Health Care Data Security in Cloud

Priya Musale

Prof. Tanuja Sali

Abstract—**Healthcare data has stringent security requirements for confidentiality, availability to authorized users, and traceability of access. The focus of this study is to investigate on these requirements and propose a solution for health care cloud providers that will help in protecting patient' data they host, which is of high importance. The focus will be on specific cloud computing health care security concerns and how cloud homomorphic encryption with splitting key and key delegation can help in meeting healthcare regulatory requirements. The suggested technique is based on FHE algorithm, RSA algorithm, Secret sharing algorithm, Data sharing algorithm with key delegation to ensure data confidentiality, authentication, integrity, and availability in a multilevel hierarchical order. This will enable the healthcare provider to apply/omit any access rule in any order, especially in medical research environment**

Index Terms—**Cloud computing, Healthcare, Homomorphic algorithm, RSA algorithm, Secret sharing algorithm, Data sharing algorithm**

I. Introduction

Cloud computing presents a new model for improving the delivery of healthcare and increasing the business flexibility of medical organizations, enabling them to operate with greater efficiency, cost-effectiveness, and agility. Use of cloud services has taken off across countless industries. Adoption of cloud computing in healthcare has taken place a little more tentatively, as providers sort out how they can benefit from cloud offerings and how much of their operations they can afford to transfer to the cloud. electronic health record (EHR), analytics and imaging systems are a few areas in which healthcare providers have found success with cloud deployments.

Aim of the paper. The contribution of our paper is to appeal to data encryption in healthcare cloud computing environment.

II. CLOUD COMPUTING FOR HEALTHCARE

Healthcare organizations (HCOs) are expected to provide new and improved patient care capabilities while simultaneously limiting healthcare cost increases. Information Technology plays a strong role in the health and patient care arenas with cloud computing slowly beginning to make its mark. However, despite the significant advantages for the utilization of cloud computing as part of Healthcare IT (HIT), security and privacy, reliability, integration and data portability are some of the significant challenges and barriers to implementation that are responsible for its slow adoption.

Technology and Healthcare: Cost, efficiency and effectiveness create ongoing complexity for the health care industry. The latest new technology will fix or mitigate these problems, for the benefit of the health care system, individual patients and those paying for health care. But the regulatory system is getting in the way of this technology making this all work. If we could just let the technology work, everything would be well.

First, it was the Health Insurance Portability and Accountability Act (HIPAA) “standard transactions” rule. This idea streamlined, uniform electronic transactions, fitting all shapes and sizes in the health care industry would create enormous efficiencies and ease transaction costs.

The latest technological opportunity comes through the use of cloud computing. As the concept of cloud computing has rapidly moved onto the scene, businesses across all industries have moved swiftly (and some would argue recklessly) to take advantage of “the cloud,” often without fully realizing the hidden risks associated with this movement because of the immediate lure of visible cost savings. The health care industry (as it often is) has been slow to take advantage of the technological opportunities presented by the cloud, but the issues with cloud computing go deeper than this general technological reluctance.

Benefits of Cloud Computing for Healthcare: “Patient centricity” has become the key trend in healthcare provisioning and is leading to the steady growth in adoption of electronic medical records (EMR), electronic health records (EHR), personal health records (PHR), and technologies related to integrated care, patient safety, point-of-care access to demographic and clinical information, and clinical decision support. Availability of data, irrespective of the location of the patient and the clinician, has become the key to both patient satisfaction and improved clinical outcomes. Cloud technologies can significantly facilitate this trend.

Cloud computing offers significant benefits to the healthcare sector: doctor’s clinics, hospitals, and health clinics require quick access to computing and large storage facilities which are not provided in the traditional settings. Moreover, healthcare data needs to be shared across various settings and geographies which further burden the healthcare provider and the patient causing significant delay in treatment and loss of time. Cloud caters to all these requirements thus providing the healthcare organizations an incredible opportunity to improve services to their customers, the patients, to share information more easily than ever before, and improve operational efficiency at the same time.

