Asian Journal of Science and Applied Technology
ISSN: 2249-0698 Vol. 7 No. 2, 2018, pp.1-8

Performance Evaluations for Orthogonal Handshaking Authentication Mechanism (OHASM) in Secure Cloud Storage

M.Mohamed Sirajudeen[1]and K. Subramanian[2]
[1]Department of Computer Science, J.J. College of Arts and Science, Pudukottai, Tamil Nadu, India
[2]Department of Computer Science, H.H. Raja's College, Pudukottai, Tamil Nadu, India
E-Mail: mdsirajudeen1@gmail.com, subjjcit@gmail.com

***Abstract* - In general, the cloud computing contributes its wide services in effective resource utilization among vendors. To share the resources such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) in a secure channel is carried out by using different cryptographic algorithms. The demand created by IT industry provides a road map in a potential way for sharing cloud storage with variety of secure mechanism. Secure storage or security in cloud storage characterizes the convergence of the approaches in four categories: method of storage, crypto graphic algorithms, key distribution and authentication. When considering privacy risks in the cloud, as considered already within the introduction, context is very important as privacy threats differ according to the type of cloud scenario. The concepts related with secure cloud data transaction is make use of different emerging trends in real time applications such as financial transactions, medical records maintenances in health care sectors like wise. The largest part of healthcare entities is required to establish strong cloud service applications with elaborated provisions 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. In this research work focus a way to secure cloud data storage in transaction aspect with healthcare domain. Each and every cloud security mechanism with healthcare record maintenances is using a variety of cryptographic algorithms. Almost it describes the encrypted documents are reside in a single cloud server along with its encrypted key. This work propose a method of such secure mechanism by using Orthogonal Handshaking Authentication Mechanism (OHSAM) with a working principle of separate storage for encrypted content and its key in a cloud server.**

Keywords: **Secure, Storage, Data, Orthogonal and Authentication**

I. INTRODUCTION

In general the healthcare entities includes medical records are highly sensitive issues while resides in cloud server providers (CSP). The data owner either individual or an organization tried their level best in order to protect its transaction over the communication channel with the help of cryptographic mechanism. Most of the approaches are always discussed few of existing symmetric or asymmetric cryptographic algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) or RSA (Rivest, Shamir and Aldimir) algorithms in order to provide secure cloud storage [4].

Whenever applies such kind of more standard algorithms, it may creates the resource sharing environments are more complex [for example, size of encrypt bits, cost for implementation] as well as to increases response time in the name of secure cloud environment. Along with thissome common attempt such as AuditingAlgorithm Shell (AAS) [6], Matrix Encryption Algorithm (MEA) [2] and Procedure Block_Authetication Algorithm (PBAA) proposed a simple encryption, decryption along with authentication mechsnaim in order to protect the healthcare records reside in Cloud Service Providers [Figure 1].

The healthcare related records reside at cloud server or cloud service provider (CS_N) is in form of encrypted text along with its key (A_K). The requisition from client access (figure 1) either may be an individual or group get authorization (in the aspect of Software as a Service –SaaS) with the help of key exchange.

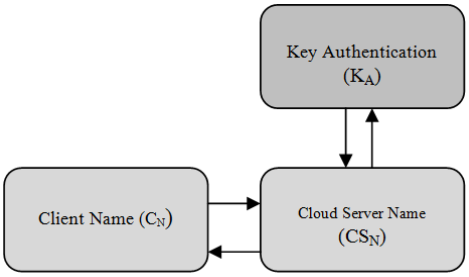


Fig. 1 Key Authentication

In this mechanism, the encrypted content and its authentication purpose encrypted key is available at same cloud server. The same thing is in the real time environment for cloud data authenticated access illustrated by the following figure 2. Initiated the access request from client get a permission to store the encrypted data in cloud server or cloud service provider is carried out with the help of token.

In private cloud, the service providers are always ensure themselves a secure data storage management or service allocation for the clients by using any kind of authentication mechanism. Anyhow, there will be numerous possibilities for intruders attack on the data transaction by the third party agents/intruders over the internet [4].

