Secure Access to the Data to be Stored on Cloud by Key Generation Using Multi Level Image Fusion for achieving Privacy of data

[1] A.V. Deorankar, [2] Tejaswini V. Deshmukh
[1]Assistant professor, [2]PG Scholar
[1] Department of Computer science and engineering,
[1]Government College of Engineering, Amravati, India.

Abstract: Data security has always been a major topic issue in cloud computing. In this environment, it becomes p serious because the data is placed at different places even. Data privacy and security protection are main factors of concerns about the cloud. Many techniques on have been studied in academics, data security is becoming important for the future development in cloud computing technology in every aspect. The issues related to data privacy and security is directly related to software and hardware in the architecture of cloud. Reviewing various security techniques and issues from both hardware and software view will help data protection in the cloud. Cloud computing is modifying the way many organizations are managing their data, because of its robustness. Privacy concerns come up whenever sensitive data is transferred on to the cloud. A simple method for protecting data privacy of data is to apply certain privacy techniques on data, and then uploading the modified data on cloud. The privacy methods used in existing research shows that privacy violation of data for cloud computing happens by external or internal attackers.

In proposed system such issues are solved using various privacy protection methods also this system has three models, which initially have zero trust among them. Multi-level image fusion technique is used for generating a strong and secure key that will be given by the transaction manager to the user whenever required. In this way proposed system will provide much better privacy and security of the data in cloud and provide a better secure access of data.

I. INTRODUCTION

Cloud computing is stated as a group of computers that are combined and used to provide different computations and tasks. Cloud computing is most important IT paradigms. One key benefit offered from this IT technology is reduced time and costs on the market for the companies. Cloud computing allows organizations to use shared storage and resources which is better than to develop and operate with their own infrastructure. Cloud computing also provides organizations to have a secure, flexible and cost-effective IT infrastructure. Data protection is one of the most important security aspects, because any of the organizations won't transfer their data to remote machines if there is no data protection guaranteed from the cloud service providers.

Authentication in cloud computing ensures that the proper person is getting access to the data from the cloud technology provider. When authentication is ensured in the cloud computing, it means that the user's identity is proved to the cloud service provider when accessing the stored information in the cloud.

This system allows secure access to the data provided on cloud. Here there are three models: first model consists of the cloud's architecture; the second model is based on the concept of transaction manager, the last model is the one concerned with the clients.

II. LITERATURE SURVEY

Kire Jakimoski et al. [1], Security Techniques for Data Protection in Cloud Computing, International Journal of Grid and Distributed Computing mentioned that Cloud computing has lot of issues related to security that are gaining a lot of attention, which includes network and virtualization security, data protection, application integrity, and identity management. Data protection is most important security issues because organizations will not transfer their data to devices if there is no guaranteed data protection from the cloud providers. Many techniques are suggested for protection of data stored in cloud in cloud computing.

Elham Abd Al Latif Al Badawi1 & Ahmed Kayed et al. [2], mentioned some of the security aspects that must be considered to achieve good cloud security

Physical security- The cloud's infrastructure including routers, storage devices, servers and other components must be physically secure and monitored.

Host security- Using host security techniques like to secure the operating system, to use malware protection and virus protection to implement web browser security.

Network security- Use network security techniques like, virtual private networks, firewalls, intrusion detection systems, network sniffers, secure routers etc.

