An Analysis of Various Security Issues and Recent Techniques in Multi-Cloud Computing Environment

K.A.Dhamotharan and Kavin

Abstract--- *Cloud computing is most widely recognized technology in today environment where the millions of users are attempting to utilize the services provided by cloud service providers. There are many types of services are distributed to the cloud users based on their requirements. The main reason behind the success of cloud computing service providers is, it is pay per use model and the also it provides the most flexible environment to the cloud users to utilize their resources. Various issues could occur in the cloud computing environment where the number of users is increased in number and the management of cloud resources becomes critical issue. In this research work, survey is conducted towards the types of issues present in the cloud computing resources. This article mainly concentrates on the security issues that might happen in the cloud computing environment. The various research works that focused on resolving the security issues are also listed and discussed shortly about them. The analysed methodologies are implemented using the CloudSim toolkit which is evaluated to know the performance of every research works. The experimental tests conducted in the environment of 3 data centers, 50 virtual machines and 500 jobs. The comparison was made between the techniques that have been listed. The performance evaluation conducted was proved that the each and every method has unique advantage and disadvantages among each other.*

Keywords--- *Cloud Security, Encryption/Decryption, Identity, Multi-Cloud, Attributes.*

I. INTRODUCTION

Cloud computing is a resource sharing environment which distributes their resources in multiple places to share them to millions of users. Cloud computing provides various types of services to the cloud users as per their requirements. The cloud computing services are divided into three types based on their types of service it provides. Those are Software as a Service (SaaS), Platform as a Service (Paas) and Infrastructure as a Service (IaaS). SaaS provided the inbuilt application like games, windows software (MS word, pdf, web application and so on) to the cloud users. The cloud users can get resources from SaaS, thus the burden of maintaining and updating the software can reduced considerably. PaaS provides the perfect environment for executing the tasks that the users intends to do. PaaS will setup the complete execution environment like front end and back end application to enable the users to execute and run their tasks without corruption. IaaS is the type of service which ensures the delivery of storage and server resources to the cloud users. This IaaS environment needs to be handled in the effective manner for provisioning the resources without failure. Likewise every resource providers provides their services to the cloud users in different ways whereas users also share their sensitive information to many users with the help of cloud storage services.

S. Vishaka, II M.E (CSE), Angel College of Engineering & Technology. E-mail:vishaka1992.s@gmail.com
S. Selvi, ME (Ph.D.), Assistant Professor, Department of CSE, Angel College of Engineering & Technology. E-mail:selvi.me08@gmail.com

The security and privacy becomes the most critical issue while sharing the cloud resources to the users. The secured environment needs to be assured for the cloud users to make them to continue their service with the cloud service provides. Cloud security could be violated in many ways while sharing the users sensitive through cloud server by storing it in there. The issues that may rise in cloud computing while attempting to store the sensitive information in the cloud service providers are listed below.

- Data Stealing/Data Corruption.
- Key Management Issues.
- Insecure Authentication.
- Revocation Handling Management and so on.

These are all some of the main issues that frequently faced by both cloud service providers and as well as cloud users. These issues need to be taken care of to assure the secured environment for cloud users to storing and sharing their sensitive information. There is various research works had been conducted towards achieving the secured cloud computing environment. The existing research works are attempting to avoid the security issues that are mentioned above by introducing various novel methodologies. The previously introduced methodologies are better in some ways by avoiding the security issues whereas it might also degrades in its performance in some factors.

The contribution of this analysis work is to discuss the various methodologies that are introduced to overcome the issues that are mentioned above. In this work, merits and demerits of all the methodologies are discussed shortly, so that one can understand and improve the demerits present in the previous research works to create novel proposed approach. Finally the performance evaluation was conducted in all the discussed methodologies to show which one of the algorithm is effective in nature by avoiding the security issues.

The organization of this work is given as like follows: In this section, short introduction about the focus of this research is discussed. In section 2 various research methodologies that are introduced to overcome the issues mentioned above has been simplified shortly. In section 3 performance evaluation that was conducted to know the better research methodology that can overcome the security issues considerably. In section 4, the findings of this overall research work is concluded shortly.

II. SECURITY ISSUES THAT OCCURS IN CLOUD ENVIRONMENT

Security is the important factor in the cloud computing environment which need to be assured to the cloud users who are attempting to store and share their sensitive information via cloud services. The attempt to store the sensitive information to the third party server itself would lead to various security issues where there is a possibility of stealing data. The problem may arise while sharing the data with other users where the authentication needs to be done preventing malicious user access. In the following sub sections, different research methodologies that attempt to enable the secured cloud computing environment are discussed shortly.

