ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Securing user data on cloud using Fog computing and Decoy technique

Manreet Kaur[1]
Information technology
Chandigarh University
India

Monika Bharti[2]
Computer Science Engineering
Chandigarh University
India

Abstract: ***Cloud computing is used as a delivery platform which is a promising way for storing user data and provides a secure access to personal and business information. The users are provided with on-demand services through the Internet. But it also involves risks like data theft and various other attacks. By performing such attacks, the intruders can peep into documents which can results in misuse of data and also interpretation of highly confidential data for illegal purposes. For securing user data from such 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. In this paper we have discussed this paradigm for preventing misuse of user data and securing information.***

Keywords: Cloud computing; Fog computing; Decoy technology; Data security and Insider theft attacks.

I. INTRODUCTION

In this era, Cloud computing is achieving popularity every day. The ease of use and storage which is provided to users for personal and business purposes is increasing its demand. . It is a ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [1]. Business agencies and software companies are admiring cloud computing for its flexible architecture and ease of access. For attaining more and more operational efficiency and managing data organization with small or large businesses are using cloud environments. Cloud Computing is a combination of service oriented architecture and many computing strategies such as virtualization and networking.

Although, cloud computing provides an environment through which managing and accessing of data becomes easier but it have consequences such as data leakage, data theft, insider attacks etc. Very common risks now days are data theft attacks. Data theft is considered one of the top threats to cloud computing by the Cloud Security Alliance [2]. To resolve these issues a mechanism which can detect such malicious activities is required. For this, Fog computing is paradigm which monitors the data and helps in detecting an unauthorized access. According to Cisco, due to its wide geographical distribution the Fog computing is well suited for real time analytics and big data. While Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization [3]. Fog computing involves a dense geographical distribution of network and provides a feature of location access. With this any unauthorized activity in the cloud network can be detected. The application built for solving the problem of data security includes a mechanism which user behavior profiling is done. The common notion of a cloud insider as a rogue administrator of a service provider is discussed, but we also present two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource [7].

In this paper, section II explains the concept of Fog computing and procedure used to access user's location in case of any abnormality detected, in section III the methodology of the prototype is discussed, further in section IV describes the accuracy results of the prototype using cusum algorithm and the last section gives conclusion to the paper.

II. CONCEPT OF FOG COMPUTER

Fog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, compute, storage, and application services to end-users. The difference is Fog provides proximity to its end users through dense geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network. Fog computing improves the Quality of service and also reduces latency. According to Cisco, due to its wide geographical distribution the Fog computing is well suited for real time analytics and big data. While Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization [3]. Madsen.H and Albeanu. G presented the challenges faced by current computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is mainly done for the need of the geographical distribution of resources instead of having a centralized one. A multi-tier architecture is followed in Fog computing platforms. In first tire there is machine to machine communication and the higher tiers deal with visualization and reporting. The higher tier is represented by the Cloud. They said that building Fog computing projects are challenging [4].But there are algorithms and methodologies available that deal with reliability and ensure fault tolerance. With their help such real life projects are possible. Z. Jiang et al. [5] Discussed Fog computing architecture and further used it for improving Web site's performance with the help of edge servers. They said that the emerging architecture of Fog Computing is highly virtualized. They presented that their idea that the Fog servers monitor the requests made by the users and keep a record of each request by using the user's IP address or MAC address. Godoy et al. [6] explained that there is a need of such profiling strategies or methods through which user profiling can be done. As there is a huge amount of information available on the web or Internet therefore from last few years personal information agents are helping the users to manage their information. In this paper the authors have discussed a learning technique for data acquisition for user profiling and so they mentioned some methods for adaption with the changes which happen time to time with the change in user's interest. They said earlier only supervised learning technique was used in general. But for moving the information agents to the next level authors are focusing on assessment of semantically useful user profiles. They said that account hijacking is a disadvantage for such user profiling. Sabahi, F. mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. In this paper he has summarized reliability and availability related issues of cloud resources provided by the trusted third party. He discussed about the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology offering the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown [8]. Considering all these requirements, this prototype is created which includes two main steps: first is to create users and generate patterns of their different access behaviors, next step is monitoring the user access patterns which is done using CUSUM that is cumulative summation algorithm to find the accuracy of the procedure.

