Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL HARDWARE PARAMETERS BASED CLOUD DATA ENCRYPTION AND DECRYPTION AGAINST UN-AUTHORIZED USERS

[1] KAVURI K S V A SATHEESH, [2] GANGADHARA RAO KANCHERLA,
[3] BASAVESWARARAO BOBBA
[1]Research Scholar, Department Of CSE, Acharya Nagarjuna University, Guntur, AP,India.
[2& 3] Department Of CSE, Acharya Nagarjuna University, Guntur, AP,India.
E-mail: [1] kns9@live.com

ABSTRACT

Now-a-days, there is a revolutionary trend to use cloud services, so more customers are attracting to use public cloud storage. Data storage outsourcing to cloud storage servers is an emerging trend among many firms and users. To relieve from the burden of storage management, broad data access with independent geographical locations and economizing of expenditure investment on software, hardware and maintenance, most of the organizations are outsourcing their data management operations to external service providers. The most attractive part of the cloud computing is the computation outsourcing with its uniqueness, which is becoming the major research area and also getting paid more attention and interest from both academia and industry. As research is progressing day-by-day, obstacles of cloud computing are getting into the focus of vision, simultaneously few challenges are getting solved, and few solutions are better optimized. Among the new born or existing, the challenge which is in most limelight always is security of the outsourced data. Consequently data owner neither have any control on hosted data nor on hosted data centers. Number of techniques addressed this problem, to ensure data security and integrity hosted in cloud. But all of them have their own limitations. In this paper, we propose a new model of CP-ABE, which uses hardware parameters such as cloud instances, server configurations are used in the setup, key generation, encryption and decryption phases.

Keywords: *Attribute-based encryption, Cloud Parameters, CP-ABE, KP-ABE, Cloud Security, Outsourcing Computation.*

1. INTRODUCTION

Cloud computing is a factious computing paradigm which provides various computing resources dynamically through internet. Cloud computing provides an easy way to start a new organization to conduct their businesses over the internet or managing large scale databases by giving easy and cheap self maintained infrastructure to run their own applications. At the same time, cloud Computing [1] faces lot of issues and those issues are still in infant stage. Those problems need to be solved to attract new customers to start their operations and spread across the globe. Numerous IT vendors are promising to offer computation, storage and application hosting services and to provide coverage across the continents cutting different time zones, offering service level agreement (SLA) backed performance and uptime promises for their services.

Cloud computing enables the clients to save their information on a remote server via the internet and make use of different other models provided by it such as Infrastructure as a service, Software as a service and platform as a service. In modern cryptography, the security of the cipher is heavily depending on the secrecy of one's cryptographic key utilized by the cipher. Obviously, one of the most secure techniques [2] to do this is to have the key in a single well-guarded location. However, when the ***well-guarded*** location is compromised, the system fails completely. Hence, the other extreme would be to distribute the secret at multiple locations. However, this type de-centralized approach raises the vulnerability to failure and also makes the work of these very potential attackers a lot simpler.

The transmission of un-encrypted data over a third party is a risky task as well as insecure. The

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cloud computing framework was designed [2] to store large volumes of data belonging to the data owner and protects the data from unauthorized access. Cloud resources suffer with many security issues that affect the encrypted data confidentiality from the un-authorized users, trusted third party and cloud service providers. Cloud users using the encrypted cloud services to protect their important information in the cloud environment are increasing day-by-day. The sensitive data must be encrypted before transmitting over the open communication environment like internet. Cloud data outsourcing through un-authorized clients and distributed systems are exponentially increasing cloud hardware and software resources consumption. Major issue is trust between data owners and cloud providers. By giving physical control to the cloud, how the data owners will secure their data and reserve its privacy is a key part. Classical schemes do not have any complex policies and the sender must know all the public keys of the receiver.

Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on demand mode. In cloud storage systems, a user may hold attributes issued by multiple authorities and the owner may share data with users administrated to different authorities. Some CP-ABE schemes have been proposed for such multi authority systems. However, due to the inefficiency of computation, they cannot be directly applied to construct the data access control scheme. Basically, there are two operations in access control that require efficient computation, namely decryption and revocation.