Privacy and Security Challenges: Data maintained in a cloud may contain personal, private or confidential information such as healthcare related information that requires the proper safeguards to prevent disclosure, compromise or misuse. Globally, concerns related to data jurisdiction, security, privacy and compliance are impacting adoption by healthcare organizations.

Data Security and Availability: Related to security is an important challenge the idea of “availability” of the data. Healthcare providers need access to patient data all the time, immediately and reliably. While the cloud often provides this, there remain concerns about accessibility of data on an automatic basis, with consistent reliability. And, where healthcare providers are concerned about this reliability, they either will refuse to use the cloud or will find a need to build redundant systems, thereby reducing or eliminating the cost benefits of the cloud.

Data Portability. Another barrier that impacts some healthcare organizations’ willingness to adopt cloud computing is the concern regarding the ability to transition to another cloud vendor or back to the healthcare organization without disrupting operations or introducing conflicting claims to the data. With traditional IT, the healthcare organization has physical control of systems, services and data. The concern is that if a provider were to suspend its services or refuse access to data, a healthcare organization may suddenly be unable to service its patients or customers. Or, if the healthcare organization were given notice that the cloud service would be discontinued, the lack of interoperability across cloud systems could make it very challenging to migrate to a new cloud service provider.

III. LITERATURE REVIEW

A. Modern Cryptography

Modern Encryption algorithms (such as RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blow-Fish) still play the main role in data security of cloud computing. The evaluation has been performed for those encryption algorithms according to randomness testing by using NIST statistical testing in cloud computing environment (Amazon EC2) [6]. From simulation results, the authors concluded that no strong indications of statistical weaknesses for the eight modern encryption algorithms when applied in cloud computing environments.

A hybrid encryption technique (uses RSA, 3- DES and Random Number generator algorithm) is suggested to enhance the security of cloud database [7]. This technique provides the flexibility in range and sequence to the user's choice. This is because a user can apply all of the three encryption methods or omit any in any order. Even if the user does not select any encryption technique, the random number algorithm will still be implemented by default, thus providing at least a single level security. The opted sequence will also be stored in the database so that the decryption can be possible. The negative effect of this scheme is that it creates an overhead on the query performance due to the multilevel nature of encryption and decryption. Also the computation time increases as the size of data increases.

Elliptic Curve Cryptography was proposed to explore data security (confidentiality and authentication of data) between clouds [8]. Elliptic curve cryptography [ECC] is a public-key cryptosystem in which every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems, i.e. Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm.

B. Homomorphic cryptography

The fully homomorphic encryption, or FHE is not a new idea as it has been, for many years, viewed as a fantasy that would never come true. Rivest, Adleman, and Dertouzos [9] suggested that fully homomorphic encryption may be possible in 1978, shortly after the invention of the RSA cryptosystem [10], but were unable to find a secure scheme for its realization. This was changed in 2009, with a breakthrough discovery by Craig Gentry [11, 12], who was then a graduate student at Stanford University. (He is now at IBM Research.) Since then, further refinements and more new ideas have been coming at a rapid pace [13].

Before trying to explain how homomorphic encryption works, we should explain the word homomorphic [14]. The Greek roots translate as same shape or same form, and the underlying idea is that of a transformation that has the same effect on two different sets of objects. The concept comes from the esoteric world of abstract algebra, but we can offer a more homely example, where the two sets of objects are the positive real numbers on the one hand and their logarithms on the other. Then multiplication of real numbers and addition of logarithms are homomorphic operations. For any positive real numbers x, y and z, if $x \cdot y = z$, then $\log(x) + \log(y) = \log(z)$. This homomorphism offers two alternative routes to the same destination. If we are given x and y, we can multiply them directly; or we can take their A logarithms, then add, and finally take the antilog of the result. In either case, we wind up with z. Homomorphic cryptography offers a similar pair of pathways..