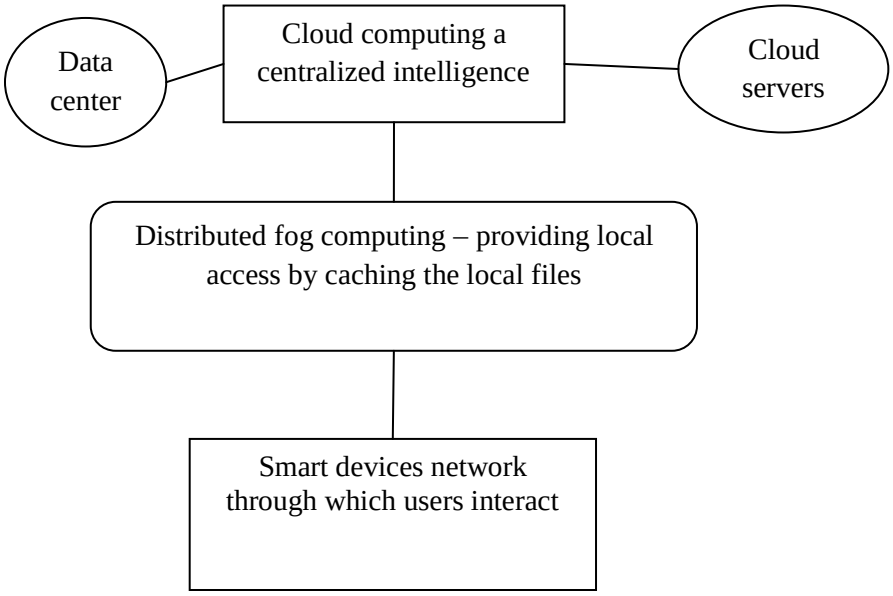


Figure 2.1: Architecture of Fog computing

III. DECOY INFORMATION

Decoy files or documents are trap files which not useful for the legitimate users but act as trap for illegitimate user that is when an attacker will enter into the system the search behavior will be random and if any trap is hit by that user then the pattern will change thus any change in usual behavior of the user will be detected and but if the trap is hit by legitimate user by mistake then by answering some secret challenge questions the legitimacy can be checked. Further, the diagram of high level security architecture makes the procedure more clear.

