Available at: www.researchpublications.org

# Enhancing Data Security on Cloud by using Hybrid Approach

Ankush S. Narkhede[1], Alok k.Shukla[2]

[1] *Asst Professor, Department of Computer Engg., Padm.Dr.V.B.K.C.O.E., Malkapur, S.G.B.A.U. ,Maharashtra, India*

[2] *Asst. Professor, Department of Computer Engg, Padm.Dr.V.B.K.C.O.E., Malkapur, S.G.B.A.U. ,Maharashtra, India*

[1]ankushnarkhede1989@gmail.com

[2]alokjestshukla@gmail.com

***Abstract*** **— In this paper, we discuss on cloud based security and data sharing over internet, which has always been an important aspect of quality of service (QOS). "Cloud computing may be the only way to handle broad, unstable feedback query loads differentiated data in any number of formats and with any number of relationships" Data Security/information security is considered as critical issue in cloud spaces . In Data security, it can be implemented with respect to client authentication and authorization by cryptographically system. Information security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. As compare, Data security becomes more and more important in cloud computing. Cloud computing has been courage as the next-generation architecture of IT enterprise. As compare to traditional solutions given by the provider , where the IT services are under valid logical, physical and personal accessibility, cloud computing moves the application software and databases to the large data centre, where the management of the data and services may not be fully trust. This unique attribute, however, poses many new security challenges which have not been well understood. In this paper, I focus on secure data storage on cloud, which has always been an important aspect of quality of service (QOS). To ensure the secure storage of user's data on cloud, our propose research work on an effective and scalable and valid authentication using face detection verified by admin. "Data computing may be the only way to handle rapid, Cloud on data in any number of formats and with any number of relationships " Data Security is considered as major aspect in cloud system while using an application. Data security can be implemented with respect to user authentication and authorization using cryptography system. Data security involves encrypting and decrypting the original data as well as ensuring that appropriate policies are enforced for data sharing. In this paper, we will discuss data security on cloud as well as network environment**

***Keywords***— Security, Cloud, Encryption, Decryption etc.

## I. Introduction

In this research we will discuss on overview about how to provide cloud "Data computing is a compilation of present techniques and technologies, established within a new environment paradigm that offers improved scalability, adaptation, and business growth, faster start up time, reduced management costs, and just-in-time availability of resources". Cloud computing is a computing model, where resources such as calculation power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion.[1]

## II. LITERATURE SURVEY

Cloud is a computing model providing web-based application software, computing adequate resources on-demand, and capabilities of Information Technology (e.g. applications, storages, communication, virtualization, collaboration, and infrastructure). At derives cloud computing environments to the software that runs in virtual software that can be used to assemble applications in minimal time. Its service has ubiquitous access through a web browser or mobile device with APIs or special desktop applications developed by cloud service provider. Cloud computing now provides organizations with latest ways to arrange and maintain applications allowing for flexibility and decrease complexity. Fully understanding the range of potential cloud computing benefits requires a broad perspective that recognizes that real computing resource optimization aligns computing capabilities with business needs. In addition to new times organizations can now achieve adoptability, integration, scalability, deployment, enhance utilization, and transparent cost accounting. Cloud computing secure to increase the velocity with which applications are organized, increase innovation, and lower costs, all while increasing business agility.

## III. CORE CONCEPT OF SECURED IMPLEMENTATION OF CLOUD COMPUTING

Cloud computing system are create multi domain environment. Which different domain can use security, privacy and trust requirements in a different manner. So as far as cloud computing is newly idea developing, security has made commercial Internet possible. Cloud can be secured only when proper user authentication can be done. Till today many technologies had been used to provide user authentication [1].Different biometrics is used to provide security. It consists of three cloud including customer relationship management (CRM), storage cloud service and separate Encryption and decryption of data can be done to maintain data confidentiality. Beyond of all these things CRM play most important role. If user is authorized then only he can store or retrieve data from cloud database. We proposed that authentication can be provided by using exchange keys. The image is combination of pixels arranged according to fixed dimension. In this methodology, each pixel has equal importance. Password can be generated by arranging sequence

