TTSM: Trust Threshold Security Model for User Assured Security in Cloud Computing

Harsh Saki
Research Scholar, Dept. of CSE
LNCT, Ujjain Road Indore
(M.P), India

Jitendra Dangra
Associate Prof., Dept. of CSE
LNCT, Ujjain Road Indore
(M.P), India

ABSTRACT
Internet and networks applications are growing very fast & hence the importance and value of the exchanged data over internet are increasing. Cloud computing technology is used to handle such scalable growth in data and the users. It supports the dynamic elasticity for increased number of application, processes, users and data. But due to its infrastructure environment various security issues raises as the data resides at remote locations. Thus the trust value of the user on such distant location is very less. Thus to do the things effectively and more securely at third party locations of cloud service provider the user must store its data in encrypted form. Information Security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security systems. Among all the encryption techniques attribute based encryption (ABE) is getting popularity day by day. As the most important factor of encryption is key thus the new key generation based on attribute based encryption mechanism is used in this work. It will control the issues related to fine grained access control and data isolation. Like most preceding mechanism, the new scheme added supports for secure and efficient dynamic operations on data blocks, counting: data update, delete and append. Thus this work proposes a novel Client end trust threshold security mechanism (TTSM) using behavior based encryption for achieving the better results. This work focuses on the application area of cloud storage platform for user satisfaction.

This model gives a unique stack based solution for achieving the end user security. According to ABE the user can be able to decrypt the file on the basis of the file attribute, which is different for each file & depends on the user category. In this methodology the attribute can be identified from the user attribute table. This attribute table is dynamic in nature & whose values are passed in the table after a pre calculation of trust & user modeling. At initial level our proposed approach seems to be better secure data access in comparison to other existing methodology.

Keywords
TTSM (Trust Threshold Security Model), ABE (Attribute Based Encryption), Cloud Computing, Third Part Security, Trust Model, Verification, Access Control

1. INTRODUCTION
Internet and networks applications are growing very fast.
In this data is a valuable assets for client considering personal, commercial, social and health information often sharable respective to time and requirement. Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure. As a result, Cloud adoption is spreading rapidly and represents a new opportunity that companies should not ignore given its profound impact. The lack of processing time and storage capacity or to save resources cost, data should be stored at third place known as cloud providers. However, there have been wide privacy concerns as data could be exposed to those third place servers and to unauthorized parties. To assure the client control over access to its own information's it is a promising method to make data unreadable and non-interpretable form as likewise example of personal health records shown [1]. As the importance and value of the exchanged data over the network are increasing, concern related to information security issues is also getting denser and abrupt. Any loss or threat to information can prove to be great loss to the organization. Data storage on cloud is provided by the service provider. Storage of this data on un-trusted storage makes secure data sharing a challenging issue. Confidentiality of the data on this unknown environment can be achieved via various access control & encryption mechanism. Conventional encryption standards & techniques will only provide the basic things of security which can be breached. Encryption technique plays a main role in information security systems. Among all the encryption techniques attribute based encryption (ABE) is getting popularity day by day. However, moving the infrastructure and sensitive data from trusted domain of the data owner to public cloud will pose severe security and privacy risks. Attribute-based encryption (ABE) is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control [2].To achieve fine grained access control & effective data access control policies attribute based encryption is well defined standard. There are various encryption algorithms available like AES, Tripple DES, blowfish etc which will also provide the encryption based security but in a general manner. It is a burdensome of user to deal with their complex processes. For further improvements in existing methodology of security focus is made on attribute based encryption with trust value. Solution needs to be defined for developing the basic utility of applying attribute based encryption (ABE) for data sharing on un trusted storage & servers [3]. This kind of sharing also required the mechanism for data retrieval having this ABE type of encryption. Thus this can be handled by searchable encryption for secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage [4]. For secure data access the client must be sure about the process used for this type of encryption but in cloud platform everything is provided by cloud. Thus the satisfaction of security at user level is not provided by any cloud. According to ABE the user can be able to decrypt the file on the basis of the file attribute, which is different for

each file & depends on the user category. In this methodology the attribute can be identified from the user attribute table. This attribute table is dynamic in nature & whose values are passed in the table after a pre calculation of trust & user modeling. Thus this work proposes a trust based model through behavior based encryption for achieving the better results. It also covers the application area of cloud storage platform for user satisfaction by giving a unique stack based solution for achieving the end user security. At initial level our proposed ABE based TTSM approach seems to be better secure data access in comparison to other existing methodology.