Data access in cloud storage systems is not static, as employees are hired/fired or promoted/demoted, it will be necessary to change the attributes of users. Third party cloud servers are vulnerable to different type of message integrity attacks. Traditional message integrity algorithms [3],[4] depend on the file size, hash size and security parameters as shown in figure 1. To guarantee the security of attribute revocation, there are two requirements: 1. Backward Security 2. Forward Security. To achieve these two requirements, a trivial method is to re-encrypt all the data. But it incurs a high computation overhead as the amount of data is massive. Attribute-based encryption, recently invented one-to-many public-key cryptography, has got the chance to enforce the increase the heterogeneity of access policies for large-scale systems. A novel option [5] is needed for defending against key attacks for ABE. In doing so, the most ideal challenge is how to efficiently conduct tracing activities without being detected through the suspected users.

In modern cryptography, the security of the cipher is heavily dependent on the secrecy of one's cryptographic key utilized by the cipher. Additionally, in the real world, the users and the key distributor would possibly not trust one another. In secret sharing, a secret is distributed and shared across a wide range of users. In classical access control schemes [3],[4],[6] a Central Authority (CA) can control the users to access the sensitive data. Classical attribute based encryption schemes are based on the static parameters which are vulnerable to the attackers.

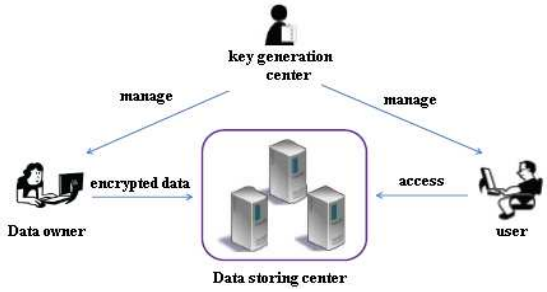


Figure 1: Traditional Message Integrity

1.1 Our Contribution

Cipher policy based encryption schemes consume high computation overhead for each user in the encryption and decryption process. If the number of attributes or policies increases, then the size of the access tree structure increases in the encryption and decryption process. Traditional cipher policy based models are independent of hash integration in the encryption and decryption process. Also, CP-ABE and KP-ABE models initialize ***static parameters*** [6] for key setup and master key generation. Multiuser authentication and integration take more time to encrypt and decrypt large amount of data to the remote cloud server. In this proposed model, hardware parameters from the cloud environment are used to generate the key in setup, encryption and decryption phases. Through this approach, the authorized clients can upload and download data from the cloud environment. Experimental results show that proposed mechanism works well against the traditional cloud encryption algorithms in terms of complexity, time and size are concerned.

In a new model of CP-ABE, each cloud user documents are encrypted using the proposed encryption model. The proposed encryption model considers cloud server instances information for key generation, encryption and decryption process.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Each document is encrypted and stored in the cloud using robust encrypted hash code of the uploaded document. Each document is decoded based on the user's credentials and user's cloud hardware parameters.

1.3 Paper Organization

The rest of the paper is organized as follows. In *section-2*, we review the preliminaries used throughout this paper, *Section-3* describes Related Work subsequently, a proposed new model of CP-ABE and proven in *section-4*. *Section-5*describesPerformance Analysis compared with interactive schemes. Finally Section-6 concludes the paper.

2. PRELIMINARIES

Access Structure In this proposed work, linear policy structure with three parameters are used to find the access matching patterns in the decryption phase. This method takes linear complexity compare to tree structure for policy patterns storage and accessing from the client side to remote server.

Basic Mathematics

Cyclic Group: A *cyclic group* G is a group that can be generated by a single element a, so that every element in G has the form a^i for some integer ***i***. We denote the cyclic group of order ***n*** by Z_n, since the additive group ofZ_n is a cyclic group of order ***n***.

Bi-Linear map: Our model is based on Bi-Linear Map. Bi-Linear maps are used in cryptographic applications. Let $G_0$and G_1be two multiplicative cyclic groups of large prime order *p*. Let *g* be a generator of G_0 and *e* be a bilinear map *e*: G_0 X $G_1 \rightarrow G_1$, with the following properties:

Bilinearity: $\forall\ \mu, \nu \in G_1$and *a, b* $\in Z_p$, we have $e(\mu^a, \nu^b) = e(\mu, \nu)^{ab}$

Non-degeneracy: $e(g, g) \neq 1$, where g is a generator of G_1

One Way Hash Function When we take an input of variable length and then we apply new hash function [7] it produces an output of fixed length 512 bit size hash value for every uploaded encrypted file in the third party cloud server. Applied hash function in one direction only and is denoted as *H(.)*. Let us assume that M is the input of variable length and by applying hash function the output will be ***h*** i.e. *H(M)=h*. It is impossible to obtain the pre-image M from the image *h* ***i.e.*** only authorized users can decrypt by presenting his/her identity along with the hash value.