A. Data Stealing/ Data Corruption

Data corruption and stealing is one of the main research issues which happen in the cloud storage services which are provided by the third party servers. The cloud users are who are willing to share their information to multiple users would require some intermediate services for sharing instead of sharing it in via emails which is an most complex process to address all each and every time whenever the resource sharing is done. At that time, the cloud resource providers who are third party server may attempt to steal the data's which are stored by the cloud users. This security violation may reduce the number of cloud users who are willing to share their sensitive information. There are various research works had been conducted which focuses on achieving the cloud security where the cloud service providers cannot steal the data's that are sent by the cloud users. Some of the research work has been discussed below shortly.

Cong wang et al [1] proposed an erasure code based data verifiability operation to ensure whether the data stored in the cloud server is handled correctly or not. This approach is based on token verification method to verify the correctness of the data that are stored in the cloud server. This method will generate the tokens to detect malicious behaviour of the cloud server by matching the tokens that are generated. The main idea behind this methodology is, "whenever the cloud users wants to check the data correctness that are stored in the cloud server, they would generate the token keys for every blocks of data with the help of signature which is computed by using the public key of cloud providers. These token would be passed to the cloud server who need to generate signature on it. If the server has not performed any malicious behaviour then he can crack the signature that was embedded on the token which was sent by cloud users. If the cloud provider not able to crack the signature for verification then we can say that the cloud service provider is malicious on who modify the contents of cloud storage". If the server found to erroneous, the automatic error correction would be invoked to restore the original data with the help of tokenized data's.

Seny Kamara et al [2] introduced the cryptographic environment for the cloud storage services where the user submitted data can be maintained securely. It is enabled by allowing the users to encrypt their data and sensitive information before storing it in the cloud storage. The encryption of data can be done by using any of the encryption techniques that are available in real world to ensure the proper delivery of resources. Once the encryption is done, the cryptographic keys need to handle in the efficient and secured way for maintaining the security of data that are stored in cloud. This cryptographic environment of the cloud storage services consist of involvement of roles like data processor, data verifier and token generator. The efficient management of data consists of the various case studies that are involved over a providing the secured and promising environment to the cloud users.

Hongwei Li et al [3] introduced the new encryption methodology for preventing the sensitive information from the malicious activities. This methodology is based on encrypting the data contents with the help of identity of users to differentiate from their access permission. The access permission can be differentiated with the help of the different identity information of individual users. The content of data owner would be encrypted in block level where each and every block would be encrypted using different identity to differentiate and separate the access permission. Based on these identity information users can get access by submitting their identity information to the cloud server for validation. If the identity information submitted by users and identity information available in the cloud server then the users would be authenticated as valid users. Else they would be authenticated as invalid users.

Joseph K. Liu et al [12] introduced two-factor data security protection mechanism which allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the ciphertext without either piece. More importantly, once the security device is stolen or lost, this device is revoked.

These are all some of the security issues which will occurs while storing the users sensitive information to the cloud servers. These data contents would lead to various security issues like data corruption, data integrity, data stealing and so on. The methodologies which can solve these issues and protect the data from the security violation are discussed above shortly.

B. Key Management Issues

The key management issue are another important issue which need to be resolved to improve the security from the unknown users who may violate the data contents by stealing the authentication keys. It is required to share the encryption/decryption keys with cloud users to enable them to retrieve the contents that are stored in the cloud server. Because while sharing the secret keys with cloud users through unknown medium there is a possibility of security violation. This needs to be avoided by handling the keys in the secured manner. The methodologies which focus on securing the transmission and reception of secret keys are discussed shortly below.

Cheng-Kang Chu et al [4] proposed key aggregate cryptosystem which is used to protect and manage the secret keys that are generated to protect the data access from the malicious users. This method is based on protecting the secret keys which are used to encrypt the content that are stored in cloud server by aggregating together which would be shared with the cloud users to give them access for data retrieval. The scalability issues also handled in this work by introducing the constant size cipher text based encryption. These constant size cipher text ids are used to encrypt the data contents in the block level which can then would aggregate together to reduce the burden of handling large volume of data’s together. These set of secret keys are aggregated together which would be shared with the cloud users for authentication process. The hackers cannot hack the secret keys while sharing with unknown users from the aggregated keys where the keys are aggregated and encrypted together.