2. BACKGROUND

Cloud computing methodology is a conceptual framework for providing effective and low cost computation as a service to the users. It is a promising computing model, enables users to distantly store their data in a cloud, so as to have the benefit of services on-demand. Migrating data from the user side to the cloud provides great ease to users, since they can access data in the cloud anytime and anywhere, using devices, without caring about the capital investment to deploy the hardware infrastructures [5]. Here resources are used in shared manner like shared software's, infrastructure and development platform. It provides all the above features as utility measured services. Storing the data at remote locations through cloud offers great convenience. While these Internet-based on-line services do provide massive amounts of storage space and customizable computing resources, the user loses control of the data. In order to secure such data encryption standards can be used. The problem that arises now is that while data can be sent to and from a cloud provider's data centre in an encrypted form; continuing work is not possible without decryption. During the storage of the data at third place client not sure about the information stored safely. There possibility of different attacks during the storage and retrieval of data from third location. Data may be tampered and accessed by unauthorized user or external attacker. To make safety and maintain privacy it needs number of security mechanisms. The loss of security control on data at cloud is the major issues related to cloud data security. This occurs because of lack of collaboration between cloud and user. Later on its solution is proposed by NIST-FISMA framework which follows all the standard of security. It improves the trust of user on services provided cloud [6]. Some of the more security standards is been proposed in [7] for third party access control. Briefly it will be described the related risk. It raises a hand on its policies for strong security, privacy and trust concerns. It assures the safe data storage by provider, privacy, law and governance, attack resistant approaches supported by revocable ABE. The above mentioned work will also assess how cloud providers can earn their customers trust and provides better security, privacy and reliability.

It identifies problem that realized at client end during the retrieval and storing of information at cloud. Here might be any attacker or unauthorized person or attacker present to tamper or access the data before data reach at client or cloud providers. Attacker may be influence client personal or financial life so here need to prevent from this kind of activity need lot of techniques are used to during data storage. However, the main purpose of the access control based cryptography is not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation for cloud based data records. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. For any cloud cryptographic storage must satisfy the properties of confidentiality and integrity as given in [8]. Presently continuous researches on the new cryptographic algorithms are going on. Access control with a large and dynamic set of users, for objects cannot easily be based on identities. The conditions under which access to an object is granted need to take into account information like the context and the history of a subject is given by these mechanisms of attributes based encryptions. Due to these shortcomings of traditional access control mechanisms, cryptographically enforced access control receives increasing attention.

Attribute Based Encryption

It is used for enhancement of cloud security models which is achieved by using user attributes as parameters for confidentiality. Here an attribute is a property or feature that a subject may have. At some point in time, any subject may become eligible for a particular attribute, meaning that it now has the respective property or feature. It then receives a token from a trusted party called attribute authority that testifies his eligibility and can be used by him to prove that he has the property or feature that the corresponding attribute represents. An attribute is usually represented as a string. In this the ciphertext and user keys are associated with policies that describe the user that is allowed to access the encrypted information. Such encryption and policy enforcement is mainly using the owner's category key rules to enhance the storage security [9]. Specifically, in Key-Policy ABE (KP-ABE) ciphertext are encrypted with a set of attributes and each user's secret key is associated with a policy describing which ciphertext he can decrypt [10]. The attribute based encryption for generating the ciphertext is an extraordinary approach in which user profiles plays a vital role. It gives the access policies for encrypted information. These are mainly used to only generate the key attributes associated with each user & its type of data which it might be access every time. Key Generated Policy Attribute for Encryption (KGPAE) ciphertext are encrypted with a set of attributes and each user's secret key is associated with a policy describing which ciphertext he can decrypt. Such a policy is a predicate over the set of attributes, usually formulated as a Boolean formula. Thus to make the system more reliable client needs to make some security trusted deals with its data. Actual deployment of cloud computing services is not reliable as they claim because the existing security model doesn't work after migration of services to clouds. This migration follows multitenant model and cloud computing is bringing remarkable impact on information security fields. Such issues generated because of following features of cloud [2]:Dynamic Scalability, Service abstraction and Location Transparency.