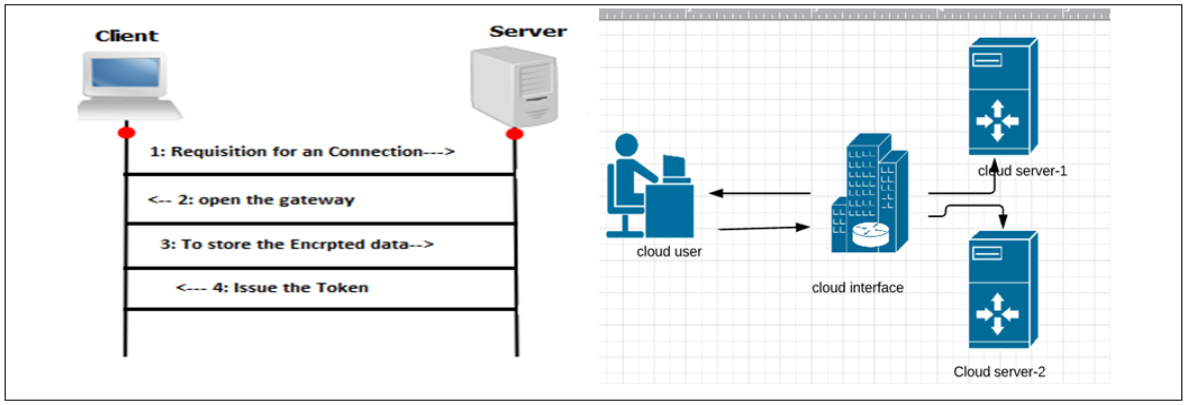


Fig. 2 Real time environments for Key Authentication

Healthcare data management includes stringent requirements for security, confidentiality, privacy, traceability of access, reversibility of data, and long-term preservation. Hence, cloud service providers must address all of these legal, regulatory and accreditation requirements. Interoperability is a key requirement that has been a chronic impediment to healthcare delivery improvement. IT approaches such as the use of cloud-based enterprise service bus (ESB) software with electronic healthcare record (EHR) connectors can help overcome this barrier. Organizational healthcare providers (predominantly physicians in private practice and general hospitals, respectively) conduct the business of healthcare according to standards and practices that may vary significantly. Standards of care differ by specialty and pathology, clinical care and treatment practices vary with provider experience and locale, and best practices for optimal case outcomes without risk of increased patient morbidity or mortality remain elusive. 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. So it is very necessary to make security of cloud more strong [5].

Healthcare entities need to establish strong cloud service agreements with detailed provisions 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. Healthcare entities must stay informed of where and how electronic protected health information is moved, handled, or stored by their CSP. For example, if a CSP moves data to another country, it may be subject to international laws and therefore non-compliant with government regulations. Additional physical security controls may be necessary for the healthcare entity and background screenings may be required for those CSP varying forms of user authentication and authorization. It is important for the healthcare entities to be able to track the creation, modification and deletion, when it is stored and processed by a cloud service.

The most successful mitigation method is the provision of location and time independent, collaborative, consistent and real-time cognitive support which only cloud-based information technology can provide. Such IT capabilities as enterprise service bus for vendor-provider-specific EHR connectivity and data communication; intelligent business process management suites for process automation; and evidence-based, predictive analytics for medical diagnosis and treatment planning can affect the positive transformation of medical practice and healthcare delivery, if deployed on CSP platforms to minimize cost and complexity.

The major issues for the security in existing cloud data in the cloud server is utilize the service via the cloud may cause the problem of data loss or an unauthorized data access. In general, the extracted features for cloud computing components are as follows:

A. Software as a Service (SaaS): Instead of dedicated software applications for an organization, everyone tries to utilize the leased software product in cloud service provisions. Growing demands in industry push the clients to move towards the software as a Service (SaaS) over the communication channel [5].

B. Platform as a Service (PaaS): The cloud computing progress take account of the leased platforms for its concerns regarding to utilize the internet based services over the cloud service provision in the communication channel. The PaaS service model creates all of the conveniences required to maintain the complete web applications and services consumption [5].

C. Infrastructure as a Service (IaaS): The competence makes available to the clients in the provision of cluster servers (Cloud Service Providers), processing units, storage infrastructures, communication channel (Intranet or Internet), and other fundamental computing resources related with build an Infrastructures residues under Infrastructure as a Service (IaaS) [5].

II. RELATED WORK

Cloud computing also offers another important service data storage as a service. The main benefit of using cloud

computing is to reduce the installation cost of hardware, software applications, complex computations at client side. All the cloud services are maintained by the cloud providers at remote centers and services are provided to the end users with a simple web browser through the internet connection. Using cloud computing small industries are getting more beneficial to their companies. Cloud computing provides more benefits to the users but still users have some consideration and worrying about their data which is stored at cloud because whatever data is stored at cloud not under control of users .All the security mechanisms are provided by the cloud providers only. The security of the data which is stored at cloud is maintained by the cloud provider or cloud user is based on the type of application choose by the user [1].