In encrypted computation, the user specifies encrypted inputs to a program, and the server computers on encrypted inputs to produce an encrypted result. This encrypted result is sent back to the user who decrypts it to get the actual result. The fully homomorphic encryption (FHE) scheme, means that there are no limitations on what manipulations can be performed [15] .

The fully homomorphic encryption (FHE) scheme allows a worker that does not have the secret decryption key to compute any result of the data (still encrypted), even when the function of the data is very complex.

Homomorphic encryption scheme, based on Residue Number System (RNS), was proposed to enhance the security [16]. In HORNS scheme, a secret is split into multiple shares on which computations can be performed independently. Efficiency is achieved through the use of smaller shares. HORNS scheme depends on the RNS property that creates multiple shares of a data and the operations on these shares are homomorphic. Security is enhanced by not allowing the independent clouds to collude.

C. Searchable Encryption

Searchable encryption is a broad concept that deals with searches in encrypted data .The goal is to outsource encrypted data and be able to conditionally retrieve or query data without having to decrypt all the data. There are two approaches to the searchable encryption. The first approach is to use symmetric encryption [17,18], whereas the second approach for is to use asymmetric encryption [19, 20, 21].

D. Attribute Based Encryption

In the Attribute Based Encryption ABE [22], the attributes and policies associated with the message and the user decide which user can decrypt a cipher text. A central authority will create secret keys for the users based on attributes/policies for each user. Users in the system have attributes; users receives a key ("or key bundle") from an authority for their set of attributes. Cipher text contains a policy (a Boolean predicate over the attribute space). If a user's attribute set satisfies the policy, he can use his key bundle to decrypt the cipher text. Multiple users cannot pool their attributes together.

IV. PROPOSED SYSTEM

The health care industry is shifting toward an information-centric care delivery model, enabled in part by open standards that support cooperation, collaborative workflows and information sharing. Services delivered by cloud computing will evolve to support a wide variety of healthcare processes. Cloud computing provides an infrastructure that allows hospitals, medical practices, insurance companies, and research agents to tap improved computing resources at lower initial capital outlays.

Healthcare IT managers understand that cloud computing has its potentials, but many are concerned about privacy and security issues and are delaying plans to move their critical patient data onto cloud-based systems. In this section, we will focus on specific cloud computing healthcare security concerns. Patient privacy is considered as the most serious problem in cloud computing and encryption is thought to be the sole solution. However, several questions need to be answered to address this issue:

1. How to make processing over encrypted data?
2. How to search over encrypted data?
3. How to grant partial access?

Our scenario will describe a proposed centralized secure data sharing framework for healthcare cloud-based EHR and, hence, addresses the above mentioned questions. Let us assume that This paper have three basic organizations A, B and C in our healthcare industry, as shown in Figure 1.

