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
595 – 597

Different Approach to Secure Data with Fog Computing

Dr. Vishal Kumar Goar
Assistant Professor
Govt. Engineering College Bikaner (India)

Abstract **-**Fog computing could be a paradigm that extends cloud computing that has become a reality that made-up the method for brand new model of computing. additionally, fog provides application services to finish terminal within the age of network. The inner information stealing attacks in that a user of a system illegitimately poses because the identity of associate other legitimate user which is an arising new challenge to the service supplier wherever cloud service supplier might not be able to defend the information. therefore, to secure the important user's sensitive data type the offender within the cloud. In this research paper I am proposing a very distinct approach with the assistance of offensive decoy data technology, that is employed for confirming whether or not the data access is permitted wherever abnormal information is detected andthereby confusing the offender with the fake data.

Keywords-*Fog Computing; Decoy Technology; Cloud Computing; Security;*

*****

I. INTRODUCTION

Cloud computing is nothing however computing power that is virtualized and thru platform-agnostics delivery of storage infrastructures of abstracted hardware and web package. The shared, on-demand IT resources, square measure created and disposed of effectively, square measure dynamically ascendible through a range of programmatic interfaces and cloud computing could be a general term for all the world that involves delivery hosted services over `the web. Cloud is being employed in varied preparation models and repair models. Out of these three service models, rock bottom layer is infrastructure as a service (IaaS) provides virtual machines and alternative resources like block and file storage, network security, load leveling, virtual local area networks (VLANs) etc. The second layer type rock bottom is Platform as a service here, cloud service supplier delivers a computing platform like software system, execution setting (programming language), information and net servers. Some PaaS service suppliers like Windows Azure, Google AppEngine alter the computers and storage resources vary mechanically to match application demand in order that the cloud user dos not need to allot resources manually. The last service model could be a software as a Service (SaaS), user square measure provided access to application package and databases. SaaS are some things additionally known as on demand service of package and is typically obtainable on a pay-per-use basis.

With this new computing and communication paradigms arise a brand-new information security challenges. Existing information protection mechanisms like cryptography have failing in preventing the information thievery attack, particularly those perpetrated by AN business executive to cloud supplier.

In this research paper, proposed a very completely different approach to securing the cloud mistreatment the decoy info technology that we've got return to decision Fog computing. like Twitter attack, by deploying decoy info inside a Cloud by the Cloud service client and inside personal on-line social networking profiles by individual users. we tend to use this technology to launch misinformation attacks against malicious Associates, preventing them from characteristic the important sensitive client information from faux trashy information.

II. INFORMATIONROBBERY

A very high and executable service is given to the business organizations, that for his or her secured information trust the suppliers of the cloud services. however, this work isn't as less complicated to try and do just in case of personal services of cloud, as less complicated it sounds. one amongst the key attacks in cloud is information felony. as an example, a series of cyber-attacks hanging major banks as believed by U.S. officials, were the work of Iranian government to increase cyber security standoff between the 2 nations. By infecting information centers at clouds rather than computers, the hackers obtained the computing power to mount huge denial of service attacks. Thus, to limit the attacks of this sort we will cut back the worth of the info that is being hold on the cloud.

III. SAFEGUARDING CLOUD THROUGH FOG

For securing information of cloud, none out of all the projected strategies is full proof because of numerous reasons. Let or not it's customary access or the coding mechanism being employed for securing cloud, they need failing as a result of a cloud's reliable atmosphere solely, isn't enough for the client. Nowadays, the client needs security that is healthy for its applications and information. therefore, such incidences should even be controlled. If we tend to decrease the worth of taken information by providing decoy documents then we will limit the hurt of the system. Following options of additional security are proposed:

 ISSN: 2454-4248
595 – 597

A. Profiled Behavior of User

its bobbing up very laborious to outline the behavior of a user. it's completely necessary that there ought to be how so we will mechanically method the behavior of the user to avoid the business executive Misuse drawback. presently even just in case of malicious business executive the information is accessed usually from the cloud because the business executive has the identity of the victim. User identification (the well-known technique) ought to be used for detection the illegitimate access. Here for legitimate users the admin about to beware} simply able to set operating baseline going to record log record of all users. To discover regarding user behavior's abnormal access the admin will keep a continuing eye on „Normal user' behavior. primarily for applications of fraud detection this security technique supported behavior will be normally used. volumetrically info like the quantity of documents, their frequency of being scan would naturally be used. we have a tendency to analyze for such kind search behavior that is dissimilar thereupon of actual user that exhibits deviation from the user's threshold limit that has standby anomaly discover. It's coming up extremely arduous to outline the behavior of a user. It is fully necessary that there ought to be how in order that we will mechanically method the behavior of the user to avoid the corporate executive Misuse drawback. presently even just in case of malicious corporate executive the info is accessed usually from the cloud because the corporate executive has the identity of the victim. User identification (the well-known technique) ought to be used for sleuthing the illegitimate access. Here for legitimate users the admin planning to beware} simply ready to set operating baseline going to record log record of all users. To discover concerning user behavior's abnormal access the admin will keep a continuing eye on „Normal user' behavior. primarily for applications of fraud detection this security technique supported behavior will be ordinarily used. meter data like the quantity of documents, their frequency of being browse would naturally be used. we tend to analyze for such kind search behavior that is dissimilar therewith of actual user that exhibits deviation from the user's threshold limit that hasstandby anomaly discover.

