www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-3

International Journal of Intellectual Advancements and Research in Engineering Computations

PPHOP survey for manage the inside threat attack detection in cloud storage

A.Shenbagam[1], Jothilakshmi[2]

[1]M.Phil, Research Scholar (Full-Time),

[2]Assistant Professor.

[1, 2]PG and Research Department of Computer Science Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam.

ABSTRACT

Privacy-preserving High-order PPHOP c-Means Scheme that allows support for all users to conveniently access data over the cloud and control and detect the inside threat attack. Data owner is not able to control all over their data and security issues. The new security issues of Insider Threat Attack Various techniques are available to support user privacy and secure data sharing and detect of control the Insider Threat attack. An insider threat was the misuse of information through malicious intent, accidents or malware. The study also examined four best practices companies could follow to implement a secure strategy, such as business partnerships, prioritizing initiatives, controlling access, and implementing technology. This paper focus on various schemes to deal with secure data sharing such as Data sharing with forward security, secure data sharing for dynamic groups, Attribute based data sharing, encrypted data sharing and Shared Authority Based Privacy-preserving High-order PPHOP c-Means Scheme for access control of outsourced data. In this paper improve the could security issuses and inside threat attack.

Keywords: PPHOP, IDC claims, Phishing attack

INTRODUCTION

Cloud storage is a system to ensure the data security and save the storage space through the functions such as clustered application, distributed cloud system. The Cloud storage enable different types of storage devices to work together to provide data storage services and business access functions through applications. The users can connect to the cloud and access the data easily through any devices connected to the Internet. At present, cloud storage technology has become a hot topic in the field of computer research. One and the major security issues in a cloud is to detect and prevent a network intrusion. There are the malicious users at client side, malicious user at cloud providers side and provider itself, can learn authentication information to gain a access of the others VMs. Malicious provider monitors network communication to gain information about client's behavior. Cloud infrastructure makes a use of virtualization techniques, integrated technologies and run through standard internet protocols. These may attract a intruder due to many vulnerabilities involved in it. Cloud computing suffer from various traditional attacks such as zombie attack (flooding attack) and Denial of service attack etc. User can communicate with cloud service provider by a Virtual Machines and CSP manage the users data on a cloud at virtual servers. An illegitimate users or malicious attackers act as a legitimate users and affects the services of its legitimate users. There are some common intrusions, which causes availability, confidentiality and integrity issues to cloud resources and services. Privacy-preserving High-order PPHOP c-Means Scheme can be used.

Author for correspondence:

M.Phil, Research Scholar (Full-Time), PG and Research Department of Computer Science Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam.

Where signature based detection is used for known attacks and anomaly is used for unknown attacks.

RELATED WORK

It presents a review on intrusion detection techniques for cloud computing and security challenges. Cloud Computing is a 1st choice of every it organization because of its scalable and flexible nature. The security and privacy is a major Challenge in CC. IDS is most commonly used mechanism to detect a various attacks on cloud. In this paper Various IDS techniques are analyzed with respect to their types, positioning, detection time, detection techniques, data sources and attacks. The analysis provides a limitations of each technique to fulfill the security needs of cloud computing environment. R.Aishwarya & Dr.Sc Malliga [13] Proposed the intrusion detection system against DOS and DDOS attacks in the cloud environment. cloud computing is a one of the emerging and glooming technology in IT where information is permanently stored in the third party cloud servers and cached temporarily on clients with the help of different devices. One of the major threats to cloud security is DOS or DDOS attack in the virtual machines. Here the DOS attack is overcome using hop-count filtering methodology. In the proposed method two layers of security are provided and MAC generator differentiates the legitimate client from the spoofed ones providing a security for the data packets allowing the clients to use the resources of the cloud server more efficiently. Fouad Guenane, Michele Nogueira and Guy Pujolle [14]. The Proposed technique is related to a reduction of DDOS attacks impacts using a hybrid cloud- based firewall architecture. This work presented a DDOS mitigation service based on hybrid cloud based architecture it provides a good performance in adopting existing technologies for the next generation of security services . As a future work it intend to study the impact of the proposed architecture on the application layer and design a better decision model. SS. Chopade, K. U. Pandey and D.S. Bhode [15] Securing cloud servers against flooding based attacks. This paper presents a simple distance estimation based technique to detect and present the cloud from flooding based DDOS attack and there by protect other servers and users from its adverse effects. Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee and Dijiang Huange (2013) [16] Propose the Network Intrusion Detection and Countermeasure Selection in virtual network system in cloud computing. Security from attacks is an important issue in a cloud computing & , attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large scale distributed denial of services. Dos attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning & compromising identified vulnerable virtual machines as zombies, with in the cloud system, especially the iaas clouds, the detection of zombie exploration attack is extremely difficult. For a better attack detection NICE employes a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, they preventing a zombie VMs. In this technique the (NICE-A) Network intrusion detection Agent is installed on each cloud server to capture and analyze the network traffic. The Proposed solution can significantly reduce the risk of the cloud system. NICE only investigates the network IDS approach to counter a zombie explorative attack. In order to improve the detection accuracy, host based IDS solutions spectrum of IDS in cloud system, this should be investigated in future work. Chirag N. Modi & Dhiran Patel (2013) [2] Propose a novel security framework hybrid network intrusion detection system. This framework aims to detect a network attacks in cloud by monitoring network traffic, while ensuring a performance and service quality. In H-NIDS two techniques signature Based detection for known attacks and anomaly detection techniques for unknown attacks are used. In signature based detection snort and signature apriority Scheme is used and in anomaly detection three different classifiers Bayesian, Associative & Decision tree are used. Moreover, a suitable score function determines whether the intrusion predicted by different classifiers are actually intrusion or not, Also it is used to detect a distributed attack in cloud. H-NIDS is deployed on each host machine in cloud. It helps to detect a internal & external network attacks. The central log and score function in H-NIDS helps to detect distributed attack in the cloud. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B