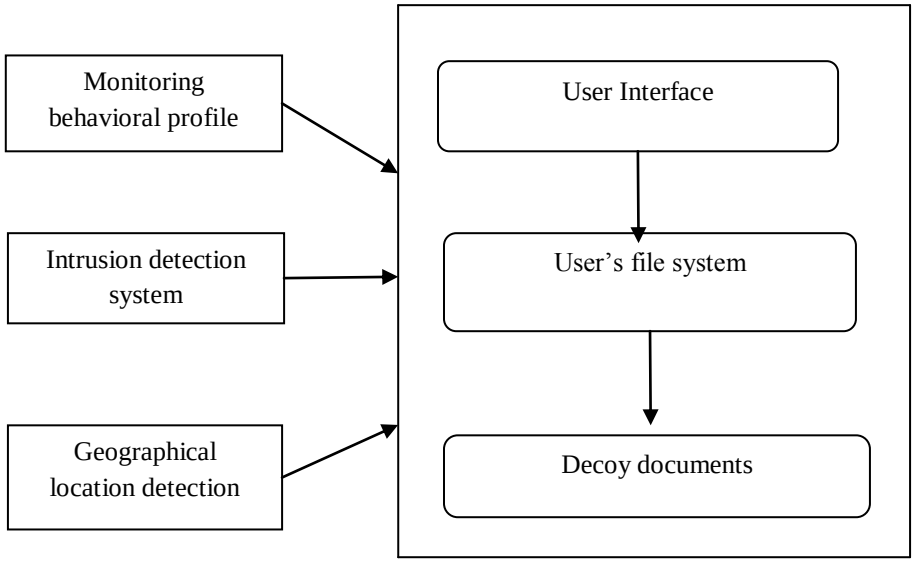


Fig. 3.1: Component architecture of high level security

The figure above illustrates the different steps which can be performed to make user's file system secure and regular monitoring of the system can help in identifying any abnormality if observed.

3.1 Injecting traps (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.

IV. RESULTS AND DISCUSSIONS

An interface is created in which user can login and access the user's file system after entering the valid information. The file system has files and folders in which trap files are also placed to detect that the user is legitimate or an attacker. On the basis of earlier profile of the user monitoring process is carried out at the back end if there is a mismatch or any abnormality the pattern starts fluctuating abruptly signifying that there is trap hit or mismatch. Cumulative sum algorithm is used which is detect abrupt changes in the pattern analysis of the user system is done.

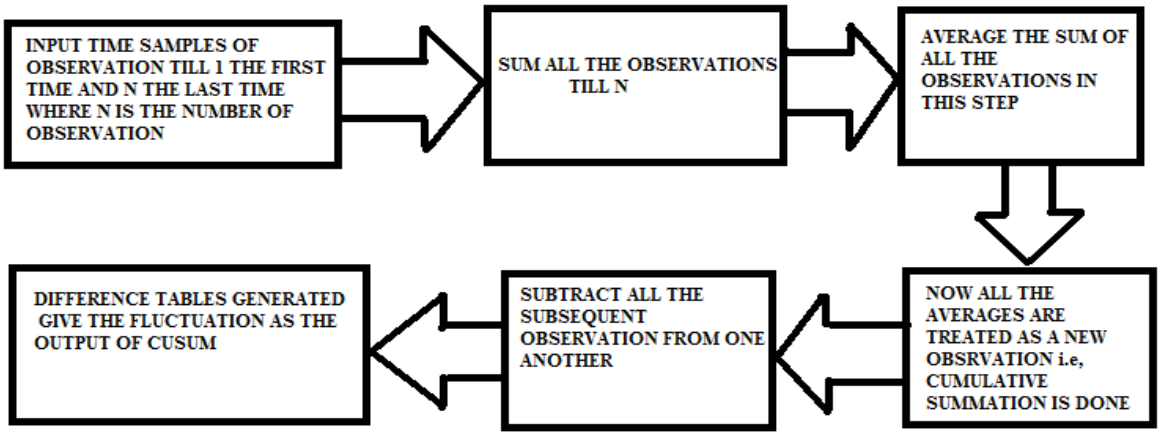


Fig. 4.1: Block diagram of cusum algorithm

The figure below shows the interface which contains the user files or documents and all the files are placed in such a way that to an attacker all files will appear as useful but some of these contain traps which are known to the legitimate user only. Whenever the attacker hits a trap the profile pattern changes and signifies that there is some abnormality in user's behaviour.

