SECURING USER DATA ON CLOUD USING CLOUD DATA CENTRE COMPUTING AND DECOY TECHNIQUE

V.N.Baskar
Francis Xavier Engineering College
Computer Science & Engineering
rakshabmaclextron@gmail.com
9489305360

J.Emmanuel John
Francis Xavier Engineering College
Computer Science & Engineering
justmailjohn3@gmail.com
8072817853

Mrs. B.Benita M.E, Ass Prof
Francis Xavier Engineering College
Computer Science & Engineering
benitabilly@gmail.com

Abstract: Cloud computing act 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, security risks at the vendor and various other attacks. By performing such attacks, the intruders can peep into documents which 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 Cloud Data Centre computing can be used. This technique will monitor the user activity to identify the legitimacy and prevent from any unauthorized user access. The technique we have discussed this paradigm for preventing the misuse of user data and securing information.

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

I. INTRODUCTION

In this era, Cloud computing is achieving popularity day-to-day. The ease of use and storage which is provided to users for personal and business purposes is increasing its urge. It is a ubiquitous, expedient, on-demand network access to a shared pool of configurable computing resources [1]. Business agencies and software companies are admiring cloud computing for its adaptable and flexible architecture and ease of access. For promoting and 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 promoting interoperability, application portability, 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, downtime, technical outages, etc. Very common risks now days are data theft attacks. Data theft is considered as one of the top threats to cloud computing by the Cloud Security Alliance [2]. To resolve these issues a mechanism used which can detect such malicious activities is required. For this, Cloud Data Centre computing is paradigm which monitors the data and helps in detecting an unauthorized access. According to Cisco, due to its wide geographical distribution the Cloud Data Centre computing is well suited for real time analytics and big data. While Cloud Data Centre nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization [3]. Cloud Data Centre

computing involves a dense geographical distribution of network and provides a feature of location access. With this any unauthorized activity in the cloud network or environment can be detected. The application built for solving the problem of data security includes a mechanism in which user behavior profiling is done. The common notion of a cloud insider who act as a rogue and unethical administrator of a service provider is discussed, but we also present two additional cloud related insider risks: the insider who exploits a cloud-related susceptibility or 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 section II explains the concept of Cloud Data Centre 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 accurate results of the prototype using CUSUM algorithm and the last section gives conclusion to the paper.

II.EXISTING WORK

Cloud Data Centre Computing is an extension of Cloud Computing. As in a Cloud, Cloud Data Centre computing also provides data, compute, storage, and application services to end-users. The difference is Cloud Data Centre provides proximity to its end users through dense geographical distribution and it also supports mobility. Access points or set-up boxes are used as the end devices to host services at the network. These end devices are also known as edge network. Cloud Data Centre computing improves the Quality of service and also reduces latency. Madsen.H and Albeanu. G presented the challenges faced by current computing paradigms and discussed how Cloud Data Centre computing platforms are feasible with cloud and are reliable for real life projects. Cloud Data Centre 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 Cloud Data Centre computing platforms. In first time 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 Cloud Data Centre computing projects are challenging [1]. But there are algorithms and methodologies exists that deal with reliability and ensure fault tolerance. With their help such real life projects make it possible. Z. Jiang et al. [2] Discussed Cloud Data Centre 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 Cloud Data Centre Computing is highly virtualized. They presented that their idea that the Cloud Data Centre 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 addressed. As there is a huge amount of information exists 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 in which the data acquisition for user profiling and so they mentioned some methods for adaption with the changes which happen from time to time with the change in user's interest. They said earlier only the supervised learning technique was used in general. But for moving the information from agents to the next level

authors are focusing on assessment of semantically useful user profiles. They said that user 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. The technology he has summarized that reliability and availability related issues of cloud resources provided by the trusted third party. He discussed about the common attacks nowadays occur which would be Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology offering the benefit of flexibility and adaptability, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown [8].

III.PROPOSED WORK

Considering all these requirements, this prototype is created in which it includes two main steps: first is to create users and generate patterns of their different access behaviors, next step is monitoring the user activity patterns which is done using CUSUM that is cumulative summation algorithm to find the accuracy of the procedure.