Application security- Secure applications that are running on systems. Cloud providers must follow and support a secure development process.
Identity management- Authenticating and Identifying enterprise users using reliable methods and systems.
Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, et al. [3], in the "Basic concepts and taxonomy of dependable and secure computing," studied and mentioned that the meaning of security is plentiful. The intrinsic problems of data security and management in terms of control within cloud computing are conversed. Security is the fusion of confidentiality, obstruction of the unauthorized amendment, prevention of the unauthorized revealing of information or deletion of information, integrity and availability.
Z. Mahmood et al. [4] has mentioned one of major issues is with regarding to the security of data, in particular: data privacy, data availability, data protection, data transmission and data location. Consumers often don't always know the location of their data. Sometimes this does not even matter. For example, photographs uploaded to Facebook can dwell anywhere in the world and Facebook members or users are generally not concerned about the where it is stored. But when an enterprise has some sensitive data kept that is to be kept on a storage device in the Cloud, they may want to know the location of their data. They may also wish to specify a preferred location (e.g. data to be kept in the USA). This then requires contractual agreement to be done, between the customers and Cloud providers that data should be in a specific place or reside on known server. The problem here is that the customers aren't aware of the problems that can arise because of this and thus no such contract is agreed before. So, the cloud providers must sure to guarantee the protection/security of systems and the data and provide authentication to keep the customer's information under any circumstances.
Data Availability- BBC, Google users hit by mail blackout, BBC News, 24 February 2009 [5] stated Customer's data is normally stored in chunks on different servers residing on different Clouds or in different locations. In this situation, availability of uninterruptible data, data availability becomes an issue. Data availability is a decisive issue that is common for providers of Cloud to credit user accounts if system downtime duration falls below that specified in the Service level agreement.
Data Security- A valid question of security of data that is residing in Cloud is: how to ensure security of data. Although, the users now know the data location and there in no data mobility, there are still questions relating to its confidentiality. The obvious answer is that data should be in encrypted format.
Sun, G. Chang, L. Sun, and X. Wang et al. [6] emphasized the privacy issues, key security issues and trust issues into the existing cloud computing environment and also help the users to review the issues related to its usage. In accordance with the authors, in cloud computing there are three threats enlisted as privacy, security, and trust.
Privacy Issues- Privacy is ability of group or an individual to keep them apart and so reveal themselves selectively.
Trust Issues- It is acceptance that uses experience, to make reliable decisions. It is essential for making security mechanism in distributed computing environments; trust has soft security attributes as confidence, honesty, dependability, reliability, competence, trustfulness, security, belief. Trust is complex relationship admist entities because it is intensely subjective, uncertain, context-dependent, non-symmetric, and transitive.
A Pandey, A. K. Tiwari and R. M. Tugnayat et al. [7], proposed a data security framework for cloud computing networks. There are some patents about security techniques on data storage. They presented a framework of cloud security management which is built on aligning FISMA standard to be acceptable with cloud computing model. The framework improves cooperation between providers of cloud service and consumers in managing cloud security. It consists of three main layers: management layer, enforcement layer and feedback layer. Each layer is responsible for key security services. They created a proof answerable to concept of their framework using .NET and unfolded it on a tested cloud platform. By handling the multi-tenant security SaaS applications they examined the framework.
Data Integrity- In cloud system it means protecting information integrity. Data must not be altered by unauthorized users or should not be lost. Data integrity in cloud computing is the foundation that can provide services such as PaaS, IaaS, and SaaS. Besides large-scaled data storage, cloud computing environment provides data processing service. By using methods such as digital signature and RAID-like strategies, integrity of data can be obtained. Substantiating data integrity in cloud scarcely is the perquisite to deploy applications.
Bowers et al. proposed a theoretical framework "Proofs of Retrievability"[8] to actualize the remote integrity of data checking by bringing combining error correction code and spot-checking together.
J. Schiffman et al. [9]. Suggested trusted platform module to remotely check data integrity.
D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve et al. [10], stated Data confidentiality is important for users to store their private and confidential data in the cloud.
Craig Gentry et al. [11] proposed a method called fully homomorphic encryption, which can perform any operation that can be performed without decrypting in clear text. It is a breakthrough in the homomorphic encryption technology. But this encryption system involves complicated calculations and the price of storage and computing is very high. This tells that this system is still far from real applications.
D. Boneh et al. [12] a cryptographic algorithm named Diffie-Hellman was proposed for secure communication, which is not similar to the key distribution management mechanism.
A. Kaur and M. Bhardwaj et al. [13] in "Hybrid encryption for cloud database security proposed a hybrid technique that can combine many algorithms such as 3DES, RSA for enhanced security and more flexibility.
F. Pagano and D. Pagano et al. [14], in cloud environment that is untrusted, for the security of confidential data a technique called In-Memory Database encryption was proposed. A synchronizer is placed between the owner and the client for seeking access to data. Client would always require a key from the manager to decrypt the shared data that is encrypted, which it gets from the customer/sender/owner. The synchronizer stores the shared data and the keys separately. A disadvantage of this technique is that a delay occurs due to the communication with central synchronizer.

