IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Orthogonal handshaking authentication mechanism (OHSAM)

[1]Dr.M.Mohamed Sirajudeen and [2]M.Fathima

[#1] Dean –PG and R&D, Department of Computer Science, Nilgiri College of Arts and Science, Thaloor, The Nilgiri District

[#2] Research Associate, Global Tree Educational and Research Academy, ILayangudi, Sivagangai District

Abstract: *Organizations are moving sensitive and regulated data into the cloud by which access the data is kept secure. Data can take many forms. For example, the cloud based application development includes the application programs, scripts, and configuration settings, along with the development tools. For deployed applications includes record and other content created or used by the cloud applications. The access controls are to keep data away from unauthorized users; encryption is another method to protect data from unauthorized access. The access controls are typically identity-based, which makes authentication of the user's identity an important issue in cloud computing. The "Data-Base" environments are used in cloud computing can vary significantly. For example, some environments are supporting a multi-instance model, while others supporting a multi-tenant model. In our research work propose a new approach named as "Orthogonal handshaking authentication mechanism (OHSAM)" in order to secure the cloud data storage in effective as well as efficient manner.*

Key words: *Authentication, Secure, Data store and Orthogonal.*

I. INTRODUCTION

The former provide a unique database management system running on a virtual machine instance for each cloud subscriber, giving the subscriber complete control over role definition, user authorization, and other administrative tasks related to security. The latter provide a predefined environment for the cloud subscriber that is shared with other tenants, typically through tagging data with a subscriber identifier. The "Cloud Computing" meets unique constraints with minimum overheads for individual clients to fulfil their on-demand needs for Data Storage and Computing Resources. It also trims down the burden of handling and maintaining own resources with more investments whether its usage is frequently or occasionally. Right now, it is not necessary for every organization has the possession of its own resources related with utilizations. The advent of "Cloud Computing" plays a vital role in resource sharing mechanism and makes more sophistication for many industrial sectors to conduct a secure data transmission with certain limitations.

The major objective of cloud computing is to avoid high-level investments are in the establishment in data storage and transactions between different industrial /institutional /organizational branches. The clouds are being used by the organizations and personals for the management or storage of their accounts, finances, software source codes and various types of other data. The security of the data is very important. During the periods when the Cloud nodes are in working condition, they need secure cryptographic keys for secure propagation of the sensitive information.

The operational environment behind in the cloud computing mechanism is to create a resource virtualization pool of other service utilizations such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS).

The "Cloud Service Providers" are in the market such as Amazon Web Services (AWS), Verizon Cloud (VC) and Digital Ocean Cloud (DOC) offers infrastructures, platforms as well as software's for services. The incredible growth of IT industries are making easier for data transaction in and around any geographical area. One of the fastest developing sectors within this boundary is health care domain. In the field of healthcare, files handling by various multi-speciality hospitals situate at different places under same network requires a great dealing of centralized service provider. At present, the data transactions are conducting by their own infrastructure with additional overhead cost either it may be profitable or non-profitable organizations.

The service sectors (for example Education, Healthcare or any other community welfare organizations) are really getting hold of more benefits from cloud computing mechanism. The migration of data among different cloud servers are managing as well as maintaining by service providers with additional resources such as dedicated cable, server storage likewise. The cloud computing donates its spacious services in the direction towards effective resource utilization among vendors.

Users should be aware of the potential downsides to the cloud-based storage. These include issues of portability or vendor lock-in, regulatory compliance issues, and the availability of cloud-based storage when one vendor's solution is unique in architecture or "Application Programming Interfaces (API)".

The data and its relevant information's are intended for a particular vendor is transferred from their domain server into the cloud server. In order to perform a secure data transaction among different clients, before transferring content it undergone for crypto mechanism. By using existing cryptographic algorithms or proposed a new security algorithm this kind of security measures are ensuring with linked transactions.

The proposed "Orthogonal Hand Shaking Authentication Mechanism (OHSAM)" functional environment for Centralized Cloud Data Server (CDS) is designed to select its successive service providing servers in an Orthogonality principle (i.e. the server located perpendicular with each other). Every existing cryptographic algorithm in the cloud computing security issues are always maintain encryption key and its data content in same server . On the other hand, this proposed "OHSAM" mechanism implies the key for encrypted content and data take place a separate storage location in its physical nature is perpendicular with each other.

II. Related Work

The security features in cloud data storage services are eventually promoting an emergence of resource sharing services from centralized Cloud Service Providers (CSP)". In this critical environment, the service approval must require to get an authentication from "Data owners" in a private cloud access. It means that, the cloud users after being successfully validated should request and access those resources as well as services for which one get an authorization in a particular security algorithm. In some situations, the user identity (Only using registration ID, but not using cryptographic algorithms) information is also considered for performing a resource sharing mechanism under private cloud data storage.