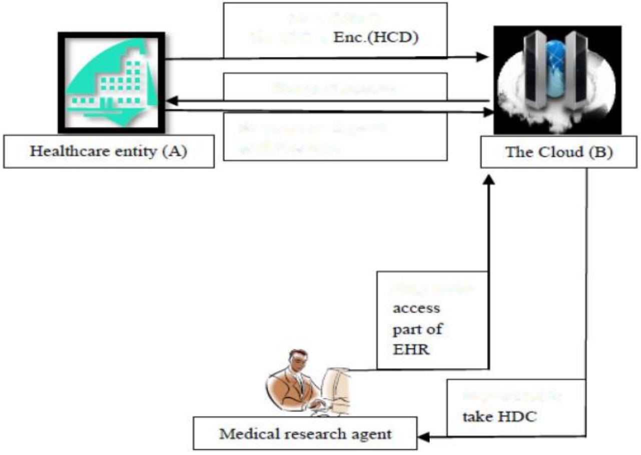


Figure 1: The centralized secure data sharing framework for cloud

Healthcare entity (A) from various domains such as primary care, pharmacy, clinic lab and emergency care hosts their EMRs in cloud (B) to achieve lower operation cost, higher interoperability, and ubiquitous service delivery and so on. The medical research agent (C) needs some healthcare data for its medical-related research. The healthcare entity (A) is the owners of EHRs who specify access control policies to control who can access which portions of their EHRs, with various roles. To satisfy HIPAA and other privacy and security requirements, the medical research agent C should not access Personally Identifiable Information (PII). Administrators perform administrative functions such as activating or deactivating users, and registering or de-registering medical research agent. The proposed solution is the using of homomorphism cryptography with Attribute Based Encryption.

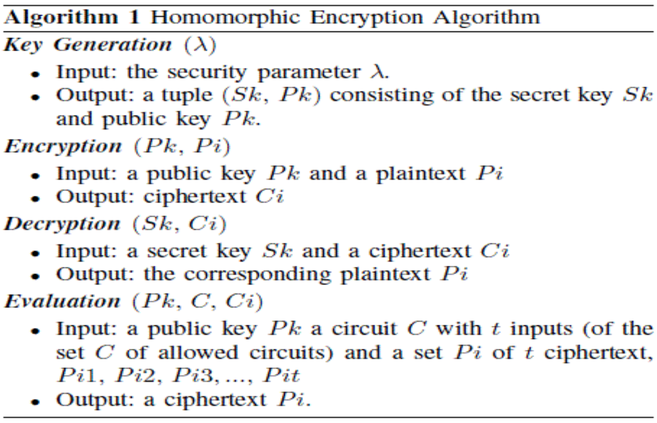
V. METHDOLOGY

A. Homomorphic encryption scheme :

Homomorphic encryption allows people to use data in computations even while that data are still encrypted. Homomorphic encryption use mechanisms similar to conventional cryptography, where plain texts and cipher texts both are treated with an equivalent algebraic function. Now the plain text and cipher text might also be not related but the emphasis is on the algebraic operation that works on both of them. In Ref. [1] it gives a definition for homomorphic public- key cryptosystem. Let Ek1(m) be the encryption of plaintext m taken from the set of plaintexts M using public key k1 and Dk2(c) be the decryption of ciphertext c using private key k2. A cryptosystem is homomorphic if the encryption and decryption functions satisfy Eq.(1) where m1, m2 are taken from M.

$$f1\ (m1,m2) = Dk2\ (f2\ (Ek1(m1),\ Ek1(m2))) \qquad (1)$$

The operation f1 on the plaintext is the same as the decryption of the operation f2 on the corresponding encrypted ciphertext according to Eq.(1). If f1 is an addition operator, the scheme is said to be additively homomorphic, and multiplicatively homomorphic if f1 is a multiplicative operator. If f1 and f2 are the same operators, the cryptosystem is algebraically homomorphic. Homomorphic encryption scheme consists of the following four algorithms:

