Enhanced Secure User Data on Cloud using Cloud Data Centre Computing and Decoy Technique

P.S.Apirajitha, C.Gopala Krishnan, G.Aravind Swaminathan, E.Manohar

Abstract: ***In recent years the storage of cloud platform was increased a lot. Large set of personal and business data can be stored and accessed at anywhere at any time. Data's are stored in a secured manner using various secured and optimized algorithms. Over this data theft and modifications are done in a highly manner. Therefore this creates a various security risks and data theft problems in cloud. There is need of security technique to overcome this problem. A proposed technique called cloud data centre technique is a new model for securing data from different attacks and security risks. This technique incorporate the FEBER and CUSCUM algorithms, which will monitor the user activity and then identify the legitimacy and prevent from any unauthorized user access. This data center technique can be used to detect and avoid data theft attacks by malicious insiders. The anonymous and miss use of data also prevented in a very good manner while compared to other techniques.***

Keywords: Cloud data centre computing; Decoy technology; Data security, Insider theft attacks, CUSCUM technique, FEBER algorithm.

I. INTRODUCTION

In day-to-day Cloud computing is accomplishing attractiveness in all fields. Cloud computing was organized by number of older technologies like grid computing, utility computing, green computing, internet of things, etc.

From the existing technologies, cloud computing provides better solution for on demand access to resources virtually. The customers under cloud environment can only pay for the amount of resources they accessed. As a result, the usage of cloud services by IT companies has risen. In today's world, all things are moving towards digitization. All the popular social networking sites, mails, chats, data sharing, etc are hosted on the cloud. Maximum software developers are working under cloud platform. Cloud computing makes the internet world appealing as it reduces the process and cost of buying hardware. The resource allocation is one of the main issues of distributed computing [1]. It is the process of distributing resources among cloud environment to meet a specified goal. The limited available resources must be allocated efficiently to maximize the overall profit and utility.

Cloud services are packed up with large data centers. These data centers capsule with lacks of computers. Datacenters are used to provide service to many users and it is hosted with lot of applications. To create this service, hardware virtualization in Uhlig *et al.* is considered as a best fit. Hardware virtualization is the concept of virtualizing computer memory, processor and I/O devices. Hardware virtualization allows the running of multiple operating systems and software's on a physical platform. The intermediate layer of software is called Virtual Machine Monitor (VMM), also called as hypervisor.

Managing and storage of data is easier in cloud computing, but it has some disadvantages like leakage of data, attacks, downtime and possibility of data theft. Among that data theft attack plays a vital issue in cloud environment [2]. It is necessary to identify the malicious attacks to solve this issue. Cloud Data Centre(CDC) computing is a technique to monitor and identify the malicious data. Real time and big data analytical is well studied in Cloud Data Centre computing according to Cisco. In this approach Cloud Data Centre nodes offer localization whereas the Cloud delivers global centralization [3]. It also provides a location access features by incorporating geographical distribution using Cloud Data Centre computing.

User behavior profiling is another technique used to maintain data security in cloud environment. But here it is difficult the insider can be create vulnerability attacks. There is a possibility to steal information from cloud systems by the local employers [7].

DDOS stands for Distributed Denial of Service. It is a type of attack which aims to make resources or services unavailable by flooding a victim with useless traffic. It outcomes in provisionally or indefinite interruption of services on the host system. Attacker hides its uniqueness from victim by spoofing its IP address [11].

The concept of CDC computing and abnormality detection procedure is explained in section IV. The implementation of prototype for abnormality identification is discussed in section III, the results obtained by the proposed methodology is presented in section IV. The concluded remarks are given in the last section.

In section II refers the existing methods explains the concept of Cloud Data Centre computing and procedure used to access user's location. Section III explains the problem statement. Section IV represents the proposed methodology used. Section V shows the algorithm and steps of FEBER algorithm. Further in section VI describes the accurate results of the prototype using CUSUM algorithm and the last section gives conclusion and future enhancement.

Revised Manuscript Received on July 05, 2019.