Michel et al. [15], this proposal provides security and privacy of data with keeping the available meanings Abstract. Nowadays enormous amounts of data is been generated from satellite imagery, experiments or simulations, access to such large amount of data becomes difficult for users who need to further process that data, existing data management method makes it difficult to efficiently access and share large data sets. This approach is to enable secure and easy collaboration based on authorization and authentication mechanisms, advanced group mechanism for flexible management of authorization and support for mapping sameness between local systems, as put into in ultimately accordant distributed file system which is called as Onedata.

Today, more and more research and commercial applications depend heavily on distributed access to large data sets, which includes data collected from physical experiments also data obtained through pure simulations or statistical data collected from web applications. Organizations using heterogeneous storage systems mainly create such data sets and often it gets difficult to completely transfer such long data sets between data centers for processing. These issues lead to several requirements that are important and necessary for a modern large scale distributed data management system, i.e. access to large data sets without transferring them completely to computational nodes, transparent data access from any machine, advanced group and role mechanisms for large group of collaborators, support for multi-tenant and single deployment, flexible metadata support allowing data discovery, protected and easy data sharing, support for open data publishing and data access using standard interfaces and protocols including Cloud Data Management Interface and POSIX. However existing data management platforms, are either focused on high performance access of data or for desktop users Dropbox like solutions, often have complex authorization and authentication mechanisms and are difficult to deploy by smaller communities.

Onedata uses OpenID and this OpenID connects standards to provide easiness and unified identity management. From user's point of view, it simplifies login and registration process as they can use one of their institutional or social accounts. The information minimum required is the email address that is served virtually by any OpenID provider. Users can associate more than one OpenID accounts to existing account in Onedata, which also gives them more login methods. Onezone acts as the account management center for users, where users can personalize their settings and also the authentication methods the other option available is to obtain client tokens to perform and authorize operations on their behalf across the whole system. Onezone is responsible for Identity management, which is center of authentication and authorization for all storage providers and users. Support for actual OpenID providers can be extended via plugins, which makes it easy to extend the range of providers or personalize the available authentication methods for every case of independent Onezone. Onedata supports basic login/password and then it is targeted at administrators of system. Upon registration, unique ID is given to the new user, which will be used universally in the system from nowonwards. Storing user identifiers acquired from OpenID providers, Onezone can map OpenID accounts onto the unique user ID easily. Later, when access to files is requested, for privilege verification this ID is used.

K. Sreekumar et al. [16] proposed a solution based on Geometric Data perturbation for privacy preservation of data. The proposal was to send data in a secure way by implementing the solution. This concept is based on storing data identified by key element and storing sensitive data in another location. Without re-assembling it from different storing locations the attacker cannot receive all data.

Maheshwari et al. [17] proposed a method to secure larger storage. The way to achieve this method is by "small secure storage for decryption keys.To secure a resizable amount of untrusted storage, TDB exploits a less amount of storage (trusted). Untrusted programs are not able read and/or modify the database because it is encrypted and then validated against a hash function that is placed in trusted storage and is called collision-resistant hash. TDB combines low-level data model with encryption and hashing, because it secures metadata and data, unlike the systems that are built atop of a conventional database system.

The implementation deprives cooperation between storage that is log-structured and hashing. Results of preliminary performance show that TDB performs better than embedded database system that is off-the-shelf, supporting suitability of TDB architecture. Trusted processing environment is provided by TDB and very less trusted storage space available on the platform. It provides privacy and security by encrypting data and in secret storage a key hidden.