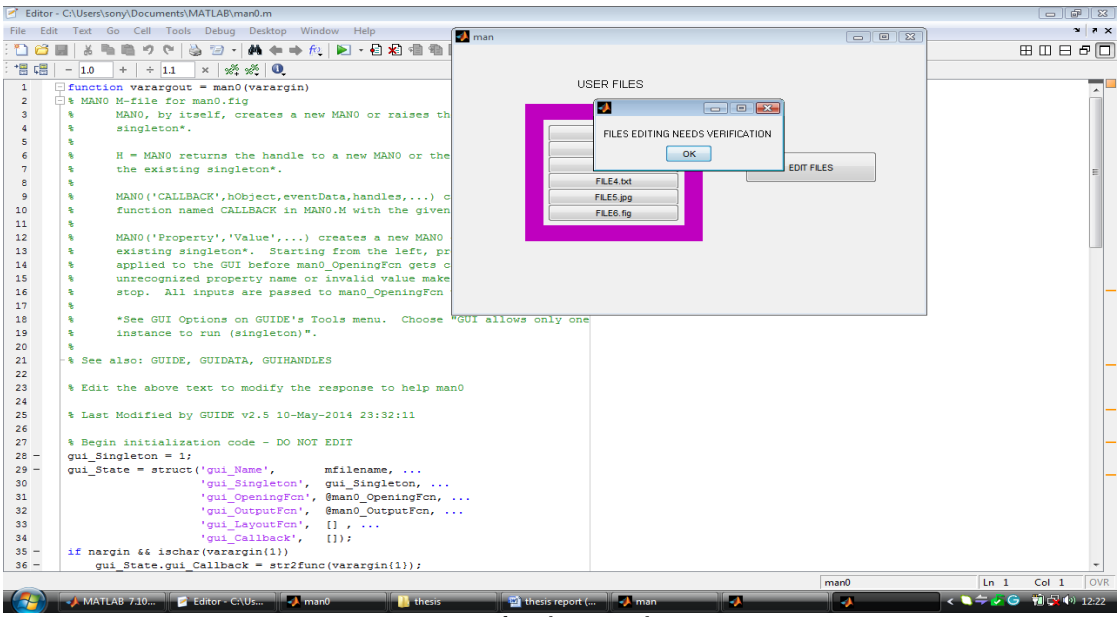


Fig. 4.2: Interface shows user documents

The system also calculates the load, average fluctuation; time based on these parameters accuracy of the built system is calculated for various users. Using MATLAB graphs of average fluctuation versus time is plotted.

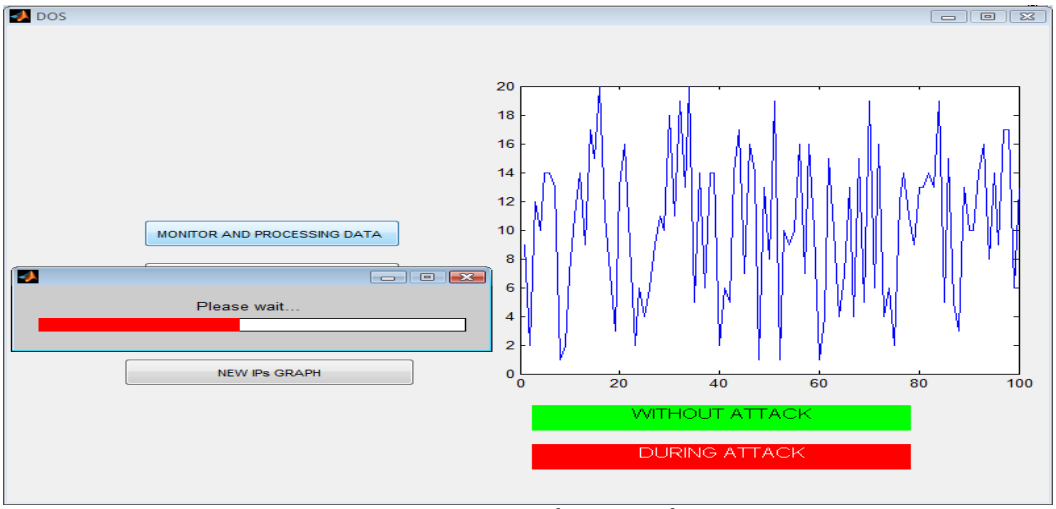


Fig. 4.2: Monitoring and Processing data

Figure shows the graphical user interface for analyzing user profile, this process goes at backend or we can say a server side so as to identify any abnormality or identify any malicious activity. If there is no frequent fluctuation in the graph that means the system is protected.