of pixel. After this overall process completes at that time, the encryption or decryption service must delete all encrypted and decrypted user data. In data storage and cryptography of user data works independently. This means that those working with data storage cloud system will have no access to encrypt/decrypt user data. we are just dividing and separating the encryption or decryption cloud service from the storage as service. Basic security and privacy in an organization, the concept of extract authority is forced in business management. If the person had decided to provide access to some of the operator of an organization to decrypt the data while some of them will work on storage service only. So, it's up to user for deciding the concept of extract the authority. Consider an example of motor service system organization, the user will supposed to divide the authority in the billing department as one of the factor named as, accountant operator and another factor is accountant. Due to this reason, the accountant is responsibility for keeping records and making billing of various Motors whee cal while cashier is responsible for making payment to the customer. So, by keeping the two sections separately the company prevents from fraud if an accountant makes any. Because as accountant has authority of making billing section only and not to provide payments to the customer and the employee. This example of division of authority is design to avoid the operational risk factor. In cloud computing environment the user ties to uses effective and efficient services provided by the cloud with some of specific function. Data generated while using these services is then stored on the storage cloud service. This study related to the business model provides division as per the responsibility for data storages and data encryption or decryption. In cloud computing, Customer relationship management application can be replaced with some other services ex.ERP cloud service, account software cloud services etc. In this manner these three clouds can put separately for insuring security. The interesting point is that the SaaS, PaaS provider the dose not stored the unencrypted user data.[6,7] This ensure security and privacy to the user and reduces discloses of the data. Because when the user requests for encrypt or decrypt of the data to the encryption or decryption as service, and when all this process conversion completes and then handled it CRM application. After this overall process completes at that time, the encryption or decryption service must delete all encrypted and decrypted user data. In addition to this, data storage and decryption of user data works independently. This means that those working with data storage cloud system will have no access to decrypted user data. In short here we are just dividing and separating the encryption or decryption cloud service from the storage as service. For enhancing the security and privacy in an organization, the concept of dividing authority is applied in business management. If the user had decided to provide access to some of the operator of an organization to decrypt the data while some of them will work on storage service only. So, it's up to user for deciding the concept of dividing the authority. A. Access to data for data retrieval system Data retrieval system consists of following steps: To access data from cloud database, user authentication is must. So firstly authentication of user can be done. This identity plays unique role during data retrieval system. Then CRM sends request to data storage, where user data is present in encrypted form. Decryption of required data takes place to fulfil the user requirement because user cannot read data in encrypted format. B. Easily access to data for data storage system the data storage system method is exactly opposite to the data retrieval. Here this process is also conducted in three main steps. To store data in cloud database, user verification is must. Until and unless user verification is confirmed the CRM cloud service will not proceed further. After successfully login the user will firstly send the request for storing data to be stored to the CRM system. Then CRM will forward the user request to the Encryption and Decryption cloud services. Presently data is in decrypted form an we will encrypt using algorithm. Encryption and decryption cloud services, enhance of decrypted data gets into encrypted form takes place in the networks the user authentication is very important while encrypting or decrypting the data as there are multiple users accessing the service. The encryption and decryption cloud service had no authority to store the data either in the encrypted form or decrypted form on the same cloud service. Cloud automatically modifies the data after sending it to its proper designation. So we will increase the data security on cloud system. After data send to the Storage Cloud Service, here the data is stored in the encrypted form along with the user Id. This will help in future to identify and differentiate the data of multiple users.

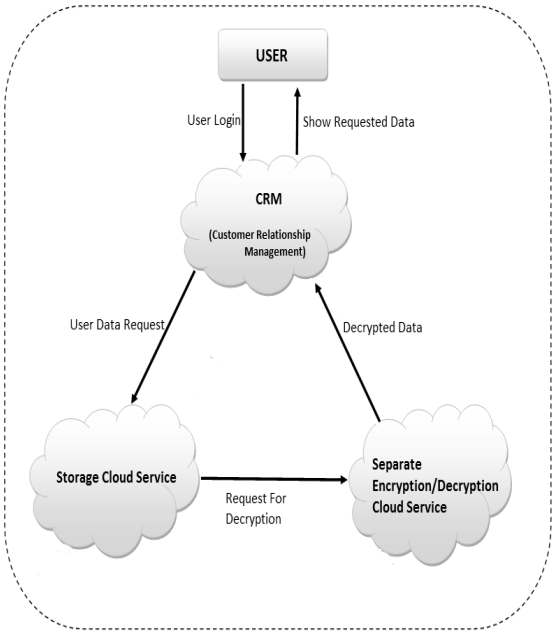


Fig: User Data Retrieval Diagram

Finally Storage Cloud Service Provider will send request to user that the data is stored in the encrypted form and then