Justus.B et al, proposed a privacy stabilizing architecture for database storage. This architecture prevents the outsourced cloud data from both internal and the external attacks. The main elements of architecture are user engine, user interface, rule engine and cloud database. Database is accessed by sending a request through the user interface to user engine, rule engine and finally to cloud database. The privacy is preserved by encrypting data and conveying protected identities for request and its response in all stages. Machine readable access practice rights are also maintained in it.

In every moment, the current industry is Vishal Paranjape et al [37], the authentication requirement after receiving the request from cloud client or any other access required source is confirmed with the help of "One Time Password (OTP)". The appropriate authenticated users are get approval for receiving "OTP" in a successful manner. The services between cloud storage and cloud service clients are activated afterwards linked with password confirmation. Most of the cloud security algorithms are evaluated based on "Time Complexity and Space Complexity" evaluation Function.

C.C.Chang et al, the stored content on third party network is always bringing a question for security. It must required authentication between service provider and service consumer. At the same moment, each and every service provider acquire the responsibility of secure the clients data on cloud storage by using sparse matrix.

Based on the client request, the request data is retrieved from a cloud database by using an authentication mechanism. The input characters for encryption /decryption progress are usually in plain text and cipher text in the crypto mechanism for almost in all applications.

The way to implement a Sparse Data Compression Algorithm (SDCA) is a modern approach to integrate with compressed data in crypto algorithms. The problem statement of this research work is focus on compression for the input values and the compressed values are applied for encryption in order to secure existing data in cloud servers. There are many number of cloud service vendors among them, only few listed here in the computing market such as Amazon web cloud services, Verizon Cloud and Digital Ocean Services. . Each and every cloud service provider vendors offers secure cloud services for users in its description of symmetric and asymmetric crypto mechanism [1][2].

The data for the transmission is used for the encryption by using any one of the crypto algorithm. C.C.Chang et al, the deterministic encryption scheme (as opposed to a probabilistic encryption scheme) is a cryptosystem which always produces same cipher text for a given input file. The Cloud Encryption Component is shown by the following Figure 1,

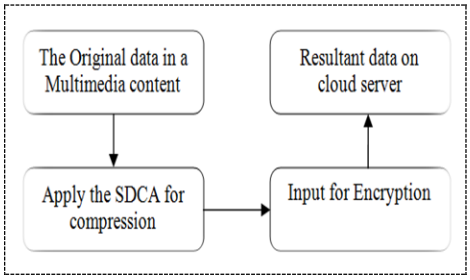

Figure 1 Cloud Encryption Components

The "Cloud storage" services have grown and diversified significantly this development eventually promotes an emergence of agreement services with feature of allowing users to choose the one that is more suitable for him/her. Services are provided in a common environment by centralized cloud storage facilities. Whenever to go for the analysis of huge volume of data, a standard encrypted or decrypted mechanism increase the time and space complexity[3][4][5]

This "SDCA" provides an " secure and efficient transmission and storage of multimedia content in public cloud environments using joint compression and encryption". From the above Figure 9, the components are in order to prevent the unauthorized data access from the cloud storage management by third party.

The "Sparse Data Compression algorithm" integrates with any one of existing crypto-mechanism. The basic principle behind this algorithm is based on the "sparse matrix representation". If the storage is required 3X3 =9 for accommodate given values on server storage .The entries for position (1,1),(1,2),(1,3), (2,2),(3,1),(3,2),(3,3) contains the value "0" .

M. Omer Mushtaq et al, the "Auditing Algorithm Shell (AAS)" is also an approach for achieving secure cloud data storage as well as ensuring authenticated data transaction under cloud environment. The working principle behind this is; the input for process will start from given data set and generate additional data bits (fake). The additional bit is attached with original content (i.e. Encrypted Text is the combination of both fake bits and original bit). The encrypted content in this manner is transfer to the cloud data storage.

Ankita Nandgaonkar et al, the working principle of Matrix Encryption Algorithm (MEA) is describing a secure data communication among cloud users. The following steps are clearly depicted its functional environment in cloud computing mechanism. They are: the initial step is describes, to calculate number of characters including blank space in the original content up to End Of Sentence (EOS). Thereafter to make, the conversion for this contents with equivalent ASCII code. Afterwards, create a matrix format. Then apply the appropriate converted ASCII code values in the matrix format from left hand side to right hand side.

Then, the matrix format is partitioned into three parts such as upper, Lower and diagonal part for further process. To perform reading the matrix from right to left formulation. Each matrix uses three different key K=K1, K2, K3 for encryption. Do the encryption. Afterwards to apply the encrypted values were in the same format. Thereafter, read the content by column wise. The decryption is performed just reverse as encryption process to repeat it [6][7].