In [5], leakage resilient cryptosystem is introduced where the keys cannot be hacked while transferring it through insecure medium. It is done by introducing the new methodology called the hashing based encryption where the keys are aggregated and it is encrypted using the identity of users. This work introduces another methodology which is based on encapsulation based encryption methodology where the aggregated key would be encapsulated with the encapsulation key after hashing the value of secret key which is used to encrypt the keys. The encapsulation of secret keys is used to improve the security level of the proposed methodology where the aggregated keys would be stored. These are all the methodologies which were concentrated to provide the security for the secret keys which would be used for decrypting the cloud stored contents. These contents need to be retrieved in order to fulfil the needs of cloud users. The retrieval and management of cloud stored data need to done in the secured and flexible manner which are all discussed in the following section.

C. Insecure Authentication/Privacy Violation

Authentication becomes the most concerned and required process in the cloud computing environment which is used to prevent the accessing of cloud contents from the unauthorized users. There are various approaches have been introduced that focuses to provide the authentication for the users and limit the data access control of them by checking their access policy information. Some of the research works has been discussed in this section.

In [6], anonymous authentication process is introduced which would prevent the malicious users from accessing of cloud contents in the secured way. This is done by introducing the mechanism called the attribute based encryption in which cloud contents are encrypted by using the general attributes that are used to differentiate the identity of users without leaking their personal information. Anonymous authentication is the process of storing and retrieving the contents to the cloud user without revealing their personal information. When the cloud users are approaching to the cloud servers for accessing the cloud stored contents, the attributes of those users would be collected to match with the attributes that are provided by the data owner. If those attribute values are matches together then the access permission would be granted. Else it would be rejected. The methodology introduced in this work decentralizes the data accessing permission in order to reduce the burden of cloud servers in the considerable manner. This is achieved by removing the centralized server concept where only the centralized server is responsible for limiting the data access permission. Whenever the data a user approaching the cloud server for accessing the contents, then the key management server resides in the particular region would take care of accessing of contents. This decentralized accessing of cloud may reduce the burden of cloud servers and as well as improve the data accessing speed.

In [7], public auditing is introduced which would preserve the data integrity level by periodically updating the cloud server and its sub servers. In this mechanism ORUTA (One Ring to Rule All) mechanism is introduced to control the contents that are updated by the cloud users. This is achieved by passing rings to the users present in the cloud environment. The user who poses the ring only can modify the contents stored in the cloud environment. Other users who are having ring, but willing to modify the cloud contents need to be waited for some time in order to preserve the updated version copy of cloud contents to every users. The users who are modifying the contents need to sign in the contents before modification, so the malicious users can be prevented. Only the users with original validity information can preserve the original copy of data. The cloud server will periodically check for the new signature that resides in the cloud contents. If it is found then the cloud contents would be updated for obtaining fresh data.

In [8], public auditing is done by using the third party servers who would check the integrity level of cloud contents that are stored in the cloud servers. The public auditing is done in the block level which eliminates the need of downloading of entire contents from the cloud server whenever the update is required. This process reduces the wastage of bandwidth and as well as avoids the more computation time. The third party server who is called as public auditor would periodically check the cloud contents for any updated contents by comparing it with the original copy of data’s. The original version of data could be preserved by downloading the contents that modified only without downloading the entire contents. Public verifier would check the authentication of users by checking the integrity level of the users. The cloud stored contents need to be preserved well for obtaining the fresh copy of data's.

In [9], discussed various mechanisms that are used to retrieve and maintain the data contents with the privacy concern in the more secured way. This methodology attempt to find the mechanism that can retrieve the fresh copy of data by checking the modification resides in the cloud environment. The users need to sign the data before accessing the cloud stored contents in which user's identity might get revealed. This signature might reveal the original identity of the users which leads to privacy violation of users. This work also discusses the various privacy methodologies that concentrated to hide the user identity as well as does an authentication to protect the data contents from malicious users. The privacy level and the authentication level of the users stored contents are well preserved for the efficient handling of data's. This section makes an overview about the various authentication and privacy mechanism which attempts to reduce the security violation and prevent the leakage of privacy preserved information.

D. Revocation Handling Management

In this section, various revocation methodologies are discussed. Revocation is the process of eliminating the access permission of malicious users from the environment. Revocation need to be handled with the concern of other user's authentication permission which might violated while trying to remove the authentication permission of revoked users. Some of the research methodologies that concentrated to avoid the revocation concepts are discusses in the following section.