Ms.P.S.Apirajitha, Assistant Professor, Department of CSE, VEL TECH UNIVERSITY

Dr C.Gopala Krishnan, Professor, Department of CSE, Francis Xavier Engineering College

Dr G.Aravind Swaminathan, Professor, Department of CSE, Francis Xavier Engineering College

Dr E.Manohar, Assistant Professor, Department of CSE, Francis Xavier Engineering College

II. EXISTING METHODS

CDC Computing is an extended version of Cloud Computing. It also offers storage, computing and data accessing facilities to end users. In addition it also offers geographical distribution by providing proximity, and support mobility. The end devises are host to the network by the set-up boxes or access points. Further CDC computing enhances QoS and decreases latency. The reliability of CDC computing in real time cloud implementation and the challenges faces are presented by Madsen.H and Albeanu. G. In this technique geographical distribution of resources are used instead of the centralized technique used in cloud computing. CDC computing is implemented using multi-tier architecture. In this architecture the visualization and reporting is carried out by higher tiers [1]. Z. Jiang et al. developed a methodology

To increase reliability and fault tolerance [2]. They suggested their terminology outperforms in web base applications. Discussed Cloud Data Centre computing architecture and further used it for improving Web site's performance with the help of edge servers. It monitors the user's requests and MAC address to identify the attacks. Godoy et al. [6] suggested that profiling strategy is needed for user profiling. In last decays personal information agents helped to manage user information. In their work author explained the learning techniques for data acquisition and maintaining user profile. The time to time change and users interest is also adopted in that work. They proposed supervised and semantically maintaining techniques for useful profiles. The user account hijacking is identified as the drawback of the proposed method. The common threats and its impact on cloud performance is stated by Sabah. The risk of privacy and security is also discussed in this work. In his summary he highlighted the issues related to availability and reliability. Some algorithms are implemented in CDC computing algorithms to maintain flexibility, adaptability and to reduce site shutdown. DoS attacks are also reduced by this algorithms [8].

Cloud computing is presently an emerging model that visualizes a new model which provides everything-as-a-service. It virtualizes physical resources, infrastructure, and applications that are obtained over services provided by the cloud. Clear and distinctive potentials in cloud society is adopted by various cloud services. The cloud providers and services are increase rapidly, hence it is difficult to identify the best cloud providers to provide best provisioned services for the new users. So there is a need for identifying service provisioning techniques with optimal time and cost. Many approaches have been used to obtain optimal cost and time in an effective manner. The continuous cloud service provision which satisfies user need is mandatory for cloud users as well as cloud service providers. The new technique with secure cloud provision is proposed in the next section.

III. PROBLEM STATEMENT

It was a challenging issue of maintaining privacy and confidentiality in maintaining user data. This cloud computing change the use of computer. If the data stored under cloud server cannot be stored in a secured manner, then it is easy to hack the data. Therefore there is need of proper secured and threat detection technique.

Proposed technique called fog computing was introduced as a method to reduce the misuse of data. It was a simple technique. This method encompasses an exclusive model for data protection in the cloud using aggressive decoy technology for drowning the intruder with untruthful data.

IV. PROPOSED METHODOLOGY

In the proposed methodology, new prototype is implemented for secure data storage in cloud environment. In the first step the users are created and the pattern is generated for different access behaviors. In the second step user activity patterns are monitored using cumulative summation algorithm (CUSUM), to find the accuracy of the procedure. The development of the proposed protocol is shown in figure 1.

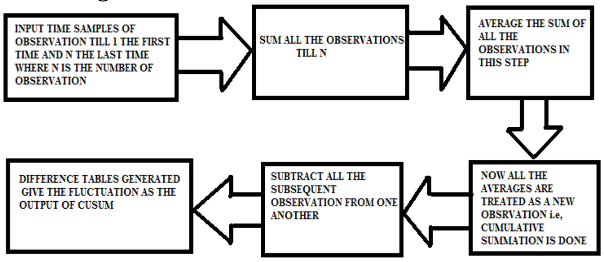

Figure 1. Methodology used

Documents or Decoy files are the trap files used to identify the illegal user in the cloud environment. These files are not useful for authenticated users but the entry of the attackers can be easily identified by Decoy files. The search mechanism of the illegal user behavior is different than the normal user. Hence it can be easily identified by the trap hit. If the trap is hit by the authenticated user by mistaken, it can be checked and solved with the help of some secret keys and answers. This procedure is illustrated in high level security architecture. The steps involved is demonstrated in figure 2. The activities are performed to maintain user file system safe and secure, also helps to identify irregularities.