decrypt on cloud. After sending confirmed request of data stored in the encrypted form to user then only the encryption and decryption Cloud data will delete the data which is stored there as on originate process for encrypting or decrypting data for completing the data storage process will delete the data. That reason would help in reduce the risk factor on data cloud of getting data hacked due to some unauthorized persons. Thus the data storage process is completed successfully. CRM business model encryption or decryption as service and storage as service are not provided by a single client. The interesting point is that the SaaS provider the dose not stored the unencrypted user data. This ensure security and privacy to the user and reduces discloses of the data. Because when the user requests for encrypt or decrypt of the data to the encryption or decryption as service, and when all this process conversion completes and then handled it CRM application. [2] After this overall process completes at that time, the encryption or decryption service must delete all encrypted and decrypted user data. In addition to this, data storage and decryption of user data works independently. This means that those working with data storage cloud system will have no access to decrypted user data. In short here we are just dividing and separating the encryption or decryption cloud service from the storage as service. For enhancing the security and privacy in an organization, the concept of dividing authority is applied in business management. If the user had decided to provide access to some of the operator of an organization to decrypt the data while some of them will work on storage service only. So, it's up to user for deciding the concept of dividing the authority. Consider and example of motor garage system organization. The user will supposed to divide the authority in the billing department as one of the factors named as, accountant operator and another factor is cashier. Due to this, the accountant is responsible for keeping records and making billing of various Motors. So, by keeping the two sectors separately the company prevents from given false query if an accountant makes any. Because as accountant has authority of making billing section only and not to provide payments to the customer and the employee. [2, 3]. These examples of division of authority are design to avoid the of the exceptional errors. In data computing environment the user ties to uses effective and efficient services provided by the cloud with some of specific function. Data generated while using these services is then stored on the storage cloud service. In this related to the business model provides division as per the responsibility for data storages and data encryption or decryption. The concept of separate encryption and decryption consider the example of CRM cloud service, storage and encryption or decryption.

**3.1 Appropriate access to data for data retrieval system**

As shown in the figure, these architecture required collaboration of tree cloud namely separate encryption or decryption, storage service and data service. Here we have clear at CRM an example of the latest business model. Before working process implement, the user authentication is verified by the administrator until user verification completed this architecture mandate that the user must to do validate login registration and contact with the CRM cloud service? For this user's access authorization process, we can use e-commerce or other services which have capabilities of securely verified the user registration, such as reply login verification, one time password etc. Using authentication of the clients and satisfaction of any criteria set out in the access delegation, and then only CRM service system accepts any kind of request feedback the user. After the user logs into the CRM system, is the CRM receive request for client information, it will execute a data Retrieval program. In the data retrieval system, one the user logging has been successfully verified by the admin, the CRM will access the user request for the data retrieval and modify. Every user associated to an organization has its own user ID for verification. This entity helps to know about the user data in the storage cloud system. The CRM will precede the user request to the storage service system, where user data are stored in to the encrypted form. So these data is not readable by the user.[2]

**3.2 Appropriate access to data for data storage system**

The data storage system methodology is exactly opposite to the data retrieval. The process of data storing is carried out in three main steps. Firstly the user will do login. Then after user authentication is done for verification purpose. This process has carried out under CRM cloud structure. After authentication, user will send request for accessing data present inside cloud storage database. Before storing things in database, user id, password, request etc has to be encrypted and decrypted many times. Only authorized users can store data inside cloud database. Cloud will automatically delete temporary data so that data integrity and security can be achieved. As authentication and authorization both are needed, chance for data to be hacked got reduced.