B. Decoy data technology

Decoy files or documents are entice files that not helpful for the legitimate users however act as entice for illegitimate user that's once an assaulter can enter into the system the search behavior are random and if any entice is hit by that user then the pattern can amendment so any amendment in usual behavior of the user are detected and however if the entice is hit by legitimate user by mistake then by responsive some secret challenge queries the legitimacy are often checked. Further, the diagram of high level security design makes the procedure additional clear Decoy means that the relative misinformation, phony info regarding the connected knowledge documents. If it gets suspicious then to mislead the assaulter false info is being free when the user search modelling. for creating certain that the assaulter fails to differentiate between the decoy files and also the actual files an equivalent information is employed for each decoy also as original file. there's direct linking to fog computing sites just in case the attack on user's knowledge is sustained by the assaulter. Through this the security of the vital knowledge is inflated. the particular user can currently determine if the phony knowledge is being sent by the cloud as he's the owner of the info. so, through an oversized range of means that the response by the cloud are often altered, like challenge inquiries to inform the cloud security system regarding its unauthorized and incorrect access.

IV. MERGING USER BEHAVIOUR AND DECOY

The current logged in user access behavior is compared with the past behavior of the user. If it's surpassing the brink price or a limit, then the remote user is suspected to be anomaly. If the present user behavior is because the past behavior, the user is allowed to work on the initial knowledge. The correlation of search behavior anomaly detection with entice primarily based decoy files ought to offer stronger proof of misconduct, and so improve a detector'saccuracy. This situation covers the threat model of illegitimate access to Cloud knowledge. moreover, AN accidental gap of a decoy file by a legitimate user could be recognized as AN accident if the search behavior isn't deemed abnormal. Combining the 2 techniques improves detection accuracy. Instead, we tend to created certain that the decoys were conspicuous enough for the assaulter to access them if they were so making an attempt to steal info by putting them in extremely conspicuous directories and by giving them engaging names.

V. CONCLUSION

In this paper, by combining user search behaviorand decoy info we tend to conferred an integrated detection approach through anomaly detection with a molestation approach supported the readying of decoy documents to secure personal and business knowledge within the cloud. In our future work, this security system as we've got explained is applicable just for single cloud possession system. If the cloud owner contains a quite one clouds to work then our security system won't be applicable for providing security, so within the future improvement we are able to enhance our existing application to manage a cloud atmosphere that has quite one cloud design. Cloud computing is that the future for organizations.

REFERENCES

[1] M. Bowen, S. Hershkop, A. D. Keromytis, and S. J.Stolfo, "Baiting inside attackers using decoy documents," inSecureComm'09: Proceedings of the 5th International ICST Conference on Security and Privacy in Communication Networks, 2009.

 ISSN: 2454-4248
595 – 597

[2] Lucky Nkosi, Paul Tarwireyi and Matthew O Adigun "Insider Threat Detection Model for the Cloud", 978-1-4799-0808-0/13/$31.00 ©2013 IEEE.

[3] M. A. Maloof and G. D. Stephens, "elicit: A system for detecting insiders who violate need-to-know," in RAID,2007, pp. 146–166.

[4] R. Baeza-Yates, C. Hurtado, M.Mendoza, and G. Dupret, "Modeling user search behavior,"in LA-WEB ˝05: Proceedings of the Third Latin American Web Congress. IEEE Computer Society, 2005, pp. 242–251.

[5] Fog Computing: Mitigating Insider Data Theft Attacks in the / Cloud. [Online].Available:http://ids.cs.columbia.edu/sites/default/files/Fog_Computing_Position_Paper_WRIT_2012.pdf

[6] M. Ben-Salem and S. J. Stolfo, "Modeling user searchbehavior for masquerade detection," in Proceedings of the14th International Sympo- sium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

[7] J. Attenberg, S. Pandey, and T. Suel, "Modeling and predicting user behavior in sponsored search," in KDD ˝09:Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. New York, NY, USA: ACM, 2009, pp. 1067–1076.

[8] B. M. Bowen and S. Hershkop, "Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/,"2009. [Online]. Ava ilable: http : //sneakers.cs.columbia.ed u /ids/FOG

[9] Kaufman, L. M., "Data security in the world of cloud computing". Security & Privacy, IEEE,2009,pp. 61-64.

[10] Claycomb, W. R., & Nicoll, A. ,"Insider Threats to Cloud Computing: Directions for New Research Challenges", In Computer Software and ApplicationsConference (COMPSAC), IEEE 36th Annual , July,2012,pp. 387-394.

[11] Buyya, Rajkumar, "Introduction to the IEEE Transactions on Cloud Computing.", Cloud Computing, IEEE, 2013, pp 3-21.

[12] Pearson, Siani, Shen Y. and Mowbray M. ,"A privacy manager for cloud computing" , Springer Berlin Heidelberg , 2009, pp. 90-106.

[13] Garfinkel S., "The Cloud Imperative", Technology Review (MIT) (3 October 2011),Retrieved 31 May 2013

[14] "Launch of IBM Smarter Computing", Retrieved 1 March 2011.

[15] "Launch of Oracle Cloud", Retrieved 28 February 2014.