The proposed TTSM approach is suggesting a novel method to generate an effective key based on user attributes and then applying the encryption. It works on a trust model of for each user which is stored at third place. This trust model gives the threshold up to which access can be granted and below which threat can be sensed. Taking the key of attribute values should be generated in secure environment. It can be only used once and will always store in encrypted form always for further references. Thus by applying the above efforts effectively security of cloud data is improved along with its user trust.

3. RELATED STUDY

There is a critical need to securely store, manage, share and analyze massive amounts of data and to improve the quality of services. Because of the critical nature of the applications, it is

important to secure clouds. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. The issues are organized into several general categories: trust, architecture, identity management, software isolation, data protection, and availability. Because cloud computing has grown out of an incorporation of technologies, including service oriented architecture, virtualization, utility computing, many of the security issues involved can be viewed as known problems cast in a new setting. Cloud computing is a complex system and is not secure by nature. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem. The combinations of various existing and new technological strategies must be used together for protecting the total cloud computing system.

TAAC (Temporal Attribute based Access Control) a user access control is given in [11]. It is an efficient data access control scheme for multi-authority cloud storage systems, where the authorities are independent from each other and no central authority is needed. TAAC can efficiently achieve temporal access control on attribute-level rather than on user-level. Moreover, different from the existing schemes with attribute revocation functionality, TAAC does not require re-encryption of any ciphertext when the attribute revocation happens, which means great improvement on the efficiency of attribute revocation. TAAC is highly scalable in nature.

Similar to that [12] present a temporal attribute based encryption (TABE) scheme to implement temporal constraints for data access control in clouds. This scheme has a constant size for ciphertext, private-key, and a nearly linear-time complexity. It has four algorithms named as setup, generate key, encrypt & decrypt. At initial level its security model seems to be good & effective.

Continuing the above solution DAAC is proposed in [13] which is distributed access control in clouds, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records. Thus, a single key replaces separate keys from owners. Owners and users are assigned certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud. Thus various approaches are suggested based on runtime environment to improve the user attribute based encryption performance.

Cloud computing should provide strong user access control which powers the licensing, certification, quarantine and other aspects of data management. Most prominent way to make encryption standard more effective and satisfy the cloud needs is to modify them. Various approaches suggested changes to algorithms like RC5, DES, AES, and Blowfish to catch up with the existing needs of cloud security. So before selecting them some needs to make better comparisons between those as given by the [14]. The users do not know what position the data and do not know which servers are processing the data. It also does not have any information about network used for transmitting the data due to its scalable & flexible nature. The different locations will also sustain various security laws about the data privacy in a confidential way. Some of the authors focus their working on processing the encrypted information without making the use of decryption key. It also makes the system more faults tolerant and reliable. Thus such system is satisfying the cloud needs. It can be achieved through arbitrary function in fully Homomorphic encryption [15].

Taking forward to above research domain of homomorphic encryption various authors had proposed many new mechanisms to improve its performance. One of them is Secure Data Sharing (SDS) framework using homomorphic encryption and proxy re-encryption schemes which prevents the leakage of unauthorized data when a revoked user rejoins the system [16]. The framework is secure under the security definition of Secure Multiparty Computation (SMC) and also is a generic approach - any additive homomorphic encryption and proxy re-encryption schemes can be used as the underlying sub-routines. In addition, it also modifies the underlying Secure Data Sharing (SDS) framework and present a new solution based on the data distribution technique to prevent the information leakage in the case of collusion between a user and the Cloud Service Provider.
In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others [17]. But the most important between them is security and how cloud provider assures it. Apart from that so many other security issues related to cloud can be sorted out by any defined preemptive mechanism. Some of these issues and their solutions are given in [18, 19]. Hence it is identified that to provide user level security in accordance with type of data usage the access control mechanism can be improved. So it can be solved by using revocable ABE techniques. It uses multiple policies for ciphertext creation and storage regarding the credential information as given in [20]. At the initial level of our research the approach seems to be effective.