## IV. PROPOSED METHODOLOGY OF PGP FRAMEWORK OF ENSURING SECURITY

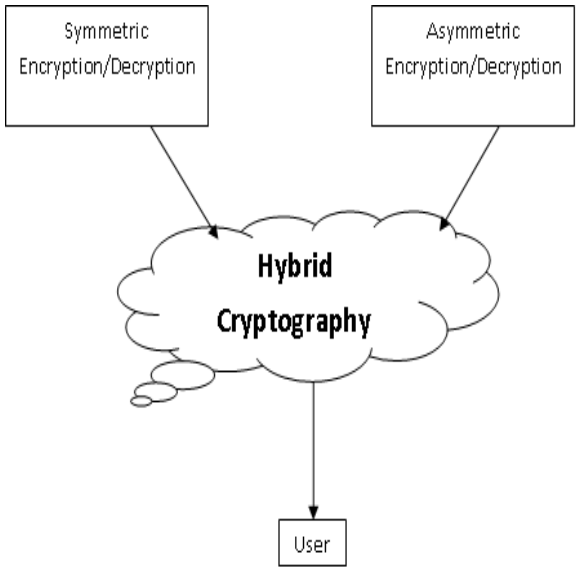


Fig: - Implementation of hybrid cryptography to secure cloud

Cloud computing environment are multidomain environment. Different domain can use security, privacy and trust requirements in a various manner. As it is provided as commercial service, developing security is must at all levels of hierarchy. So there are various techniques of providing security to cloud on various levels.

Cryptographic protocols such as Secure Socket Layer (SSL) are used for securing data and encryption purpose. The concept of Open Pretty Good Privacy (PGP) is also used for developing cryptographic privacy and authentication. It is a computer program which developers uses for combining different widely algorithms for ensuring security and privacy into a secure system. Symmetric algorithm and asymmetric algorithm provides different ways of encryption and decryption.

These two algorithms provide security by encrypting and decrypting text to strengthen the access. Also various biometric and text based password techniques are develop for providing authorization and authentication. We tried to combine these two types of encryption and decryption technique so that level of security should be increased. In symmetric algorithms, the same key is used for encrypting and decrypting the data. That is why symmetric algorithm is fast processing algorithm. But Asymmetric Encryption is better than symmetric encryption for performing encryption of the data and it simplifies key management. Comparatively it is slower than symmetric encryption. So we combine both Symmetric and asymmetric technique to form hybrid approach. It gives us improvement in providing much stronger security. Data in the cloud can be protected separately with symmetric key and those keys will be managed through asymmetric key.

## V. CONCLUSIONS AND FUTURE WORK

The security of data is maintained by providing authentication and authorization to user at very first level. It improves level of accuracy which leads to increase security. To ensure the correctness of user's data in cloud data storage, we proposed effective and flexible methods of hybrid cryptography. We believe that data storage security in Cloud Computing, an area full of challenges and of immense importance, is still lagging now, and many research problems are yet to be identified. This becomes too slow for login as we are using both cryptographic techniques. So in future we will try for reducing login time by directly encrypting keys used. This can be implemented with more security by using strong biometric measures like eye. There are several security challenges including security aspects. There believes that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. So security issues for cloud are important. These issues include storage security, data security, network security and application security. The main goal is to securely store and manage data that is not controlled by the owner of the data. Then there is focused on specific aspects of cloud computing. This kind of structured security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computation concept for industrial as well as future research farms.

## VI. REFERENCES

[1] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni. Cloud Security is not (just) Virtualization Security, CCSW'09, Nov. 13, 2009, Chicago, Illinois, USA.

[2] L. Litty and D. Lie. Manitou: a layer-below approach to fighting malware. In ASID '06: Proc. of the 1st workshop on Achitectural and system support for improving gsoftware dependability, pages 6-11, New York, NY, USA, 2006. ACM.

[3] B.D. Payne, M. Carbone, M. Sharif, and W. Lee. Lares: An architecture for secure active monitoring using virtualization. Security and Privacy, IEEE Symposium on, 0:233-247, 2008..

[4] M. A. Rahaman, A. Schaad, and M. Rits. Towards secure SOAP message exchange in a SOA. In SWS '06: Proceedings of the 3rd ACM workshop on Secure Web Services, pages 77–84, New York, NY, USA, 2006. ACM Press.

[5] Meiko Jenson, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono. On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing 2009. [8] D. Kormann and A. Rubin, ―Risks of the passport single sign on protocol, Computer Networks, vol. 33, no. 1–6, pp. 51–58, 2000.

[6] V.Vijay Kumara and N. Suriyanarayanan, Performance Measure of Local Operators in Fingerprint Detection", Academic Open Internet Journal, vol. 23, pp. 1-7, (2008).

[7] Schneier.B, "The uses and abuses of biometrics". Communications of the ACM, August 1999 .

[8] M. A. Rahaman, A. Schaad, and M. Rits. Towards secure SOAP message exchange in a SOA. In SWS '06: Proceedings of the 3rd ACM workshop on Secure Web Services, pages 77–84, New York, NY, USA, 2006. ACM Press

`