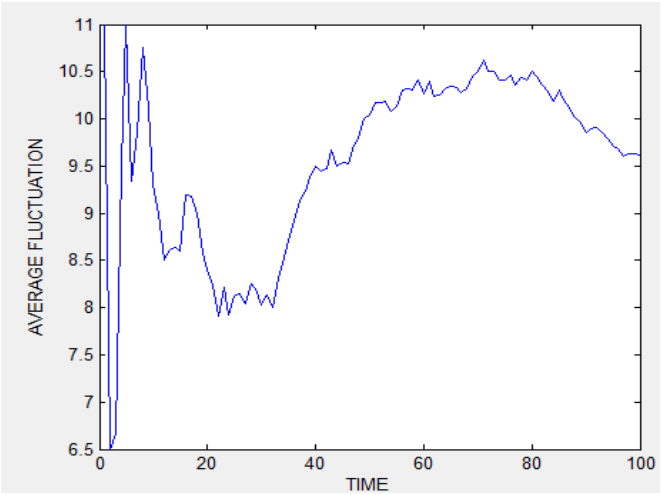


Fig. 4.3: Depicting average fluctuation over time

The system also calculates the load, average fluctuation; time based on these parameters accuracy of the built system is calculated for various users. Using MATLAB graphs of average fluctuation versus time is plotted.

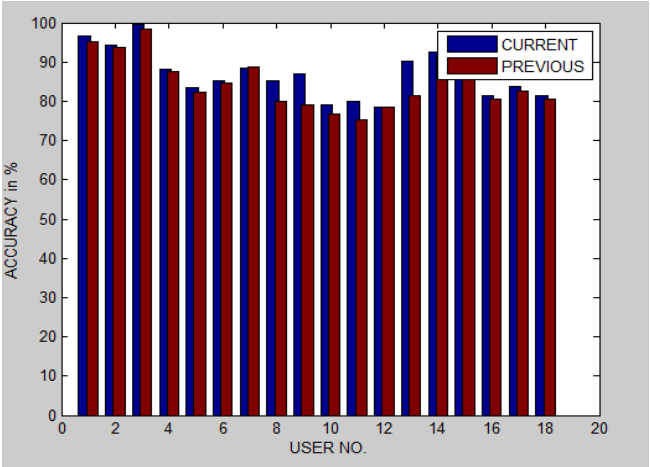


Figure 4.3: Graphical comparison of the previous results and current results

The application successfully detects the abnormality in the user system. Also accuracy comparison is made with previous results which depict an average of approximately 10% inclination in the results drawn using CUSUM algorithm.

V. CONCLUSION

A model is created using fog computing and decoy technology which detects the insider theft attacks. Previous method used to secure data was encryption techniques but in this research work the technique used is CUSUM change point detection algorithm for detecting the abnormalities in user behavior profile. Different scenarios are considered by varying the number of users and their corresponding patterns were analyzed. Using CUSUM, time, load and average fluctuation in user profile or access behavior is evaluated. On the basis of these parameters the accuracy of the system using CUSUM monitoring technique showed an inclination upto 10% in the results. This also depicts that fog computing and decoy technology together are able to detect abnormalities and give more accurate results as compared to previous techniques. Later on this work can be extended by working on algorithm for the prevention from the insider data theft attacks. Also, the performance evaluation of the technique can be calculated by considering other attributes. The concept of fog computing is very vast other than security of data we can extend this research for network security through fog computing and also localising the user data a secure geographical locations.

ACKNOWLEDGEMENT

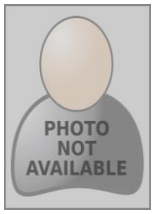
This research paper is made possible with the help and support of my parents, teachers, family, friends, and all the people who guided me throughout my work. Especially, I am thankful and I express my gratitude to the following people who contributed and helped to make this work possible. First and foremost, I would like to thank Ms. Monika Bharti for her support and encouragement with which I was motivated and was able to write this paper. She kindly read my paper and suggested me advices on grammar, matter, and the title of the paper. Second, I would like to thank all the other professors of my department who have suggested me and helped me in writing this paper. Finally, I sincerely thank to my parents, family, and friends, who gave me emotional and financial support. Without the support of these kind people the product of this research paper would not be possible.