The Related work performs a detailed study about three existing cloud storage security algorithms named as Auditing Algorithm Shell (AAS), Matrix Encryption Algorithm (MEA) and Procedure Block Authentication Algorithm (PBAA). In the first related work, the author discussed about security concerns and challenges at numerous levels in the cloud computing. Most of the cloud data transactions the security challenges in cloud computing have high impact to limit the scope of this domain. Due to privacy, integrity and confidentiality concern of data, there is a need of security architecture that should overcome the security risks in cloud computing and reduce the fear of enterprise customer to adopt cloud [13].

Thus, we developed an architecture known as cloud trusty architecture. It provides four defensive layers that ensure security of the outsourced data in the untrusted cloud data center: Core Layer, Intermediate service provider, Data description and Data transfer. The process of implementing or updating the security architecture of Cloud Computing is difficult or evenimpossible to navigate because of the rapid change and agile nature of information technology. System networks are now evolving very fast with the revolution in the cloud computing. Furthermore, old models for the network security have been proved useless against the new coming malwares and advanced threats. Target data breach is an example, which result the loss of more than 100 million user archives [6][7].

Big multinational companies like Adobe and eBay emphasize on the serious risks associated with the insufficient cloud security. In addition, a set of roughly integrated security applications and devices make it problematic for the IT groups to identify the threats, as they are incapable to correlate the different security reports, logs, alerts and events. The analysis of our work ensures maximum security for data breaches. It is an integrated framework to provide security for IT organizations. The following diagram (Figure3) illustrates functional architecture for Auditing Algorithm Shell (AAS) along with its working principle.

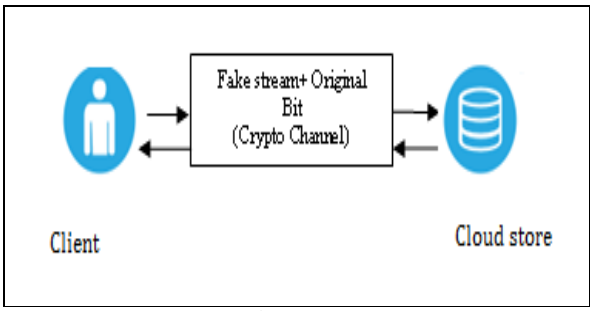


Fig. 3 Architecture for Auditing Algorithm Shell

$$\mathbf{E_T} = \sum (P_T + \Phi) \quad \ldots\ldots\ldots\ldots (1)$$

$$\mathbf{D_T} = \sum (E_T - \Phi) \quad \ldots\ldots\ldots\ldots\ldots (2)$$

$$\mathbf{T= \{}t_1, t_2, \ldots\ldots\ldots, t_m\mathbf{\}} + \Delta t \quad \ldots\ldots\ldots (3)$$

$$S= \{B_1, B2, \ldots\ldots\ldots, B_n) + \Delta s \quad \ldots\ldots\ldots (4)$$

```
Begin AAS_Encrypt ( )
While (n! =0) do
S: =Plain Text;
Φ: =Fake Stream;
E_T: =S+Φ;
End while;
End;
```

Algorithm 1 Auditing Algorithm Shell (AAS)

From the equations 1 and 2, the set of symbolic representations **(**E_T , P_T, D_T , Φ) are describes Encryption Text, Plain Text , Decryption Text and Fake stream Bit) as well as the equations 3 & 4, are describing Time and Storage requirement for the cloud data transfer by using AAS. The actual time for data transfer **{**t_1, t_2, ……., t_m**}** among the cloud clients exceeded (Δt), because of fake stream annexure with original data. At the same cost, it may also increase the genuine storage space ({B_1, B2,……., B_n) with addition of (Δs), because the insertion of fake stream bits (E_T: =S+Φ). The same working principle is explained by the AAS encryption algorithm. In this approach, the method of key generation depends on fake stream bits and key distribution (original content +key) happened in same cloud server[8].

The second category of related work, proposed technique emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry about the vulnerability of remote data to criminals and hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem [2].

Both substitution and transposition techniques have used alphabet for cipher text. In the proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. In classical encryption technique,

the key value ranges between 1 to 26 and key may be string (combination alphabets). The method of encryption and key distribution is also carried out as a normal procedure. The domain required to make a secure data transactions under the cloud computing environment has to choose same cloud server for storing the encrypted data and the required key to break it.