3. RELAED WORK

Sahai and Water et.al [5] introduced ABE Scheme which defines complex infrastructure. In an ABE scheme user's secret keys and cipher text are labeled with set of attributes. The receiver must obtain the secret key from the Central Authority before decrypting the received cipher text. The receiver can decrypt successfully if there is a match between his secret key and attributes listed in the cipher text. This ABE scheme underwent rigorous research. ABE scheme can classify into Key-Policy Attribute Based Encryption scheme and Ciphertext Policy Based Encryption scheme.

In KP-ABE, a private key is associated with a monotonic access structure like a tree [5], which describes the user's identity, *eg.* (DHAN AND(Ph.D OR TEACHER)) and a cipher text is associated with a set of attributes. An authorized user can only decrypt the ciphertext if and only if his private key is satisfied by the set of attributes in the ciphertext. Data owner does not have any control over the encryption policy. He has to trust the key generators, issues keys with correct structures to correct users. KP-ABE schemes go well with structured organizations with rules [8] about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast. Although the cloud service provider takes different measures to protect data from network hacker, attacker or some unauthorized person, still an open communication environment is always dangerous. So security is always an ongoing research area in cloud. The sensitive information in cloud is secured using the keys of the client attributes such that a valid client who has all the relevant attributes will be able to decode the protected information.

In CP-ABE system [9], user's private-keys of the users are generated with a set of attributes and cipher texts are generated with an access structure will specify the encryption policy. There are several important properties and security issues in *CP-ABE*, such as the efficiency of ciphertext-size, the expressiveness of decryption policy and the chosen ciphertext security. The length of ciphertext has been a mainly concerned issue since the efficiency of bandwidth is very important factor in the communication networks. Considering on the whole, recommended-ABE [10] the size of ciphertext build up on the number of attributes in the access structure. The diction of the access structure is a far-reaching property of CP-ABE.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Jing-Jang Hwang et al. [11] has proposed a model for cloud computing for information security using information encryption and decryption. In this approach cloud server has responsible for data encryption, data decryption and data storage tasks, which takes more processing overhead on the cloud server. The main challenge of this method is, there is no access control mechanism to restrict data on the server. *Green et al.* [8] uses two keys secret key and transformation key are used in his proposed Outsourced decryption method.

Boneh D et al. [12] presented a new HIBE system where the ciphertext size as well as the decryption cost are independent of the hierarchy depth l. Ciphertext are always in their system has three group elements and decryption only by using two bilinear map calculations. Private keys in their system contain only l group elements. *Boneh D et al.* [13] presents homomorphic public key encryption scheme based on finite groups of Composite order that support a bilinear map. To overcome the problems in single authority attribute based system.

Chase et al. [14] proposed a new multi-authority attribute-based encryption system which uses a central authority (CA) and multiple attribute authorities (AAs). The drawback of the system is that every ciphertext is decrypted by the CA, thus reduces the privacy and confidentiality of user's data.

Cheung et al. [15] raised a provably secure CP-ABE scheme to be secured under the standard model. Mainly their scheme supports AND-gate policies which contains negative attributes and also used wildcards in the cipher text policies. A set of attributes are associated with every secret key and for every cipher text is associated with access structures on attributes.

Goyal et al. [16] proposed a scheme for fine-grained sharing of encrypted information that it has the tendency to developed Key-Policy Attribute-Based coding. In that, attributes and personal keys are related to access structures that manage the cipher texts that the user is ready to rewrite. It didn't hide the set of attributes underneath that the information is encrypted.

Waters et al. [17] proposed a method; the encrypted data should be confidential even if storage server is un-*trusted*. Then only it frees from collision attacks. Previous ABE systems used attributes are used to define the encrypted data and policies are building into user's keys and a party encrypting data determines a policy for who can decrypt. Almost all the previous schemes are closer to the traditional access methods like Role-Based Access Control (RBAC).