Fernandez (2013) [1] Proposed the analysis of security issues of cloud computing. They worked up upon SPI model i.e SaaS,PaaS,IaaS) vulnerabilities and threats .As when data is travelled through internet or involvement of third party is there, at that time we have to ensure the security factors and provide proof of security to organization. List of vulnerabilities and different threats, relationship between then is also discussed. Different types of virtualization technologies approach security mechanisms in different ways. Storage, virtualization, and networks are the biggest security concerns in Cloud Computing. They have focused on this distinction, where we consider important to understand these issues. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. Due to some complexities in previous security mechanism it doesn't work properly because it was combination of different technologies, so new security techniques and technology is needed to avoid those problems. When virtual network communicate with remote virtual machines, it is also target for some security attacks and vulnerabilities. They have discussed some vulnerabilities and left with some for future work. Jian Yu, Quan Z. Sheng, Yanbo Han [3] Proposed special issues and service computing of cloud computing. Cloud services include reliability model, service virtualization, and user-centric services. Cloud service reliability mode l , service virtualization, and user-centric services. They have proposes a stochastic reliability model of atomic Web services. Some fault tolerance techniques have been proposed using recovery block adaptation to improve the quality of service. Fuzzy requirements and a two-level ranking Scheme are discussed and evaluated. One of them have proposes a spreadsheet-like programming environment called mashroom to support situational data integration by non professional users. This paper focus on key directions in this vibrant and rapidly expanding area of research and development. One important issue is that large-scale data centers must offer reliable and secure services with high quality standards to satisfy the on-demand needs of users, to develop service security. Joel Gibson, Darren Eveleigh, Robin Rondeau, Qling Tan [2]: Proposed the challenges that are faced by the service models in cloud. The three pre dominant models that are present in the cloud computing are mainly infrastructure as service, platform as service and software as service. Infrastructure as service provides with the use of servers, storage and virtualization to enable utility like services for user. Security becomes the major challenge in the infrastructure as service as rest of the top cloud services run on the top of this service In software as service and platform as service the major challenge that arises is that at times it becomes critical to understand the cloud service models which determine the cloud services hosting are an appropriate business solution.

This paper gives clear indication that services should be available at anytime and anywhere so that availability of services do not decrease. Main issue is lack of services and resource availability which leads to inadequacy. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom [4]: Proposed the research related to security of single cloud and multi-cloud and solution regarding them. As dealing with single cloud became less popular, due to innovation of "multi-cloud", "inter cloud", "cloud of cloud".

Various security factors have different impacts on different services. As its being described that multi-cloud infrastructure requires less security attention as compare to single cloud. Recently several users faced many problems due to data intrusion, availability. Security techniques such as encrypting data using cryptographic hash function for maintaining data integrity and storing data on different servers to overcome the limitation of availability of data.