The third related work has to specify a procedure Blocks for make an encryption and perform services via cloud environment. The working principles of the Procedure Block Authentication Process is , Divide the original data or message (M) into fixed size of Packets (S) and group the specified number of packets into a Block (B) as a fixed size or variable –length size. Thereafter, to assign the authentication code from any one of cryptographic algorithms for secures access[9][10].

Cloud Computing is the process of providing cloud services on the internet. Cloud services allows the organizations and individuals to use the software that managed by cloud services provider. Cloud computing model allow accessing the services and information remotely. Because of moving data to cloud services, organizations are looking for protecting their data against unauthorized access[11]. Securing the cloud means secure the calculation, storage and applications. Security goals located into three points: confidentiality, integrity and availability.

Cryptography is caring about the confidentiality of data in the cloud. Cryptography these days is a combination of three algorithms types: (1) Symmetric Key Algorithms (2) Asymmetric Key Algorithms and (3) hashing. Data cryptography is encoding the content of the data like text and media to make it not understandable, meaningless and invisible during transmission and storage, this term known as encryption. The reverse process of to retrieve, the original data from encrypted data is known as decryption. To encrypt data on cloud storage both symmetric key and asymmetric key can be used, but according to the huge size of the database and data stored in cloud storage using of symmetric key algorithm is faster than asymmetric key [3][12].

Then do the authentication process by using the key (K) at the time of receive any request from cloud clients or users. If the Authentication process is success, then provide the service, otherwise to terminate from the request. Among all the above three related work in order to enhance the secure cloud data storage management proposed and implemented encryption algorithm by using their own logics. But most of these security algorithms follow a same streamline for data storage selection in the same cloud server or service provider. In this gap, provides a opportunity for data loss or an intrusion of unauthorized users with respective cloud service providers (CSP). While choose to, the healthcare records maintenance or transaction under private cloud issues list out the following performance analysis metrics (Table I).

TABLE I PERFORMANCE EVALUATION BASED ON HEALTHCARE DOMAIN

Algorithms	Storage(Kb)	Speed(mS)	Security (%)
AAS	25.5	19	45.8
MEA	20	32	35.6
PBAA	43	45	51.3

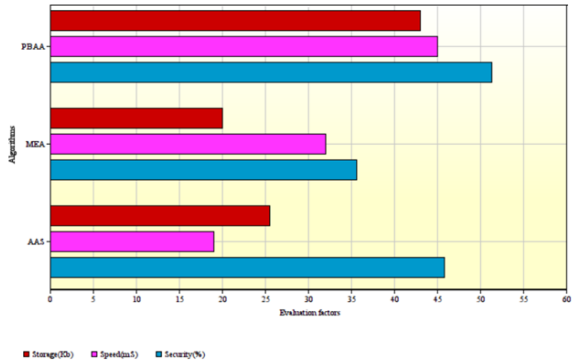


Fig.4 Evaluation Metrics for Cloud Secure Algorithms

In the healthcare records transactions under the cloud service providers are usually to avoid the standard security algorithms such as Advanced Encryption Standards (AES), Data Encryption Standards (DES) or any one. Because the consideration for storage space, speed of retrieval as well as the complexity in security. Due to that many researchers proposed varieties of cloud security algorithms such as mentioned in these related work. In the compilation of data, with respect of storage, speed and the security from the observation are listed in the table I and the graph based on evaluation metrics (figure 2).

III. IMPLEMENTATION

The cloud data storage and secure mechanism for cloud service utilization is carrying with the help of Orthogonal Handshaking Authentication protocol or Mechanism (OHSAM). In general, the term “orthoganality” is generally referred to as “Perpendicular with each other” working principles on cloud data storage set. Whenever the cloud services (SaaS, PaaS or IaaS) is required by the cloud clients or user is initiated with the steps for registration on the trusted third party network. The registration process is illustrated with the following diagram (figure 5). The new cloud client or user before to initiate the service utilization, must be register on the relevant cloud service provider and get an ID for authentication purpose through the random ID creation module. The performance evaluation includes with details analysis of following implemented Steps: Registration in the cloud service providers (CSP), Encryption or Decryption Mechanism, Key Distribution, Authentication – Handshaking and the Retrieval or Response.

A. OHSAM Key Generation for Registration

In order to initiate the secure cloud storage management first step begins with registering cloud service providers with the help of key generation. The given original content

textual information's are considered as equivalent numeric value (NV) for an English alphabet and special characters. Usually, the encrypted message will be stored in the cloud server data storage along with the key in the identical server. It creates an opportunity for the malicious users attack.