Junzuo et al. [18] raises an Attribute Based Encryption (ABE) scheme to verify the retrieved content. Just it checks whether the retrieved content is modified or not. If the data was changed it does not mention where the data get modified. If the results of the retrieved data content are modified then there is no use of the data where the modified data is present. The major drawback of this approach is needs more computation and storage overhead for checking of the outsourced encrypted data.

4. PROBLEM FORMULATION

A new model of CP-ABE encrypted and decrypted models are shown in the figure 2 and figure 3. The data to be shared should be secured and only for intended users of the group. This can be achieved through data encryption using identity of users which comprises cloud server credentials. This saves the data from un-authorized users and further to protect integrity of the encrypted data, hash value can be computed [7] can be stored on cloud server which may be used for integrity checking by the cloud server. Encrypted data stored in the cloud server can be accessed by producing the user credentials. Then it undergoes integrity checking by calculating the hash value [7] which is cross checked with the hash value stored along with encrypted data on the cloud server. Once the integrity of the encrypted data is sustained, it is decrypted using the cloud server credentials and then finally data is now accessible to the intended users without loss, modifications and retaining its confidentiality.

Setup: Let α, β, γ ,*e* are the parameters taken from Cloud Credential Server with G= $G_\alpha \times G_\beta \times G_\gamma$ .p,q,r are the cloud parameters in Zp. First compute g_p, g_q, g_r are the generators of $G_\alpha, G_\beta, G_\gamma$ respectively. Following algorithm generates setup parameters for the given Total policy pattern (T.P). Given Total policy pattern is divided into three patterns with AND ($\wedge$), OR ($\vee$), *. Algorithm takes Attribute list *Attlist*, Policy list *polilist*, operator's list *oplist* and an operator position list *poslist* as input and generates *hashcodes* of three policy patterns of policy list.

Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

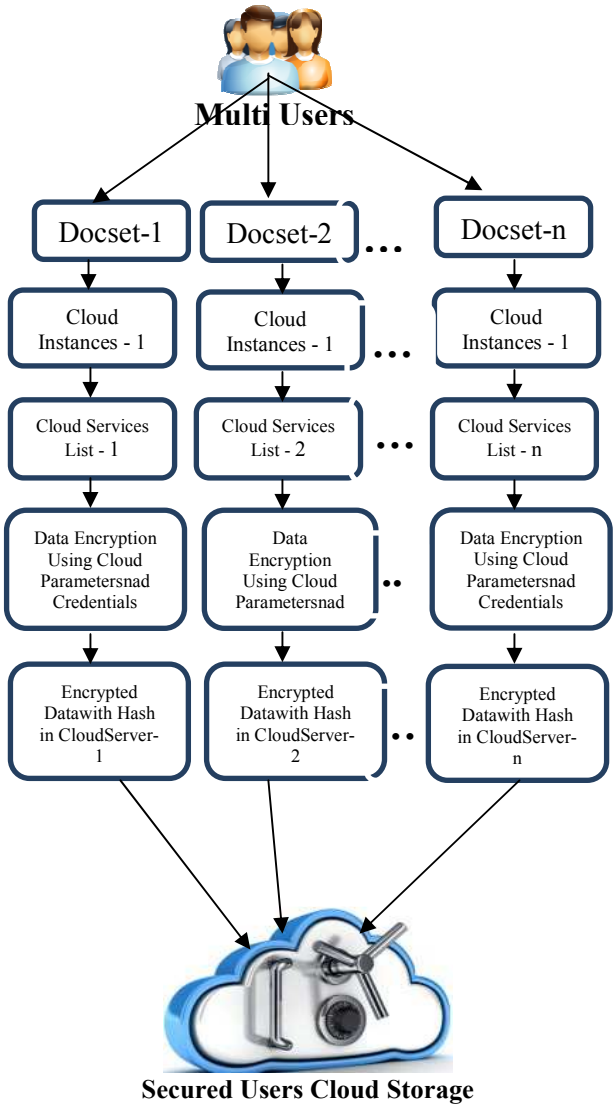


Figure 2: Cloud Credentials And Hardware Information Based Encryption Process.