METHODOLOGY

This paper proposes a PPHOP c-Means Scheme for cloud storage. PPHOP is one important scheme of cloud. PPHOP can reflect the typicality of each object to different clusters effectively and it is able to detect the inside attack in cloud process .However. Specially, it cannot capture the complex correlation over multiple modalities of the heterogeneous data object. The paper proposes a high order PPHOP Scheme by extending the conventional PPHOP Scheme in the tensor space. In this paper, the proposed PPHOP c- means Scheme represents each object by using a tensor to reveal the correlation over multiple modalities of

the heterogeneous data object. To increase the efficiency for detecting the inside attack on cloud storage, we design a distributed PPHOP c-means Scheme based on Map Reduce to employ cloud servers to perform. However, the private data tends to be in disclosure when performing PPHOP on cloud. Take the medical data which is a typical type of cloud storage for example. A large amount of private information such as personal email address and diagnostic data is included in the medical records. The disclosure of the private information will threaten people's lives and property greatly. Therefore, to protect the private data on cloud, we propose a privacy preserving PPHOP c-means Scheme technique that is of high efficiency Unfortunately, BGV does not support the division operations and square root operations that are the necessary computation in the functions for updating the membership matrix and clustering centers in the PPHOP c-means Scheme although it is a fully for inside attack detection on cloud storage.

PROBLEM STATEMENT

Cloud computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including modification, insertion, deletion, appending and reordering, etc. To ensure storage accuracy under dynamic data update is most importance. However this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. In the previous times various effective distributed techniques with overt dynamic data support to ensure that of users data in the cloud is correct. They depend on Elimination correcting code in the file distribution preparation to provide redundancies and guarantee in the data dependability. This design reduces the communication and storage overhead as such as the traditional replication based file distribution scheme. By using the homomorphism token with distributed verification of erasure coded data and their scheme achieves the data correctness insurance and data error localization whenever data corruption has been identified during the storage correctness verification their method can almost guarantee the simultaneous localization of data errors, i.e., the detecting the misbehaving server(s). The new method further supports secure and efficient dynamic operations on data blocks including: deletion data update and append. Extensive performance and described security analysis shows that the proposed technique is highly efficient and resilient against Byzantine failure, malicious data altering attack and even denial of services attacks also. In future work, we propose a novel technique to isolate zombie attack in cloud architecture and tried to detect malicious attackers with secure authentication between user and server.

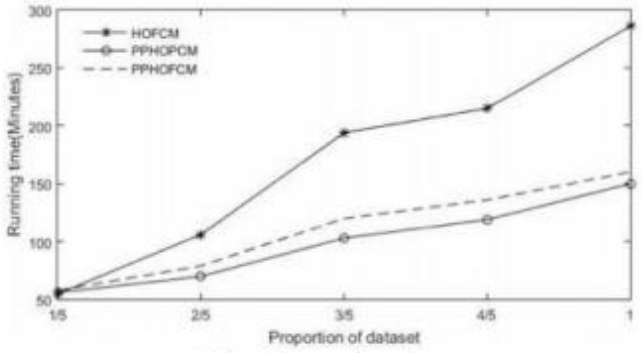

Fig .1 Running time

This paper proposes a privacy preserving high order PCM scheme (PPHOP) for clustering. PCM is one important scheme of clustering. PCM can reflect the typicality of each object to different clusters effectively and it is able to avoid the corruption of noise in the clustering process .However, PCM cannot be applied to clustering directly since it is initially designed for the small structured dataset. Specially, it cannot capture the complex correlation over multiple modalities of the heterogeneous data object. The paper proposes a high order PCM Scheme by extending the conventional PCM Scheme in the tensor space. Tensor is called a multidimensional array in mathematics and it is widely used to represent heterogeneous data in analysis and mining. In this paper, the proposed HOPCM Scheme represents each object by using a tensor to reveal the correlation over multiple modalities of the heterogeneous data object. To boost the effectiveness for cluster big data, we design a distributed HOPCM Scheme based on Map Reduce to employ cloud servers to perform the HOPCM Scheme. However, the private data tends to be in disclosure when performing HOPCM on cloud. Take the medical data which is a typical type of for example.

RESULT AND DISCUSSIONS

To evaluate the performance of the proposed Scheme carry out some experiments an one important technique for attack on distributed network. A PPHOP c-Means Scheme has been widely used in analysis and knowledge discovery. However, it is difficult for PPHOP to produce a good result for inside attack detection, especially for heterogenous data, since it is initially designed for only small structured dataset. The paper proposes a high-order PPHOP Scheme for cloud data storage. Clustering by optimizing the objective function in the tensor space. Further, we design a distributed PPHOP method based on Map Reduce for very large amounts of heterogeneous data. Finally, we devise a privacy-preserving PPHOP Scheme to protect the private data on cloud by applying the BGV encryption scheme to PPHOP, In PPHOP, the functions for updating the membership matrix and clustering centers are approximated as polynomial functions to support the secure computing of the BGV scheme. Experimental results indicate that PPHOP can effectively cluster a large number of heterogeneous data using cloud computing without disclosure of private data.