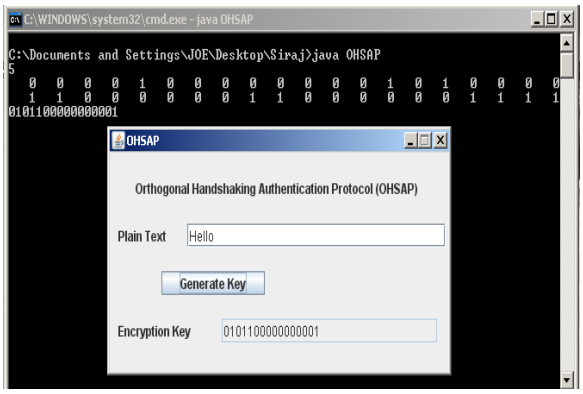


Fig.5 Orthogonal Encryption Key generation

For this reason, in this proposed work, the encryption message (Ciphertext) and the Encryption key (OE_K) in two different servers (Φ) and to select the Orthogonal cloud server Selection (C_S) along with the key (O_K). The Orthogonal Block Link Table is maintaining physical address for orthogonal cloud servers and its link address and it describes under the heading of key distribution and authentication.The OHASP key generation is begin with Plain text -English alphabets' equivalent numeric numbers such as A or a=1,B or b=2, is like that. The encryption bit position for the message as well as the key generation will be considered as 128-bit binary format and the numeric value conversion for the required encryption to be considered as 4 bit position.Then encrypt the message before store into the cloud service provider (CSP) under the Software as a Service (SaaS). For example consider the message as "HELLO". The equivalent numeric value for the given message is "00080005001200120015". Then the numeric value will be converted into the equivalent binary value (4 bit input string will be considered for the conversion of 128bit position).

1. Initialization before to start
2. Input (I) ← Equivalent NV
3: Storage (S) ← Initialized with "0"
4: while (not end) do {
n
5: I (n) ← $\sum_{i=1}$ C_i (NV)
6: Φ← Encryption
7: End while
8: $OE_K = H + (O_K)_{128}$
9: OBLT ← C_p + L
n
10: O ← $\sum_{i=1}$ P_i $+C_s$

Algorithm 2 Algorithm for OHASP key generation

The Orthogonal encryption key will be generated from the storage that initiates to store the binary values for individual character in row for individual position (M x N). Then the resultant key for given plain text is "OEK = 0101100000000001". It shown in the figure (6) and the OHASP (Orthogonal Hand Shaking Authentication Protocol) displayed in Algorithm 2. After separate the key values from the encrypted text , the remaining binary digits are grouped together as "Encrypted Text" for the purpose to store in a cloud service provider(figure 6). The key as well as the encrypted content has to select its cloud storage based on the orthogonal principles by using Orthogonal Block Link Table (OBLT). The content resides in CSP, whenever it requires clients or users is performed based on Orthogonal Hand Shaking Authentication Mechanism (OHSAM).

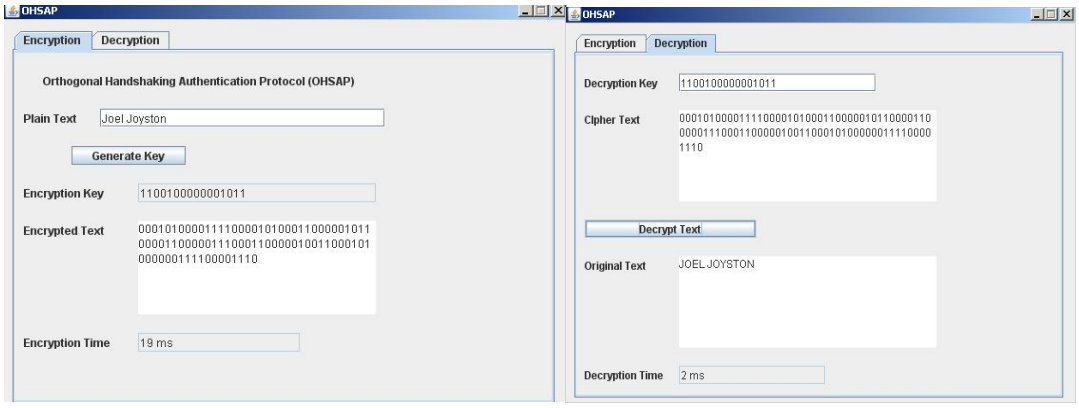


Fig.6 OHSAP Encryption and Decryption

B. Authentication, Key Distribution and Cloud Storage Mechanism

From the specification, initially the service request (S_{Req}) will beinitiatedby the end user/client towards the cloud Service provider (CSP). If the CSP receive a service request, then it will send the authentication encryption key (A_K) from the Cloud server storage of the encrypted key portion. Then the authentication key will be forwarded to the service request initiation end user /client. Then confirm,

the "Key" with the service request client and the CSP. Then the client or end user utilizes the required service from the appropriate CSP. (The information retrieval taken place the CSP perpendicular with each other). It has shown in the following Algorithm 3.