Prakash G.L et al , the "Procedure Block_Authetication Algorithm (PBAA)" mechsnaim of ensuring authentication in order to makes a secure data transfer among the cloud clients with the help of frame. Cloud data storage content and its encryption mechanism is performed mapping for required service with the help of table named as "Block Sequential Allocation Table (BSAT)" for conducting secure cloud data storage.

III. Proposed Architecture

The Encryption Content and Encryption key are stored in two different servers by using an orthogonal mechanism generating "encryption key" for plain text is in the "Orthogonal Positions" in order to secure data during its transmission over internet. The remaining bit values of plain text simply considering into row-wise for encrypting content. The decryption process is performed in the way to get an "Encryption-key" from cloud storage and decrypt the original text just a reverse manner. It will explain clearly in the forthcoming chapter named as "Key distribution and Orthogonal Decryption".

The encrypted file storage and retrieval to or from the cloud servers is performing with a help of "Orthogonal Hand Shaking Authentication Algorithm (OHSAA)". The working principle behind this authentication is a "Hand Shaking" procedure applied in the orthogonal based encryption file in cloud data storage. It is ensure the authenticated users by using registration identification and fetch related files from cloud data storage with the help of "Orthogonal Block Allocation Table (OBAT)". The encrypted content and its key storage are split into two different cloud servers from main Cloud Service Provider (CSP) in the existing cloud computing environment. The proposed work includes the following working Steps;

- Registration in the cloud service providers (CSP)
- Orthogonal Key generation algorithm (OKGA) and Orthogonal Encryption Algorithm (OEA)
- Cloud Storage Allocation
- Orthogonal Hand Shaking Authentication Algorithm (OHSAA)
- Key distribution and Orthogonal Decryption Algorithm (ODA)
- Retrieval or Response

The following diagram depicts, in Figure 10, is fundamental components of "Orthogonal Hand Shaking Authentication mechanism (OHSAM)".

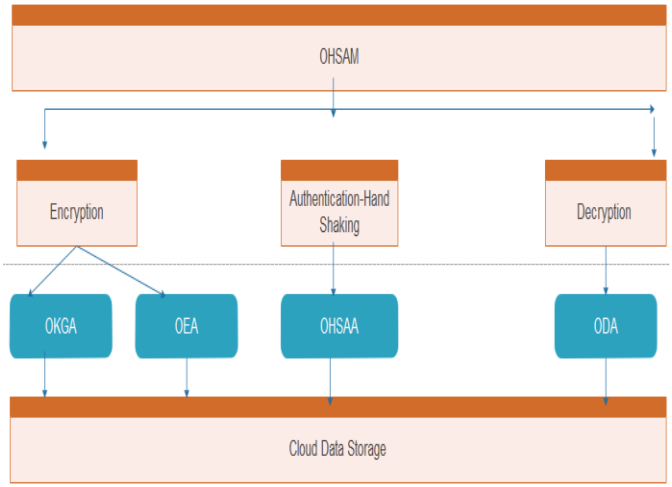

Figure 2 Proposed frameworks for OHSAM

Figure 2, depicts the process like Encryption, Authentication, Decryption and Cloud Storage. The functional unit of encryption is performed in this proposed work as "Orthogonal Key Generation Algorithm (OKGA) and Orthogonal Encryption Algorithm (OEA)". All the components are explained in a detailed manner by using a heath care domain data set from different cloud service providers such as: Amazon Web Servers (AWS), Verizon Cloud (VC) and Digital Ocean Cloud (DOC). The implementation design for user interface of proposed work "OHSAM" is shows in the following Figure 3, along with the above specified components in addition the field of "Upload file". It is point out the selected input file for performing "OHSAM".

Figure 3 User interface for OHSAM

The registration procedure having one more mandatory filed is giving a hint for securing the file access from cloud servers. This secure hint is limited by only four letter alphabets. In other security algorithms, it is used as "string" for validating authorized users. But in this proposed mechanism, it is used as numeric value and considering as 2x2 matrix representation. Then the diagonal values are called as "Orthogonal hint value (OHV)", it send for a verification at the time of service request arises from cloud clients during authentication. Based on the response provides an authentication status is accepted or rejected to the requesting user.

The encryption key is generated for given plain text by using proposed "Orthogonal Key Generation Algorithm (OKGA)".The working principle of the proposed algorithm is, initially create a logical view of storage matrix for selected input file (Eg. Create an 8x8 matrix for Text1.docx) after perform a client

registration in cloud computing secure storage environment. Thereafter, to represent equivalent binary value of alphabets from input file considering in Orthogonality make an encryption key. The remaining bit positioning values are grouped into encrypted text by using Orthogonal Encryption Algorithm (OEA). Then, divided Encryption Message (M_E) and Encryption Key (E_K) is separately in order to store the cloud server's located perpendicular with each other. At the same moment, Key for the encrypted text is stored along with the reference links into cloud the service.