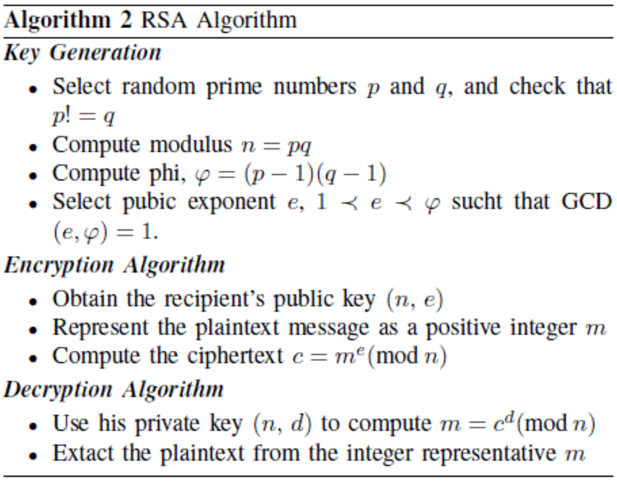


```
Algorithm 1 Homomorphic Encryption Algorithm
Key Generation ($\lambda$)
  • Input: the security parameter $\lambda$.
  • Output: a tuple $(Sk, Pk)$ consisting of the secret key $Sk$
    and public key $Pk$.
Encryption ($Pk, Pi$)
  • Input: a public key $Pk$ and a plaintext $Pi$
  • Output: ciphertext $Ci$
Decryption ($Sk, Ci$)
  • Input: a secret key $Sk$ and a ciphertext $Ci$
  • Output: the corresponding plaintext $Pi$
Evaluation ($Pk, C, Ci$)
  • Input: a public key $Pk$ a circuit $C$ with $t$ inputs (of the
    set $C$ of allowed circuits) and a set $Pi$ of $t$ ciphertext,
    $Pi1, Pi2, Pi3, ..., Pit$
  • Output: a ciphertext $Pi$.
```

B. RSA Cryptosystem :

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the RSA is a commonly adopted public key cryptography algorithm. It uses public key and private key to encrypt and decrypt messages. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. Using an encryption key (e, n), the algorithm is as follows:



```
Algorithm 2 RSA Algorithm
Key Generation
  • Select random prime numbers $p$ and $q$, and check that
    $p! = q$
  • Compute modulus $n = pq$
  • Compute phi, $\varphi = (p-1)(q-1)$
  • Select pubic exponent $e$, $1 \prec e \prec \varphi$ sucht that GCD
    $(e, \varphi) = 1$.
Encryption Algorithm
  • Obtain the recipient's public key $(n, e)$
  • Represent the plaintext message as a positive integer $m$
  • Compute the ciphertext $c = m^e (\text{mod } n)$
Decryption Algorithm
  • Use his private key $(n, d)$ to compute $m = c^d (\text{mod } n)$
  • Extact the plaintext from the integer representative $m$
```

C. Secret sharing algorithm:

Secret sharing algorithm is used to share a piece of information between the numbers of clients. The encryption takes place in the server and produce pieces of data in encrypted form. The decryption takes place on client side.

Only few shares are enough to reconstruct the original data. The threshold value is used as key i.e number pieces required to reconstruct the data. So it is also called as threshold scheme. Secret sharing algorithm is shown in figure 2.

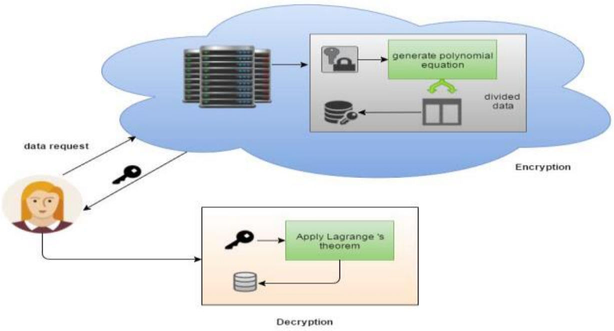


Figure 2. Secret sharing algorithm

D. Data sharing algorithm:

The data sharing in our framework. The Data sharing is done by user. Here, jill shares the data to Ross which she doesn't have access. Firstly, jill shares the data. The CSP of the Jill , Domain authority generate the secret key to jill. The secret key needs to share with the ross. And the Rose is being authorized by the attributes. Jill and Rose has different CSP. The algorithm 2 explains about the decryption process.