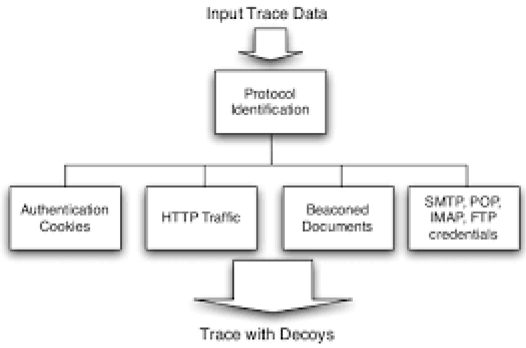

Figure 2. Decoy technique steps

Injecting traps (decoy technology): Injecting trap is a trick technology to confuse the attacker by including tap files. This trap files are included within the user's file system. If the attacker tries to open or access the file in a random manner the trap files are opened. So that an attacker cannot be access the original file. When the attacker tries to open a file the abnormality of a file is detected and the user behavior is detected.

The experimental parameters used are,

1) System Parameters-The experiments are conducted using 1 GHz processor with RAM 256MB or higher and hard disk 10 GB or higher.

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

2) Experiment Factors- To estimate the performance of CUSUM algorithm on the base of time, average fluctuation and true positive.

V. FEBER ALGORITHM

The proposed FEBR (Flow level Bandwidth Provisioning) algorithm used to reduces the switch scheduling problem to multiple instances of fair queuing problems. It was a queuing algorithm. For each individual flow the bandwidth of data is granulized. This algorithm inject various types of 'bait' traffic into each entities. A real time experiment is conducted to check if the user do not use the protection encryption method. This experiment generate a proof of detecting snooper and attacker. This algorithm have the following steps.

Algorithm 1:

Step 1: Initialize parameter for each router.
Step 2: Wait for the request until the current window is less than T.
Step 3: If the current window ends go to step 1.
Step 4: Else, If a request arrives identify the egress router.
Step 5: If $r_{p} < R(i)$ admit the request
Else Refuse the request

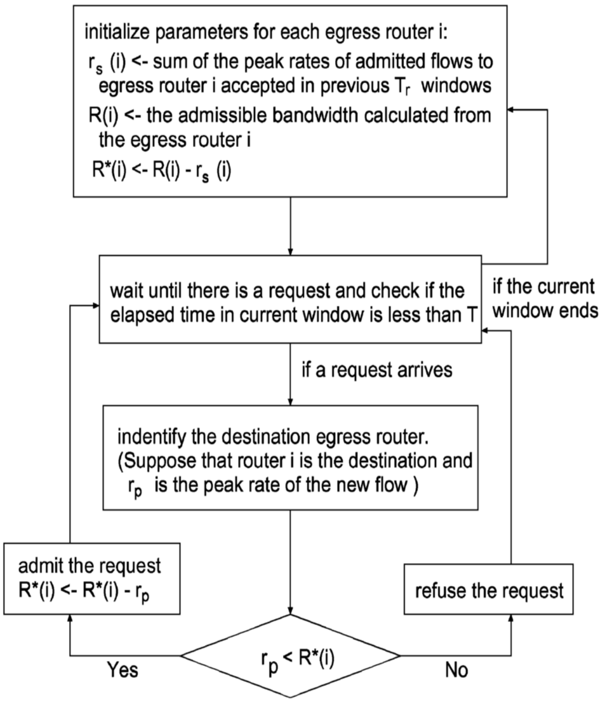

Figure 3. Steps in FEBER algorithm

Decoy broadcaster is an architectural component used for injecting duplicate file with the original file in a network environment. The injection workflow is mentioned as:

1. In a decoy broadcaster a new VAP is created.
2. A bait traffic is uploaded.
3. Inject the decoy traffic in a wireless cell.

In API the decoy information is generated by upcoming steps:
STEP 1: For each new file system a trap file is included.
STEP 2: Using authentication appliance user files are kept secure for reading and editing. If somebody accesses the trap file then using HMAC technique, we can identify the third party.
STEP 3: The CUSCUM algorithm will isolate the user behavior via following,
For applying CUSCUM on N no of observations
Let, initial average av1 -> N =0;
Sump = Sum till previous observations = 0;
For loop n=1 -> N
sump = sump(previous)+Current(n)av(n)=sump/Nend for loop
Now a v is the cumulative summary averages and difference in two sequential averages contributes the fluctuation.
STEP 4: If the threshold value more than 12 then the user is identified as an attacker.
STEP 5: After identifying an attacker they are classified as black and white list. List is updated for new user.
STEP 6: If a user satisfies the above conditions of an attacker, then, ask for email id and password for the authentication step.
STEP 7: If the user enters the id and password in a correct form, then the attacker is the actual one else the account of the user is temporarily locked.