References

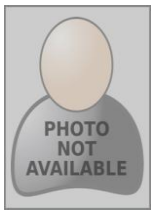
1. Hashizume K., Rosado D. G.,Fernandez- Medina E. and Fernandez E. B. “An analysis of security issues for cloud computing”. Journal of Internet Services and Applications, 2013, 4(1), pp. 1-13.
2. Archer, Jerry,l. "Top threats to cloud computing v1. 0." Cloud Security Alliance ,2010.
3. Bonomi, Flavio, 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.
4. 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.
5. Zhu, Jiang,“Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture”, Service Oriented System Engineering (SOSE), IEEE. 2013.
6. Godoy D., “User profiling for web page filtering”, IEEE Internet Computing, Jul. 2005, vol. 9, no. 4, pp. 56–64.
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. Sabahi, F. “Cloud computing security threats and responses”, In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on 2011,pp. 245-249.
9. Marinos A. & Briscoe G., “Community Cloud Computing”, Heidelberg: Springer, 2009,pp. 472-484.
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. 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.
13. 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.
14. Montelibano, Joji, and Moore A. ,"Insider threat security reference architecture", In System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE, pp. 2412-2421.

15. Mathew S., Petropoulos M., Ngo, H. Q. and Upadhyaya S. ,"A data-centric approach to insider attack detection in database systems", In Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2010, January, pp. 382-401.
16. Kaufman, L. M., "Data security in the world of cloud computing". Security & Privacy, IEEE,2009,pp. 61-64.
17. Claycomb, W. R., & Nicoll, A. ,"Insider Threats to Cloud Computing: Directions for New Research Challenges", In Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual , July,2012,pp. 387-394.
18. Buyya, Rajkumar, "Introduction to the IEEE Transactions on Cloud Computing.", Cloud Computing, IEEE, 2013, pp 3-21.
19. Pearson, Siani, Shen Y. and Mowbray M. ,"A privacy manager for cloud computing" , Springer Berlin Heidelberg , 2009, pp. 90-106.
20. Garfinkel S., "The Cloud Imperative", Technology Review (MIT) (3 October 2011),Retrieved 31 May 2013
21. "Launch of IBM Smarter Computing", Retrieved 1 March 2011.
22. "Launch of Oracle Cloud", Retrieved 28 February 2014.
23. COMPUTING, CLOUD. "Cloud computing privacy concerns on our doorstep." Communications of the ACM, 54.1,2011.
24. Brodkin J. ,"Gartner: Seven cloud-computing security risks" ,Infoworld (2008), pp. 1-3.
25. Roberts II J. C. and Al-Hamdani W., "Who Can You Trust in the Cloud? A Review of Security Issues Within Cloud Computing," Proc. Information Security Curriculum Development Conference,Kennesaw, 2011 ,pp. 15-19.
26. Shatnawi, Nahla, Althebyan Q. and Mardini W. ,"Detection of insider misuse in database systems", Proceedings of the International MultiConference of Engineers and Computer Scientists,Vol. 1,2011.
27. Van Dijk M. and Juels A., "On the impossibility of cryptography alone for privacy-preserving cloud computing",in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. "Berkeley, CA, USA": "USENIX Association", 2010, pp. 1–8.
28. Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. ,"Common sense guide to prevention and detection of insider threats" 3rd edition – version 3.1, CMU SEI, 2009.

AUTHOR(S) PROFILE



Manreet Kaur, M.E. degree in Information Technology from Chandigarh University, Gharuan and B.tech in Computer Science from Lovely Professional University, Phagwara, India



Monika Bharti Assistant professor at Chandigarh University, Gharuan.