Algorithm 1 Data sharing algorithm

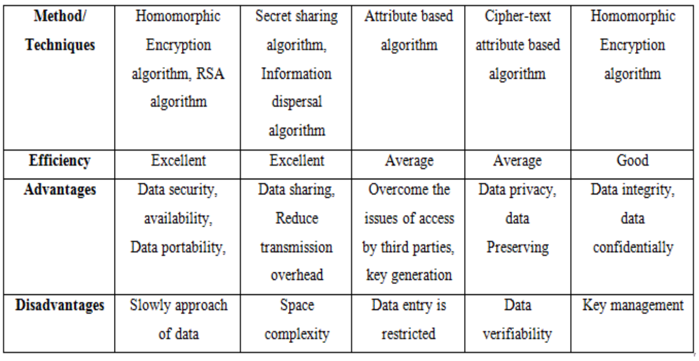
```
0: procedure SEARCH FILES
0: input
0: output ciphertext $\tau$ _= 0 $ie\ non - empty\ for\ each$ request  $search\ Id$
0: $for(i = 0; i < n; i{+}{+})$, then
0: Output $Fid\ for\ each$ Fid $outputs\ respective\ ciphertext$
0: Jill $generates\ the\ secret\ key\ for$ Rose $Domain\ authority$  $generates\ the\ Access\ Grants$ By respective CSP's
0: $for(j = 0; i < n; j\ {+}{+})$,then
0: Output cloud server Transfer key to outsourced decryption  server by step 6
0: endfor
0: endfor
0: end procedure=0
```

The Algorithm 2 explains about the decryption process of our framework. Once the cipher-text are transferred, The proxy server will re-encrypt the data and finally by matching the transformation key the rose able to decrypt the data. The role of semantically connected cloud is to assign the proxy servers with nearest distance and assigning the sharing the cipher-text to freely available servers. As the semantic cloud are connected by means of geographic location, it easier to for brokerage service to delegate the service to the user.

Algorithm 2 Decryption algorithm

```
0: procedure KEY MATCHING
0: input Access structures, key, ciphertext, transfer key.
0: output Message. $for\ each$ Ciphertext $there\ exist\ Id$
0: $for(j = 0; j < n; j\ {+}{+})$, then
0: Output $Re\text{-}encrypt\ Message\ for\ each$ Fid $outputs\ respective$  $ciphertext$
0: Rose $utilize\ the\ secret\ key\ to\ decrypt\ DA\ of\ rose\ verifies\ the\ Access\ Grants$ By respective CSP's
0: if $the\ Transfer\ key\ matches,\ then$
0: Output decryption server response with msg 5560: else  Access Denied
0: endfor
0: endfor
0: end procedure=0
```

TABLE NO.1 COMPARATIVE ANALYSIS



Method/ Techniques	Homomorphic Encryption algorithm, RSA algorithm	Secret sharing algorithm, Information dispersal algorithm	Attribute based algorithm	Cipher-text attribute based algorithm	Homomorphic Encryption algorithm
Efficiency	Excellent	Excellent	Average	Average	Good
Advantages	Data security, availability, Data portability,	Data sharing, Reduce transmission overhead	Overcome the issues of access by third parties, key generation	Data privacy, data Preserving	Data integrity, data confidentially
Disadvantages	Slowly approach of data	Space complexity	Data entry is restricted	Data verifiability	Key management

VI. CONCLUSION

This paper presented a data sharing systems that can be used to store sensitive health information which can be outsourced in the cloud with high security. The patients can send queries to specified doctors which are updated in the cloud. The doctors can reply to the queries which is updated and then encrypted by the admin. The patients view the details after proving the encryption key. The details remain encrypted to other users who view the health care information, ensuring the increased security. all data security method will also prove out to be successful in applying data security in a cloud computing environment thus maintaining the Confidentiality principle for storing the secure data on cloud in Healthcare.

ACKNOWLEDGMENT

This is great pleasure and immense satisfaction to express my deepest sense of gratitude and thanks to everyone who has helped me in completing my work successfully. I would like to thank the Prof. Tanuja Sali for her valuable support and guidance as well as our department members. And of course my family for always being there for me. I also acknowledge the research work done by all researchers in this field.