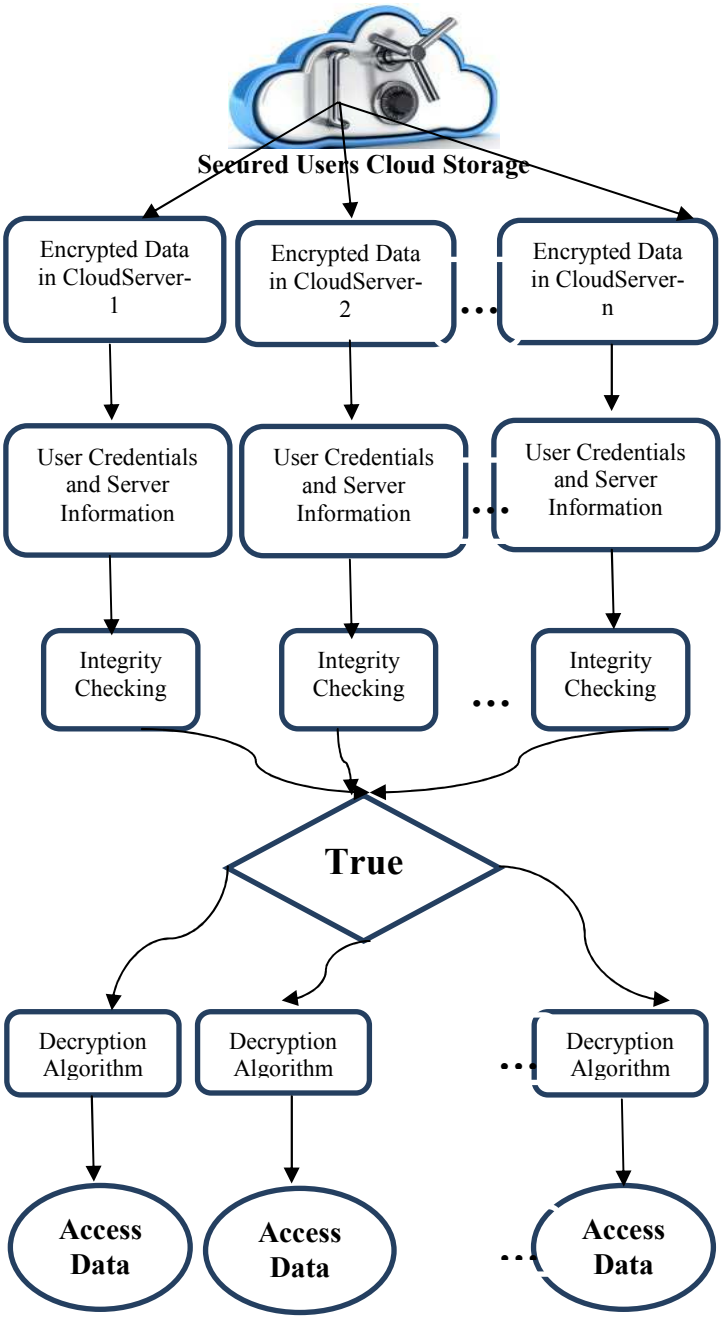


Figure 3:Cloud Credentials And Hardware Information Based Decryption Process

Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Setup Algorithm:

Input:

List:=Polilist, Attlist, Oplist, Poslist, Hardware parameters

Procedure:

oplist[]:=$\{\wedge,\vee,*\}$;

Step1: Read polilist,attlist,oplist and Total Policy Pattern(T.P)

Step2: Identifying the each operator's position in the total policy pattern.

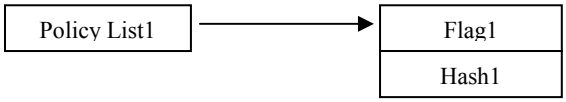
Step3: Copy three pattern policy values in three mapping lists.

Step4: Process AND policy pattern for Hash calculation.

hash[i]=HashAlg(poli1);

hash(pat1):={concat(hash1[i],” “)};

i=0…..poli1.length.



List Mapping of Pattern1

Step5: Process OR policy pattern for Hash calculation.

hash2[i]=HashAlg(poli2);

hash(pat2):={concat(hash2[i],” “)};

i=0…..poli2.length

Step6: Process * policy pattern for Hash calculation.

hash3[i]=HashAlg(poli3);

hash(pat3):={concat(hash3[i],” “)};

i=0…..poli3.length

$H_1^{'}$=HextoDecimal(hash(pat1));

i=0…pat1.length.