In [10], introduced the identity based encryption which attempts to authenticate the users by using the identity information of the users. This work also attempts to protect the revoke the users who are acting as malicious providers in the environment. This revocation might violate the accessing permission of other users with the presence of common identity information in other users access permission key. The revocation process in this methodology is outsourced to reduce the burden of cloud server from the update process of generating update keys. The outsourced revocation is done with the help of key updating server and the key distribution centre that takes responsibility of generation and outsources the update keys to the cloud user. The cloud user will update their access permission key locally with the help of update key. Thus the revoked user's identity could be fully revoked without violating the access permission of other users.

Yan Zhu et al. [11] proposed a novel dynamic audit service for the untrusted and outsourced data from the cloud. The main goal of this approach is to provide a data integrity check when the data are shared to the untrusted cloud. This work tries to achieve the security metric given in the following list to check the performance of this approach. Those security metrics are Public auditability, Dynamic operation, Timely detection, Effective forensic, Lightweight.

The architecture of this work consists of four entities, namely data owner, Cloud service providers, Third party public auditor and authorized application. The audit service in this approach comprises of three processes. Those are Tag Generation, Periodic sampling audit, Audit for dynamic operation. The performance of TPA and storage service providers is enhanced by introducing the concept of periodic sampling audit mechanism.

E. Analysis

The performance analysis of this work is done to identify the merits and demerits of these methodologies. So that, the comparison can be made between the methodologies that were discussed above. The analysis of this work is given in the following table

Table 1: Analysis of the Discussed Methodologies

S.No	Title	Author	Method	Merits	Demerits
1	Toward Secure and Dependable Storage Services in Cloud Computing	Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou	Erasure code based data correctness	reduce the data integrity and availability threats. efficient storage correctness validation	only providing binary results for the storage verification
2	Cryptographic Cloud Storage	Seny Kamara, Kristin Lauter	Cryptographic functions	Better security of cloud services. Improves confidentiality	Data integrity can be compromised
3	Identity-Based Cryptography for Cloud Security	Hongwei Li, Yuanshun Dai, Bo Yang	Identity based Encryption, Identity based Signature	Better data access control Can revoke users efficiently	Less security at the time revocation where the revoked users may hack the secret keys with the help of partial information
4	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng	Key-Aggregate Cryptosystem	Efficient handling of large volume of data. Scalability support.	The aggregated key might get corrupted in the less secured medium. The large volume of data cannot be supported due to presence of constant cipher text id’s.
5	Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions	Sherman S.M. Chow, Yevgeniy Dodis, Yannis Rouselakis, Brent Waters	Leakage resilient cryptosystem	More flexible approach to protect the keys in the secured manner. Can handle large volume of data’s securely.	Hashing would be more complex to do for large volume of data’s
6	Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds	Sushmita Ruj, Milos Stojmenovic, Amiya Nayak	Attribute based encryption	Decentralized access permission which makes the computation fast More security.	More burden of handling large volume of attributes.
7	Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”, IEEE Transactions On Cloud Computing	Boyang Wang, Baochun Li, and Hui Li	ORUTA	Better auditing process. More data integrity.	More computation time. User need to wait until they get ring key for further modification.
8	Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud	Boyang Wang, Baochun Li, and Hui Li	Public auditing	Better preservation of cloud stored contents. Improved data integrity level. Reduced computation time.	Security violation might occur in case of presence of malicious third party server.
9	Enhancing Data Integrity and Privacy in the Cloud: An Agenda	David S.L. Wei, San Murugesan, Sy-Yen Kuo, Kshirasagar Naik, Danny Krizanc	Privacy preserved data integrity checking	Improved data integrity level. More privacy concern.	Less accuracy of detection of data integrity level.
10	Identity-Based Encryption with Outsourced Revocation in Cloud Computing	Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou	Identity based Encryption	Better access control.	Less security due to leakage of identity information’s.
11	Dynamic Audit Services for Outsourced Storages in Clouds	Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu	Dynamic audit services	Less communication overhead. Less memory storage.	Highly causes from security attacks.
12	Two-factor data security protection mechanism for cloud storage system	Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y	Two-factor data security protection mechanism	Automated updation cipher text is done which ensures the data integrity	More computational complexity

From this analysis table, we can conclude that the every methodologies proposed previously consists of various merits and demerits in their way of application. All the merits and demerits involved in these works are considered for the review from which new methodology can be proposed by combining the merits of all the methodologies. The performance analysis were conducted to check the consistent level of the various proposed methodologies which is described detailed in the following sections.