Begin procedure AUTH ()
1: S_{Req} → CSP
2: CSP→ A_K from CSP (A_K)
3: A_K→S_{Req}
4: if (S_{Req} (K) ==A_K) then
5: Fetch the information from CSP (D)|| CSP (A_K)
6: end if
End AUTH;

Algorithm 3OHSAP- Authentication Mechanisms

The authentication handshaking taken place under the private cloud clients and the CSP and the transaction will be secured by OHSAP. The OHSAP is the set of rules and regulations on how to encrypt and decrypt the content as well as to select the cloud server for its storage. The OHSAM is the process for how to apply OHSAP in various domains. In order to consider the healthcare records (Healthcare Domain) transactions under private cloud provides the efficiency of the OHSAP algorithms and its implemented work. It proves better way to generate the encryption key, Speed for encryption and decryption, Retrieval ability and the cloud Storage (Table II).

TABLE II EVALUATION METRICS FOR KEY GENERATION

Algorithms	Key Size(bit)	Speed (ms)	Storage (Kb)	Retrieval Time(ms)
AAS	32	28	125	24
MEA	16	34	89	18
PBAA	64	42	78	33
OHSAM	128	19	43	11

According to the evaluation of encryption or Decryption Key Size,
y = -25.7x + 148
R^2 = 0.964
According to the evaluation of Storage,
y = 32x - 16
R^2 = 0.833
According to the evaluation of speed,
y = -1.9x + 35.5
R^2 = 0.063

Most of the cloud service applications are usually protected with the help of encryption and Decryption mechanisms either it may use symmetric or asymmetric key structure. The implementation basics also provide a concrete foundation by using the orthogonal handshaking authentication key generation. In the above equations "y" represents the comparison resultant axis values for the factors such as key size, storage and speed for different existing cloud storage security algorithms along with OHSAM.