VI. RESULTS & DISCUSSIONS

This section evaluates the performance of the proposed technique. The performance study is prepared in terms of transmission time essential for uploading files to the cloud server and to the fog nodes. It is perceived that time needed for uploading files to the cloud server is more than to the fog node. The processing time is extra in the cloud server. By considering three parameters of time, load and average fluation the accuracy is calculated. The accuracy of data is calculated using following equation (1). Where, TP = True Positive.

$$\text{Accuracy} = (\text{TP}/ \text{Total no. of cases}) * 100 \quad (1)$$

Table 1. Result for accuracy

User No.	True Positive	Accuracy
1.	1243	95
2.	1215	93
3.	1285	98
4.	1132	87
5.	1062	82
6.	1080	85
7.	1133	86
8.	1164	79
9.	1105	78
10.	1165	82

*Published By:
Blue Eyes Intelligence Engineering & Sciences Publication*

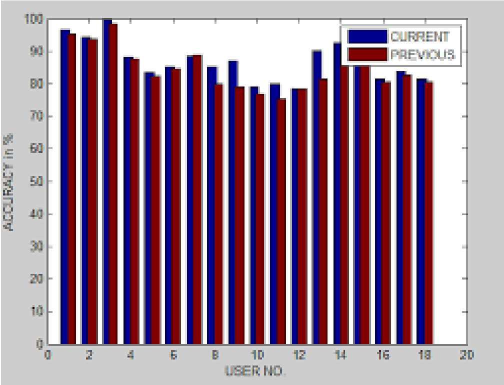

Figure 4. Performance graph

VII. CONCLUSION AND FUTURE ENHANCEMENT

To detect theft attack a CDC computing and decoy technology was proposed in this work. Former techniques used the encryption and decryption methods to secure data. But in proposed work CUSUM detection algorithm for detecting the abnormalities in user behavior profile. The time, fluctuation and load of user profile was evaluated using CUSCUM. Based on above mentioned parameters the results are evaluated. This also illustrates that CDC computing and decoy technology composed are able to meet the abnormalities and offer more perfect results as paralleled to previous techniques. Future work can be extended by applying various other algorithms and prevents from the insider data theft attacks. Also, the performance estimation of the technique can be measured by considering further attributes. It can be extended for network security via fog computing and also localizing the user data a protected topographical locations.

REFERENCES

1. Hashizume K., Rosado D. G., "An analysis of security issues for cloud computing". Journal of Internet Services and Applications, 2013, Vol 4(1), pp. 1-13.
2. M. Van, A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", 5th USENIX conference on Hot topics in security, ser. HotSec'10. ‖Berkeley, CA, USA‖: ‖USENIX Association‖, 2010, pp. 1–8.
3. 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. 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. 5.Zhu, Jiang,"Improving Web Sites Performance Using Edge Servers in Cloud Data Centre Computing Architecture", Service Oriented System Engineering (SOSE), IEEE. 2013.
6. 6. A.M. Anusha Bamini and Sharmini Enoch, "Dynamic Scheduling and Resource Allocation in Cloud", International Journal of Control Theory and Applications, Volume 10, No. 3, pp. 63-72, 2017.
7. 7. S. et al, "Decoy document deployment for effective masquerade attack detection," Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment, ser. Berlin, Heidelberg: Springer-Verlag, 2011.
8. 8. A.M. Anusha Bamini and Sharmini Enoch, "Optimized Scheduling and Resource Allocation using Evolutionary Algorithms in Cloud Environment", International Journal of Intelligent Engineering and Systems, Volume 10, No. 5, pp. 125-133, 2017.
9. 9.Marinos A. & Briscoe G., "Community Cloud Computing", Heidelberg: Springer, 2009, pp. 472-484.
10. 10.Grobauer, B., Walloschek, T., & Stocker, E., "Understanding cloud computing vulnerabilities". Security & Privacy, IEEE, 2011, pp. 50-57.
11. 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. 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. 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. 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. 15. M. Ben-Salem, "Cloud Computing Vulnerability Incidents: A Statistical Overview", Cloud Security Alliance, August 23, 2012; Revised March 13, 2013.
16. 16. N. Alon, H. Kaplan, M. Krivelevich, D. Malkhi, and J. Stern. Scalable secure storage when half the system is faulty. In ICALP, 2000.
17. 17. C. Wang et al., "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Trans. Computers*, vol. 62, no. 2, 2013, pp. 362–375.
18. 18. M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos. Hourglass Schemes: how to prove that cloud files are encrypted. In CCS, 2012.