III. PROPOSED METHODOLOG

This paper is based on a case study that is built on the basis of three models: the first model consists of the cloud's architecture, which involves all the transactions for the other models, the second model is consist of the transaction manager who will provide keys, manage the queries and grant users and the last model deals with the clients, the people that have the access to use data in the cloud. Additionally, this concept is based on assuming zero trust between the three models. This situation is because all transactions will be performed by third party and data movements through various levels of security. The tasks of the transaction manager can be listed as: user registration, revocation, system parameters generation and verifying the identity of data owners. The client's model is dynamic, as it is dependent on the kind of transactions to be performed and the type of data used.

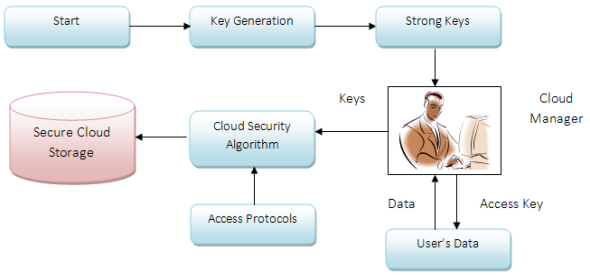

Figure 1: Architecture diagram

The above is the architecture diagram of the proposed system. The cloud/transaction manager here plays the important role of all. The new key generation method is used to generate more strong keys, the parameters of a strong must to be decided such that it must be not be easy to predict which can cause unwanted accessed of data stored on cloud. Multiple combinations of images are used to create a key, which will give a key that will definitely be unpredictable.

REFERENCES

[1] Kire Jakimoski, (2016), Security Techniques for Data Protection in Cloud Computing, International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016), pp.49-56.

[2] Elham Abd Al Latif Al Badawi1 & Ahmed Kayed, (2015), SURVEY ON ENHANCING THE DATA SECURITY OF THE CLOUD

[3] Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1,no. 1, pp. 11–33, 2004.

[4] Z. Mahmood, "Data location and security issues in cloud computing," in Proceedings of the 2nd International Conference on Emerging Intelligent Data andWeb Technologies (EIDWT '11) pp. 49–54, IEEE, September 2011.

[5] BBC, Google users hit by mail blackout, BBC News, 24 February 2009. [Online]. Available at http://news.bbc.co.uk/1/hi/technology/7907583.stm (Accessed: March 2011).

[6] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," in Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS '11), pp. 2852–2856, chn, August 2011.

[7] Pandey, R. M. Tugnayat, and A. K. Tiwari, "Data Security Framework for Cloud Computing Networks," International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178–181, 2013.

[8] D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in Proceedings of the ACM Workshop on Cloud Computing Security (CCSW'09), pp. 43–53, November 2009.

[9] Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel, "Seeding clouds with trust anchors," in Proceedings of the ACM workshop on Cloud computing security workshop (CCSW '10), pp. 43–46, ACM, October 2010.

[10] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal of Computer Applications, no. 5, pp. 11–14, 2012.

[11] C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University, 2009.

[12] D. Boneh, "The decision Diffie-Hellman problem," in Algorithmic Number Theory, vol. 1423, pp. 48–63, Springer, 1998.

[13] Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security," Journal of Engineering Science Technology, vol. 2, pp. 737–741, 2012.

[14] F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud," in Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (IWSSC '11), pp. 30–37, September 2011.

[15] Micha_l Wrzeszcz, _Lukasz Opio_la, Konrad Zemek, Bartosz Kryza, _Lukasz Dutka, Renata S_lota, and Jacek,(2017), International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland.

[16] Ram, C. P., and G. Sreenivaasan. "Security as a service (sass): Securing user data by coprocessor and distributing the data." In Trendz in Information Sciences & Computing (TISC), 2010, pp. 152-155. IEEE, 2010.

[17] U. Maheshwari, R. Vingralek, and W. Shapiro, "How to build a trusted database system on untrusted storage," in Proceedings of the 4th USENIX Symposium on Operating System Design and Implementation, Berkeley, CA, USA, 2000.