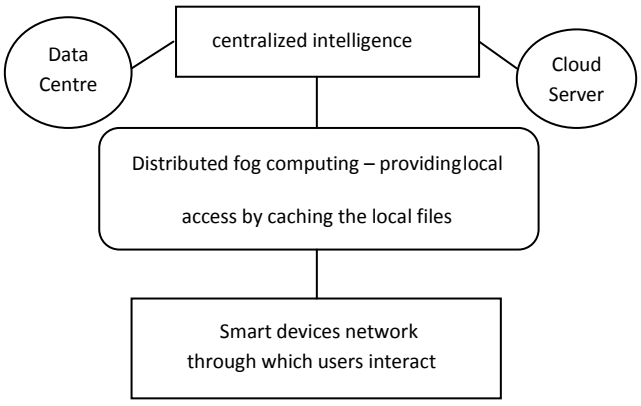

Fig. 3.1: Architecture of Cloud Data Centre computing

Decoy files or documents are trap files which will be not useful for the legitimate users but act as trap for illegal 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, but if the trap is hit by legitimate user by mistake then by answering some secret challenge questions then only legitimacy can be checked. Further, the diagram of high level security architecture which makes the procedure more clear.

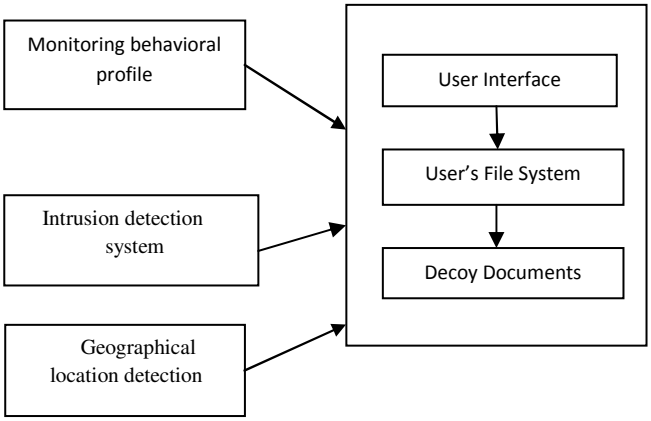

Fig. 3.2: Component architecture of high level security

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

Injecting traps (decoy technology): This is where the 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/she will open the files to

which the access is open and will search in a random manner, but here in the system only the files which are left open to the users that are trap files. So when the attacker will open those trap file the abnormality in user behavior will be detected. With CUSUM change point will be detected.

IV.ALGORITHM

The FEBR (Flow lEvel Bandwidth pRovisioning) algorithm, which reduces the switch scheduling problem to multiple instances of fair queuing problems, each employing a well studied fair queuing algorithm. The FEBR offers fine granularity bandwidth assurance for individual flows. a task scheduling algorithm IBPS based on static priority in different subintervals. IBPS possesses a priority traceability property which facilitates the system designers to debug a system during development and maintenance. a Hybrid Method based Reliability Evaluation (HMRE) model, which combines Continuous-Time Markov Chain (CTMC) and Mean Time To Failure (MTTF) metrics to measure the effect of physical-resource breakdowns on system reliability. HMRE model can be used to design a reliable system for cloud computing.

V.ADVANTAGES

A Multi Objective Resource Scheduling (MORS) mechanism to reduce execution time and improve reliability of cloud service

VI.RESULTS & DISCUSSIONS

An interface is created in which the 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 in order to detect that the user is legitimate or an attacker. On the basis of earlier profile of the user monitoring process which 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 occurrence. Cumulative sum algorithm is used which detect abrupt the changes in the pattern analysis of the user system is done.

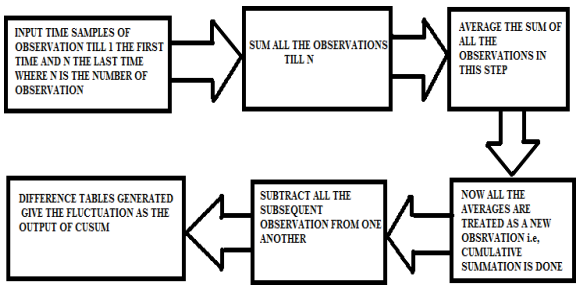

Fig. 6.1: Block diagram of CUSUM algorithm

The figure above 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 to be useful but some of these contain traps which are known to the legitimate user only. Whenever the attacker hits a trap the profile pattern gets change and signifies that there is some abnormality in user's behavior.

VII.CONCLUSION

A model is created using Cloud Data Centre 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 which 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 accurate result of the system using CUSUM monitoring technique showed an inclination up to 10% in the results. This also depicts that Cloud Data Centre computing and decoy technology together are able to meet the abnormalities and give more accurate results as compared to previous techniques. Later on this work can be extended by working on algorithm that prevents from the insider data theft attacks. Also, the performance evaluation of the technique can be measured by considering other attributes. The concept of Cloud Data Centre computing is very vast other than security of data we can extend this research for network security through Cloud Data Centre computing and also localizing the user data in a secure geographical locations.

VIII.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. "Cloud Data Centre 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 Cloud Data Centre 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 Cloud Data Centre 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.