The following Architecture diagram for detection on cloud storage

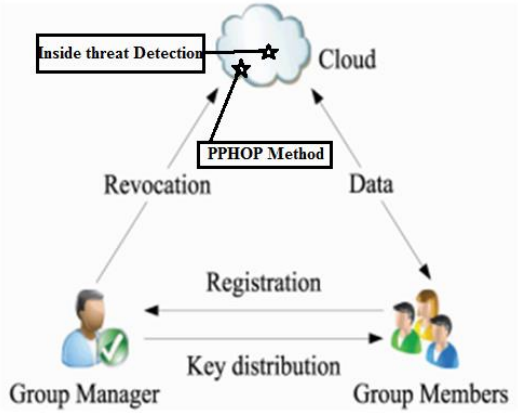

Fig .2.0 Architecture

CONCLUSION

We proposed a high-order PPHOP scheme for PPHOP c-Means Scheme storage ifs well support inside attack detection on cloud storage. Furthermore, cloud servers are employed to improve the efficiency for cloud data storage by designing a distributed PPHOP scheme depending on Map Reduce. One property of the paper is to use the BGV technique to develop a privacy-preserving PPHOP Scheme for preserving privacy on cloud. Experimental results show PPHOP can cloud storage by using the cloud computing technology

without disclosing privacy. In fact, for the large scale of heterogeneous data that does not require to be protected, the PPHOP is more suitable since it is more efficient than PPHOP. The efficiency of PPHOP and PPHOP can be further improved when using more cloud servers, making them more suitable for big data clustering, since they are of high scalability demonstrated by the experimental results.

REFERENCES

[1]. Zhongma Zhu and Rui Jiang, "A Secure AntiCollusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, 27(1), 2016..

[2]. Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy Preserving Authentication Protocol in Cloud Computing,"

[3]. Xin Dong a, Jiadi Yu a, Yuan Luo , Yingying Chen, Guangtao Xue , Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," Science Direct journal homepage: www.elsevier.com/locate/cose computers & s e c u rity 42, 2014, 151, e1 64, Elsevier Ltd 2013.

[4]. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, 24(6), 2013.

[5]. Kaiping Xue and Peilin Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," Citation information: DOI 10.1109/TCC.2014.2366152, IEEE Transactions on Cloud Computing.

[6]. HUANG Qinlong, MA Zhaofeng, YANG Yixian, FU Jingyi and NIU Xinxin, "EABDS: Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing," Chinese Journal of Electronics 24(4), 2015.

[7]. Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE Transactions On Knowledge And Data Engineering, 25(10), 2013.

[8]. Ming Li Member, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, " Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption," IEEE Transactions On Parallel And Distributed Systems 2012.

[9]. Qiang Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, 9(11), 2014.

[10]. Xinyi Huang, Joseph K. Liu, Shaohua Tang, IEEE, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," IEEE Transactions On Computers,64(4), 2015.

[11]. R. A. Popa and N. Zeldovich, " Multi-Key Searchable Encryption," Available: http://eprint.iacr.org/2013/508.

[12]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, 79–88.

[13]. Tim, Mather, SubraKumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance," O'Reilly Media, Inc., 2009.

[14]. Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Base Solution for Flexible and Scalable Access Control in Cloud Computing" in Proc. IEEE Transactions on Information Forensics and Security, 7(2), 2012.

[15]. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. Communications of the ACM, 53(4), 2010, 50-58.

[16]. S.Yu, C.Wang, K.Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Infocom 2010, 2010, 534– 542.

[17]. C. Modi, D, Patel, b. Borisanya, A. Patel, an," M. Rajarajan," A novel framework for intrusion detection in cloud ,"Proceeding of the Fifth International Conference on Security of Information and Networks(SIN-2012), 2012, 67-74.

[18]. Snehal G. Kene and Deepti P. Theng (2015), "A Review on intrusion detection techniques for cloud computing and security challenges" , IEEE 2014 .

[19]. R.Aishwarya & Dr.Sc Malliga (2014) , "IDS – An efficient way to thwart against DOS/DDOS attack in cloud environment", IEEE 2015.

[20]. Fouad Guenane, Michele Nogueira and Guy Pujolle (2014)," Reducing the DDOS attacks impacts using hybrid cloud-based firewalling architecture", IEEE2014.

[21]. S.S. Chopade, K. U. Pandey and D.S. Bhode (2013), "Securing a cloud servers against flooding based DDOS attacks", IEEE 2013.

[22]. Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang (2013), "Network Intrusion detection and countermeasure selection in virtual network systems ", IEEE (2013).