The design of any cloud service architecture is permit users to use virtual machines of different configurations as per cloud environment client's requirement. The data storage of cloud service providers are creating a group within the organization or institution in order to perform secure data by using simple authentication mechanism such as matching with user name and password without any crypto algorithms as well as specialized storage selection procedures. The cloud data storage includes stringent requirements for Data confidentiality, Data integrity, Data availability, Key distribution and Authentication. Interoperability is a key requirement that has been a chronic barrier in the healthcare delivery improvement. Cloud computing is mostly used because it provides much storage space to its user, so it becomes necessary to provide security to that data. There are many security algorithms, but security of all these algorithms can be broken by anyone.

It has a link with Data Owner's description about the utilization of linked records. Once the data getting ready for transferring towards cloud server, the encrypted key is considered as a handshaking filed to ensure appropriate user. Therefore, a conversation is initiated by the cloud service provider in order to find matching encryption key. If the key resides in "Cloud Server-Memory Blocks" and issued by Service Requested client is "equal", then only resource sharing or any other access on the stored content is open for transaction between them. It means, if the authentication progress phase becomes successful is help to open the gateway for cloud data encryption.

Healthcare entities need to establish strong cloud service agreements with detailed provisions for different cloud service providers such as Amazon Web Services (AWS), Verizon Cloud (VC) and Digital Ocean Cloud (DOC) relating to security and privacy in order to fully understand their liabilities and risks as well as being able to absorb those risks in the event of non-compliance. So it is very necessary to make security of cloud more strong. The following Unified Modeling Diagram (Figure 4) clearly describes an authentication process taken place with the help of OHSAA. Let us consider one of the registered cloud users or client required a reference for existing its parental records in the Cloud Server accessed with an attributes Session Identifier(Session_ID, Service Description _SD, Service type).

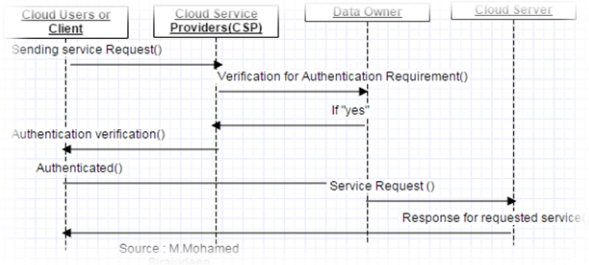

Figure 4 Orthogonal Hand Shaking Authentication

The authentication is ensuring appropriate user's identity, and then relevant key is distributed regarding to retrieve data from cloud storage. The cloud client is going to utilize existing content from the cloud servers with the help of Key distribution and Orthogonal Decryption Algorithm (ODA).The designing principle of ODA comprising following steps;

- Ensure the authentication for appropriate user is an authorized client.
- Fetch related file from the Centralized Cloud Server along with its encrypted content.
- Substitute the distributed key values in diagonal positions from left to right, thereafter fill the left out positions as per header description layout.
- Grouping the binary bit values into 4 bit position from left to right.
- Convert binary into ASCII values, thereafter derives its equivalent numeric values and English alphabets.

IV. Conclusion

In this research paper discussed about the fundamental principles were behind the architectural design of OHSAM comprising the mechanism of registration, design of OKGA, Key Distribution, OEA and ODA. In this approach, the Orthogonality principle plays an important role for service provider's selection and perform a secure cloud data communication the cloud service providers. The design of Cloud Storage allocation also discussed followed by an exposition of the Orthogonal Hand Shaking Authentication Algorithm. The challenges facing the security of data on cloud storage and the ways to mitigate them are proposed through OHSAM. In the continuation of this work will perform a comparison with proposed architecture versus existing one.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Liu, "Techniques for data hiding," in Proceedings of SPIE , 1995, pp. 2420-2440. [13] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamo on, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing , vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE . Sp ecial Issue on Protection of Multimedia Content, vol. 87, no. 7, pp. 1079-1107, July 1999.419

[3] M. D. Swanson, M. Koyabashi, and A. H. Tewfik, "Multimedia data embedding and watermarking strategies," Proceedings of the IEEE , vol. 86, no. 6, pp. 1064-1087, June 1998.

[4] R. B. Wolfgang, C. I. Po dilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," Proceedings of the IEEE . Sp ecial Issue on Protection of Multi- media Content, vol. 87, no. 7, pp. 1108-1126, July 1999.

[5] M. Bellare, A. Boldyreva, and A. O'Neill. Deterministic and efficiently searchable encryption. In CRYPTO, 2007.

[6] B. Berger and P. W. Shor. Approximation alogorithms for the maximum acyclic subgraph problem. SODA, 1990.

[7] A. Boldyreva,N. Chenette, Y. Lee, and A. O'Neill. Order-preserving symmetricencryption. In EUROCRYPT, 2009.