$H_2^{'}$=HextoDecimal(hash(pat2));

i=0…pat2.length.

$H_3^{'}$=HextoDecimal(hash(pat2));

i=0…pat2.length.

$S^{'} = H_1^{'} + H_2^{'} + H_3^{'} + \text{hardwareparams};$

Public Key

$:=\{S^{'}, g_p, g_q, g_r, G_\alpha, G_\beta, G_\gamma, H_1^{'}, H_2^{'}, H_3^{'}\};$

Master key :=$\{\alpha,\beta,\gamma\}$; known to T.A

Key Generation: Key Generation algorithm will take set of attributes Policy pattern hash values as input and returns Secret key as output. Each user is associated with secret key and it will be generated using three pattern keys as

$K_{1,i} = g_p^{1/(S^{'}+\alpha)}$; i=0…..pat1.length;

$K_{1,j} = g_q^{1/(S^{'}+\beta)}$; j=0…..pat2.length;

$K_{1,k} = g_r^{1/(S^{'}+\gamma)}$; k=0….pat3.lenght;

Secret key :={TP, Hash(pat1), Hash(pat2), Hash(pat3), $K_{1,i}, K_{1,j}, K_{1,k}$ };

Encryption Process:

Input: Public key, Policy Patterns, Message;

Procedure:

Public Key:=$\{S^{'}, g_p, g_q, g_r, G_\alpha, G_\beta, G_\gamma, H_1^{'}, H_2^{'}, H_3^{'};\}$;

Calculations:

$C_0 = g_p^{S^{'}}$;

$C_0^{'} = g_p^{(\alpha+\beta+\gamma)}$; where $\alpha,\beta,\gamma \in G_\alpha, G_\beta, G_\gamma$;

$C_{1,i} = g_p^{H_2^{'}+H_3^{'}}.g_p^{H_1^{'}+\alpha}$ i:=0……pat1.length;

$C_{2,j} = g_p^{H_1^{'}+H_3^{'}}.g_p^{H_2^{'}+\beta}$ j:=0……pat2.length;

$C_{3,k} = g_p^{H_1^{'}+H_2^{'}}.g_p^{H_3^{'}+\gamma}$ k:=0……pat3.length;

Encryption algorithm encrypts the message using policy pattern structures. Algorithm uses three patterns with homomorphic encryption and decryption process. Additive and Multiplicative homomorphism takes two inputs and generate secure encrypted values as output. Homomorphic encryption and decryption uses $C_0, C_0^{'}$ as an input.

Additive Homomorphic Encryption

$$Enc(M_1 + M_2) = Enc(M_1) + Enc(M_2);$$

Multiplicative Homomorphic Encryption

$$Enc(M_1.M_2) = Enc(M_1).Enc(M_2);$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$M_1 := C_0$;

$M_2 := C_0^{'}$;

Enc(M_1):=Enc(C_0)=($C_0 + \gamma * \beta$)mod n

Where n= $\alpha * \beta$;

Enc(M_2):=Enc($C_0^{'}$)=($C_0^{'} + \gamma * \beta$)mod n

Where n= $\alpha * \beta$;

Enc(M_1+M_2) :=Enc($C_0 + C_0^{'}$)

:= Enc(C_0)+Enc($C_0^{'}$);

:= ($C_0 + \gamma * \beta$) mod n +

($C_0^{'} + \gamma * \beta$) mod n

Enc(M_1.M_2):=Enc($C_0.C_0^{'}$)

:= Enc(C_0).Enc($C_0^{'}$);

:= ($C_0 + \gamma * \beta$)mod n +

($C_0^{'} + \gamma * \beta$) mod n;

Cipher Text CT =

$\{TP, H_1^{'}, H_2^{'}, H_3^{'}$,M.e($Enc(M_1 + M_2)$,

Enc($M_1.M_2$)),{$C_{1,i}, C_{2,j}, C_{3,k}$},C};

Cipher Text CT is publicly available to all the attribute policy holders. This CT will be decrypted only those users who have exact policy matching patterns.