F. Survey Result

The performance evaluation is done to know the improvement of various research methodologies which was plotted in the graphical representation. This comparison was done based on the parameters called the execution time and computation overhead which is done to compare the effectiveness of algorithms discussed previously. The performance evaluation is done based many performance metrics. Those are Query time and computation overhead.

Query Time: The time taken to submit a query with difference workload sizes are evaluated and compared with the existing algorithms. The below graph shows the comparison of various methodologies in terms of execution time which is observed for different file sizes.

Computation Overhead: The computation overhead defines the overall processing capacity utilized for process the user submitted query. The computation overhead should be minimized in order to improve the overall effectiveness of the proposed method

Some of methodologies are better in the query response time by retrieving answer for user queries fastly. Some of the methodologies lack to produce result with response time where it may consume more computation overhead value. The conclusion of this analysis is given in the following section.

III. CONCLUSION

Cloud computing is an emerged technology used by the many consumers to store and share the data publicly where the security and privacy is the main concern. In this paper theoretical analysis of various kinds of security threats and various issues that affect the privacy preservation of the data users are analysed. Also the methodologies used to solve the security threats occurred in the real time cloud environment is discussed. The ways to solve the issues that are preventing the privacy preservation are also analysed. The detail explanation of these techniques is briefed and also summarizes the advantages with parameters of the different techniques in cloud computing environment. Various types of possible ways to overcome these issues are discussed and different types cryptographic mechanisms that are used to resolve the security threats are analysed. At the end of this survey, conclude that effective cryptographic mechanism is proposed to provide the effective prevention from the security attacks as well as better privacy preservation for the data owners and data consumers.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, N. Cao and Lou, W, “Toward secure and dependable storage services in cloud computing”, IEEE transactions on Services Computing, Vol. 5, No. 2, Pp. 220-232, 2012.

[2] S. Kamara and K.E. Lauter, “Cryptographic Cloud Storage”, Financial Cryptography Workshops, Vol. 6054, Pp. 136-149, 2010.

[3] H. Li, Y. Dai and B. Yang, “Identity-Based Cryptography for Cloud Security”, IACR Cryptology ePrint Archive, 2011.

[4] C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou and R.H. Deng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage”, IEEE transactions on parallel and distributed systems, Vol. 25, No. 2, Pp. 468-477, 2014.

[5] S.S. Chow, Y. Dodis, Y. Rouselakis and B. Waters, “Practical leakage-resilient identity-based encryption from simple assumptions”, Proceedings of the 17th ACM conference on Computer and communications security, Pp. 152-161, 2010.

[6] S. Ruj, M. Stojmenovic and A. Nayak, “Decentralized access control with anonymous authentication of data stored in clouds”, IEEE transactions on parallel and distributed systems, Vol. 25, No. 2, Pp. 384-394, 2014.

[7] B. Wang, B. Li and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud”, IEEE transactions on cloud computing, Vol. 2, No. 1, Pp. 43-56, 2014.

[8] B. Wang, B. Li and H. Li, “Panda: Public auditing for shared data with efficient user revocation in the cloud”, IEEE Transactions on services computing, Vol. 8, No. 1, Pp. 92-106, 2015.

[9] D.S. Wei, S. Murugesan, S.Y. Kuo, K. Naik and D. Krizanc, “Enhancing data integrity and privacy in the cloud: An agenda”, Computer, Vol. 46, No. 11, Pp. 87-90, 2013.

[10] J. Li, J. Li, X. Chen, C. Jia and W. Lou, “Identity-based encryption with outsourced revocation in cloud computing”, IEEE Transactions on computers, Vol. 64, No. 2, Pp. 425-437, 2015.

[11] Y. Zhu, G.J. Ahn, H. Hu, S.S. Yau, H.G. An and C.J. Hu, “Dynamic audit services for outsourced storages in clouds”, IEEE Transactions on Services Computing, Vol. 6, No. 2, Pp. 227-238, 2013.

[12] J.K. Liu, K. Liang, W. Susilo, J. Liu and Y. Xiang, “Two-factor data security protection mechanism for cloud storage system”, IEEE Transactions on Computers, Vol. 65, No. 6, Pp. 1992-2004, 2016.