REFERENCES

[1] Samir Bahsani, Tarik Nahhal," Encryption as a Service for Data Healthcare Cloud Security ",IEEE,2016.
[2] Mr.K.A.Muthukumar,Dr.M.Nandhini,"Modified Secret Sharing Algorithm for Secured Medical Data Sharing in Cloud Environment",IEEE,2016.
[3] Fahad Saeed Alamri, Ki Dong Lee, "Secure Sharing of Health Data OverCloud",IEEE,2015.
[4] Alex Page,Ovunc Kocabas, Scott Ames, "Cloud-based Secure Health Monitoring: Optimizing Fully Homomorphic Encryption for Streaming Algorithms",IEEE,2014.
[5] Huda Elmogazy, Omaima Bamasak," Towards Healthcare Data Security in CloudComputing",IEEE,2013.
[6] S. El-etriby, E. M. Mohamed, H. S. Abdul-kader, "Modern Encryption Techniques for Cloud Computing", ICCIT. 2012.
[7] A. Kaur, M. Bhardwaj, "Hybrid Encryption for Cloud Database Security", UESAT, Vol-2, Issue- 3, pp737 - 741, May-Jun 2012. (http://www.ijesat.org)
[8] V. Gampala, S. Inuganti, S. Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography",USCE, Vol. 2, Issue 3, ISSN: 2231-2307, July 2012.
[9] R. L. Rivest, L. M. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Sec.Comp., pp. 169-180, 1978.
[10] R. 1. Rivest, A. Shamir, and 1. M. Adleman. A method for obtaining digital signatures and public-keycryptosystems. Common. ACM, 21(2):pp.120-126, 1978.
[11] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009, www.crypto.stanford.edulcraig.
[12] C. Gentry, "Fully homomorphic encryption using ideal lattices", In M. Mitzenmacher, editor, SIOC, pp.169- 178.ACM,2009.
[13] M. Tebaa, S. EI hajji, Abdellatif EI ghazi,"Homomorphic Encryption Applied to the Cloud Computing Security" ,World Congress on Engineering (WCE) Vol. 1, July 2012.
[14] B. Hayes, "Alice and Bob in Cipherspace", AmericanScientist, Vol. 100, pp. 362-367, Sep-Oct 2012,www.americanscientist.org
[15] C. Gentry, "Computing Arbitrary Functions of Encrypted Data", ACM, Vol. 53 Issue 3, pp. 97-105, March 2010
[16] M. Gomathisankaran , A. Tyagi , K. Namuduri"HORNS: A Homomorphic Encryption Scheme for Cloud Computing using Residue Number System", CISS, March 2011.
[17] D.x. Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data", In Proceedings of 21 st Symp. on Security and Privacy (S&P), Berkeley, California, May 2000, pp. 44-55. IEEE Computer zociety, Los Alamitos, 2000.
[18] R. Curtmola, 1. A. Garay, S. Kamara, R. Ostrovsky, Searchable symmetric encryption: improved definitions and efficient constructions", In Proceedings of 13th ACM Conference on Computer and Communications Security (CCS '06) , pp. 79-88, 2006.
[19] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persian, "Public key encryption with keyword search", In EUROCRYFI 2004. LNCS 3027, pp. 506-522.Springer, Heidelberg, 2004.
[20] G. D. Crescenzo, V. Saraswat, "Public key encryptionwith searchable keywords based on Jacobi symbols", In Proceedings of the 8th International Conference on Progress in Cryptology (INDOCRYPT'07), Springer-Verlag, Berlin, Heidelberg, pp. 282-296, 2007.
[21] H.S. Rhee, J. H. Park, W. Susilo, D. H. Lee, "Improved searchable public key encryption with designated tester". In ASIACCS, pp. 376-379. ACM, New York, 2009.
[22] S. Kaur, "Cryptography and Encryption In Cloud Computing", VSRD International Journal of CS & IT, Vol.2 (3), pp. 242-249,2012.