$$e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} \cdot \prod_{i=1}^{n} e(C_{1,i}, K_{1,i}) \cdot \prod_{j=1}^{n} e(C_{2,j}, K_{1,j}) \cdot \prod_{k=1}^{n} e(C_{3,k}, K_{1,k})$$

$$\Rightarrow \text{M. } e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} .1.1.1$$

$$\Rightarrow \text{M. } e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$$

Now Based on the user entered policy A ***and*** D parameters may vary as

If user entered policy is in pattern1 then

$$D_{1,i} = g_p^{\alpha} \; A_{1,i} = g_p^{\beta+\gamma}$$

If user entered policy is in pattern2 then

$$D_{2,j} = g_p^{\beta} \; A_{2,j} = g_p^{\alpha+\gamma}$$

If user entered policy is in pattern3 then

$$D_{3,k} = g_p^{\gamma} \; A_{3,k} = g_p^{\alpha+\beta}$$

If the user entered policy is in patter1 then decryption follows:

Decryption:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$/e(C,D*A)

:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$/e($g_p^{S'}, g_p^{\alpha}.g_p^{\beta+\gamma}$)

:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$/e($g_p^{S'}, g_p^{\alpha+\beta+\gamma}$)

:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$/e($g_p, g_p$)$^{S'(\alpha+\beta+\gamma)}$

:= M

Similarly, other policies can decrypt the original message to M.

5. PERFORMANCE ANALYSIS

5.1 Experimental Setup

To assess the proposed model, the implementation of the model and experiments are conducted in cloud environment. The code is written in JAVA Language. All the computations involving the construction are performed in the real time Amazon cloud instances and client configurations as Intel(R) CPU 2.13GHz, 1 GB RAM, and the minimum Operating System platform is Microsoft Windows-7 Professional (SP2). The prototype requires third party libraries cp-abe, abe, amazon aws ,jama.etc.

5.2 Efficiency Analysis

By using the experimental setup, implemented prototype model performance evaluation is obtained. The performances are evaluated in terms of the encryption and decryption time, hash time, upload and download time, key size. It is analyzed in comparison with *CP-ABE, KP-ABE, FH-ENCRYPTION* in all terms.

Table 1: Encryption and Decryption time with other existing schemes

Algorithm	Data Size (KB)	Hash Time (ms)	Encryption Time (ms)	Decryption Time (ms)
CP-ABE	>1000	4465	6788	5624
KP-ABE	>1000	5287	5478	5197
FH-Encryption	>1000	6554	7664	6922
Our New Model	>1000	2431	3714	3698

Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

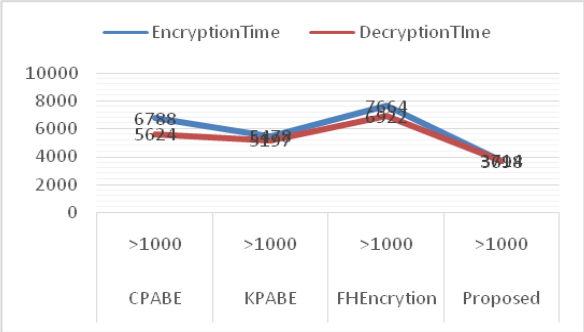


Figure 4: Encryption and Decryption Time Computation in proposed prototype with other existing schemes

Table 2: Irrespective of Upload and Download Time with varying key size (bits).

Algorithm	Cloud instances	Key size	Upload Time	Download Time
CP-ABE	3	512	5355	6455
KP-ABE	3	512	7412	6122
FH-Encryption	3	512	6745	5898
Our New Model	3	1024	4844	4623