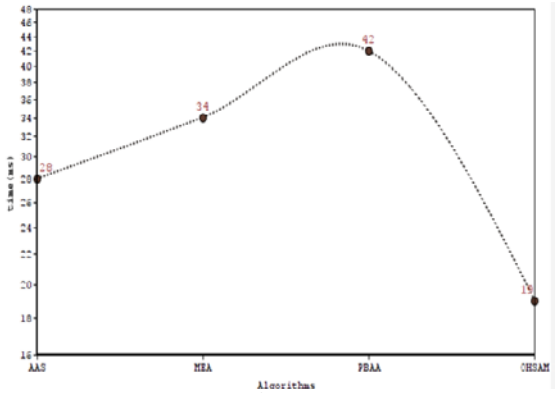


Fig.7 Evaluation of Key generation speed

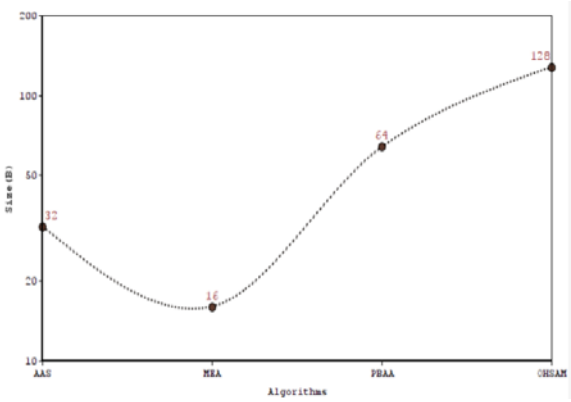


Fig.8 Evaluation of Key Bit size

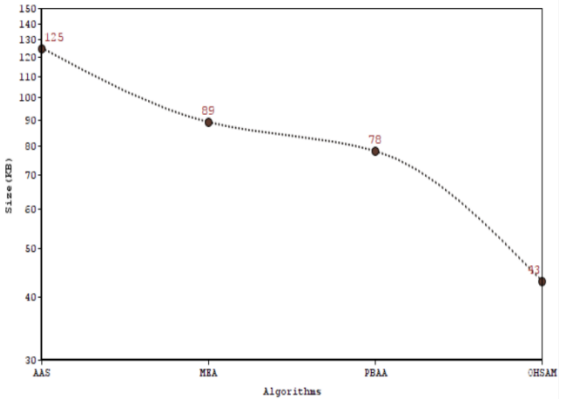


Fig. 9 Evaluation of Storage

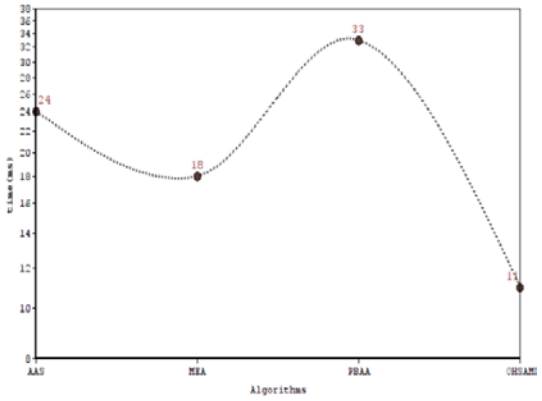


Fig. 10 Evaluation of Retrieval time

The peformance analysis graphs from the figure [8][9][10][10] are depicted the evaluation factors such as key generation, size, speed and retreibval mechanism along with OHSAM. In all the it proves an effective key generation as well as the modern approach for storage selction by using Orthogonal. The way to finding cloud servers from any service provider (for example Amazon Wen Services-AWS), based on the Orthogonal Hand Shaking authenticion mechsnaim (OHSAM) with the help of Orthogonal Block Link Table(OBLT).

TABLE III OBLT PHYSICAL IDENTIFICATION

Sequence Number	Physical Address	Data (D)	Predecessor Link(P_L)	Successor Link(S_L)
N1	100	AA	000	200
N2	200	AB	100	400
N3	400	AC	200	300
N4	300	AD	400	500
N5	500	AE	300	600
N6	600	AF	500	000

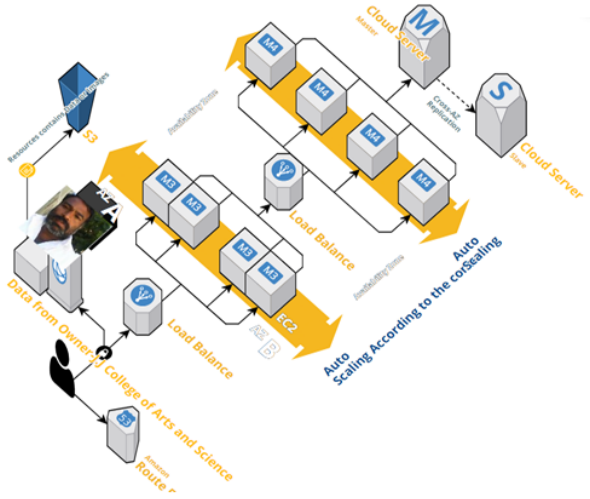
From the given sample data collection set related with Healthcare Domain is depicted by the figure 11. Data owner either may be a invidual or an institution to store their content (Data or Image) by using OHSAP with respective cloud service providers. Each and every cloud service providers physcial configuration has to be considered as a doubluy linked list representation node (N) having three comoments for: Predecessor Link, Data and the Succesor Link. The physical identification for node selection is depicted by the Table III.

$$B=\int_{0}^{n-1}\Sigma \{ (P_L,D,S_L)_1, (P_L,D,S_L)_2,.., P_L,D,S_L)_n\} \rightarrow (5)$$

$$N= (P_L, D, S_L) \rightarrow (6)$$

$$B=\int_{0}^{m-1} \Sigma (N_1, N_2, N_3...N_m) \rightarrow (7)$$

$$B=\int_{0}^{5} \Sigma \{(000, AA, 200), (100, AB, 300), (200, AC, 400), (300, AD, 500), (400, AE, 600), (500, AF, 700) \} \rightarrow (8)$$



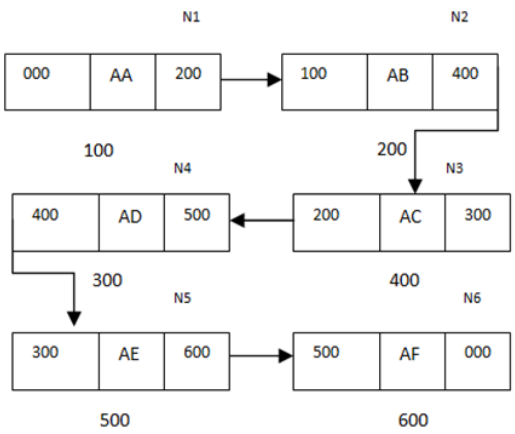


Fig. 11 OHSAM Cloud Storage-Authentication

The OBLT having the node specification as a collection of existing cloud service providers(equation 5) has to replaced by symbolic representations "N" (from the equation 6). Finally the summarized content selection is considered based on its orthogonal features.