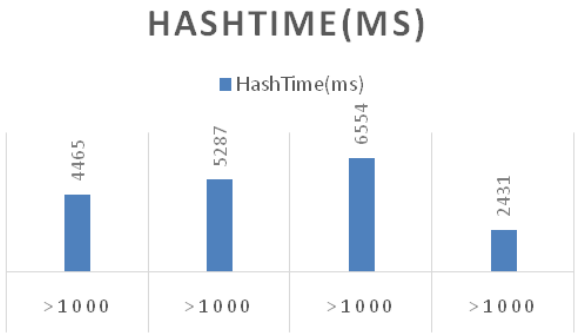


Figure 5: Hash Computation in proposed prototype with other existing schemes

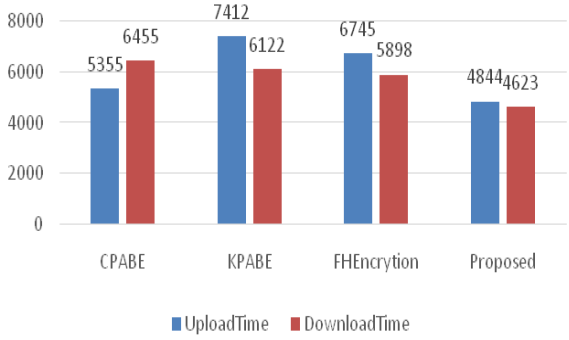


Figure 6: Upload and Download Time Computation in proposed prototype with other existing schemes

REFRENCES:

[1] Taeho Jung; Xiang-Yang Li; Zhiguo Wan; Meng Wan, "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption," *Information Forensics and Security, IEEE Transactions on* , vol.10, no.1, pp.190,199, Jan. 2015 doi: 10.1109/TIFS.2014.2368352.

[2] Chun-I Fan; Huang, V.S.-M.; He-Ming Ruan, "Arbitrary-State Attribute-Based Encryption with Dynamic Membership," *Computers, IEEE Transactions on* , vol.63, no.8, pp.1951,1961, Aug.2014.doi: 10.1109/TC.2013.83.

[3] B.C. Neuman and T. Ts'o, "Kerberos: An Authentication Sewice for Computer Networks," IEEE Comm. Magazine, vol. 32, no. 9, pp. 33-38, Sept. 1994.

[4] N.P. Smart, "Access Control Using Pairing Based Cryptography," CT-RSA '03: Proc. RSA Conf. The Cryptographers' Track, pp. 111-121, 2003.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3494. Heidelberg, Germany: Springer-Verlag, 2005, pp. 457–473.

[6] Boneh D., Gentry C., and Waters B., "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," in Proceedings of the 25th Annual International Cryptology Conference, USA, pp. 258-275, 2005.

[7] Kavuri. S.K.S.V.A.; Kancherla, G.R.; Bobba, B.R., "Data authentication and integrity verification techniques for trusted/untrusted cloud servers," Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on , vol., no., pp.2590,2596, 24-27 Sept. 2014.doi: 10.1109/ICACCI.2014.6968657.

[8] M. Green and S. Hohenberger, "Blind Identity-Based EncryptionandSimulatable Oblivious Transfer," ASIACRYPT '07: Proc. 13thInt'l Conf. Theory and Application of Cryptology and InformationSecurity: Advances in Cryptology, K. Kurosawa, ed., pp. 265-282,Dec. 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] Bethencourt, J.; Sahai, A.; Waters, B., "Ciphertext-Policy Attribute-Based Encryption," *Security and Privacy, 2007. SP '07. IEEE Symposium on* , vol., no., pp.321,334, 20-23 May 2007 doi: 10.1109/SP.2007.11.

[10] Jinguang Han; Susilo, W.; Yi Mu; Jianying Zhou; Man Ho Allen Au, "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," *Information Forensics and Security, IEEE Transactions on* , vol.10, no.3, pp.665,678, March 2015. doi: 10.1109/TIFS.2014.2382297.

[11] Jing-Jang Hwang; Hung-Kai Chuang; Yi-Chang Hsu; Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," Information Science and Applications (ICISA), 2011 International Conference on , vol., no., pp.1,7, 26-29 April 2011.

[12] Boneh D., Boyen X., and Goh E., "Hierarchical Identity Based Encryption with Constant Size Ciphertext," in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Denmark, pp. 440-456, 2005.

[13] Boneh D., Goh E., and Nissim K., "Evaluating 2- DNF Formulas on Ciphertexts" in Proceedings of the 2nd Conference on Theory of Cryptography, USA, pp. 325- 342, 2005.

[14] M. Chase, "Multi-authority attribute based encryption," in Proceedings of the Theory of Cryptography Conference, pp. 515–534, 2007.

[15] L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Computer and Communications Security,2007, pp. 456–465.

[16] V.Goyal, O. Pandey,A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security, 2006, pp. 89–98.

[17] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53–70.

[18] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng "Attribute-Based Encryption With Verifiable Outsourced Decryption" in IEEE transactions on information forensics and security, vol. 8, no. 8, August 2013.