ACKNOWLEDGEMENT

The Healthcare Domain related works are: John Barton (Pillsbury Law), Frank Chin (iTGRC Asia Advisory and Consulting), Chris Dotson (IBM), Mike Edwards (IBM), Melvin Greer (Intel), Elizabeth Koumpan (IBM), John Meegan (IBM), Peter Melrose (Independent IT consultant for Healthcare), Rahat Mujib (IBM), Osakpamwan Osaigbovo (IBM), Bill Parker (Presidio), John Sanders (CIO Management Group, Inc.), Karolyn Schalk (IBM), Karl Scott (Satori Consulting), Joel Thimsen (Perficient) and Mark Underwood (Krypton Brothers).

portions to the Cloud Standards Customer Council Impact of Cloud Computing on Healthcare, Version 2.0 (2017).

REFERENCES

[1] K. Subramanian and M. Mohamed Sirajudeen, "An Architectural Framework for Secure Cloud data Storage Management by using Orthogonal Handshaking Authentication Mechanism (OHSAM)", *International Journal of Mechanical Engineering and Technology*, Vol. 9, No. 3, pp. 791–799, 2018.

[2] K. Subramanian and M. Mohamed Sirajudeen, "Implementation of Secure Cloud data Storage- Data Transaction by using an Orthogonal Handshaking Authentication Mechanism(OHSAM)", *International Journal of Computer Science and Information Technology (IJCSIS)*, Vol. 16, No. 3, pp. 221-227, March 2018.

[3] B. Veerendra and Y. V. Durga Prasad, "A Trusted Framework for Authentication and Security for Business Applications in Cloud", *International Journal of Modern Trends in Science and Technology*, Vol. 3, Special Issues No. 1, pp. 32-35, Feburary, 2017.

[4] Manish, RadhaiMahavidyalaya, R. Shinde and Rahul D. Taur, "Encryption Algorithm for Data Security and Privacy in Cloud Storage", *American Journal of Computer Science and Engineering Survey*, ISSN: 2349-7238.

[5] Eng. Hashem H. Ramadan and Mousse Adamou Djamilou, "Using Cryptography Algorithms to Secure Cloud Computing Data and Services",*American Journal of Engineering Research (AJER)*, Vol. 6, No. 10, pp. 334-337, 2017.

[6] T. Ramaporkalai, "Security Algorithms in Cloud Computing", *International Journal of Computer Science Trends and Technology (IJCST)*, Vol. 5, No. 2, pp. 500-503, Mar – Apr. 2017.

[7] PapriGhosh, Vishal Thakor and Dr.PravinBhathawala, **"**Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms", *International Journal of Advanced Research in Computer Science and Software Engineering*,ISSN: 2277 128X, Vol. 7, No. 5, pp. 469-471, May 2017.

[8] K. V. Nasarul Islam and K. V. Mohamed Riyas, "Analysis of Various Encryption Algorithms in Cloud Computing", *International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol. 6, Issue 7, pp. 90 – 97, July 2017.

[9] M. Omer Mushtaq, FurrakhShahzad, M. Owais Tariq, MahinaRiaz and BushraMajeed,"An Efficient Framework for Information Security in Cloud Computing Using Auditing Algorithm Shell (AAS)", *International Journal of Computer Science and Information Security(IJCSIS)*, Vol. 16, No. 11-2016,pp. 317-331.

[10] JasleenKaur and Dr.SushilGarg, "Security in Cloud Computing using Hybrid of Algorithms ", *International Journal of Engineering Research and General Science*, , Vol. 3, Issue 5, pp. 300-305, September-October 2015.

[11] Er. AshimaPansotra and Er. SimarPreetSingh, "Cloud Security Algorithms", *International Journal of Security and Its Applications*, Vol. 9, No. 10, pp. 353-360, 2015.

[12] M. Mohammed Sirajudeen and K. Subramanian, "Enhancement of the Private Cloud Data Transaction by using an Orthogonal Handshaking Authentication Protocol (OHSAP)", *International Journal of Computer Applications*, Vol. 96, No. 23, 2014.

[13] Jean Raphael NgnieSighom, Pin Zhang and Lin You, "Security Enhancement for Data Migration in the Cloud", *Future Internet*, Vol. 9, No. 23; DOI: 10.3390/fi90300232017.