4. PROBLEM IDENTIFICATION

These two working areas are the origin for the greatest concern of organizations transforming to cloud services. Security can be guaranteed and the service will be available always. In existing scenarios the cryptography – exclusively based on trust and could be implement as a cloud service. It has many options and areas related to the security, trust and availability which cannot be fully assured. As of the viewpoint of data protection, which has forever been an significant aspect of quality in cloud computing. Some the identified issues in that are:

Data Protection

For those data which is stored on the service provider of the cloud side must not be accessed or changed by unauthorized user or intruders. In addition, the service provider must present the assurance of data integrity for the user of client side. Therefore, an enterprise shall evaluate the risk of storage damage, data loss, and networking security on the cloud side as they plan to adopt the application of cloud computing.

Cloud Data Encryption

One of the fundamental security tools for protecting data in multitenant environments is encryption. When implemented properly, cloud encryption can allow you to protect data when you don't have full control of the environment. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

The primary objective of this work is stated as:

- To develop a security framework for cloud that can work on cross platform.
- To propose a novel behavior based access control & encryption (BBACE) model for providing Security as a Service in cloud platform
- To propose a new encryption standard for cloud computing
- To clearly isolate the user access & data transfers.
- To focus which security threats can be unsafe to cloud computing and how they can be avoided.

5. PROPOSED TTSM APPROACH

The purpose of this proposed work is to identify the unauthorized access of data; cloud made unreliable for client and various issues related to cloud storage with customized client end security services is rising. It provides the virtual security mechanism as a service. It solves the problem raises due to remote data locations. The study also develops an approach to implement above mentioned service on real cloud platform. It meets all the security requirements of deploying configuration of security as a service. To provide reliability on cloud, an approach TTSM is advised at client end to make safe and secure storage of data. The proposed approach is stack of multiple protections layer that deals with clients' data to providing overlapping layers of authentication, behavior analysis and make data unreadable form using behavior based encryption mechanisms. The suggested TTSM approach consists of several phases. Firstly to coated authentication layer to the data by providing identity of users and verifying the claimed identity. Secondly to coated behavior analysis layer to the data by regular observing the activities of users on the basis of historical property. Third phase is to coated behavior based encryption layer by converting client data into encrypted data and send for storage on the cloud. Figure 3 depicted suggested approach.

The proposed model for cloud security is based on trust calculation of user access control on the basis of their behavioral elements. This trust model in combination of behaviour based encryption is satisfied all the constraints. Various other existing encryption algorithms are studied but can't be able to solve the client level security problem. All the existing security mechanisms are only up to the provider's level & consumer doesn't know anything about the security.

The proposed work is providing a novel method which gives priority to client systems and make their data secure by taking their behavior elements as a key for encryption. This can be achieved by a known key cryptography method named as public key infrastructure with attribute values of user and data working as a key. It also added an additional padding bit with modified hash function to make the cloud more secure & reliable.

TTSM Model Description

TTSM is a trust model based fine grained access control method for improving the protection of storage on cloud. The proposed architecture is shown in figure below. In this when a user wants to access the data area a request has to be generated to any third party server which verifies its integrity from its databases & having a specified trust value in case of each user. Third party auditor revokes the reply of the user with its service ID having a unique kind of certificate is given to access the data. Same certificate is also been provided to cloud service provider. When user demand an access to cloud this token is get verified and the permission is granted. During the cloud storage client needs to work on the trust model. It depends upon the different attribute elements of their own data elements. It also gives the basic area of access control mechanism. In this access mechanism user can store and retrieve its own data in an encrypted form having attribute elements works as a key for this.

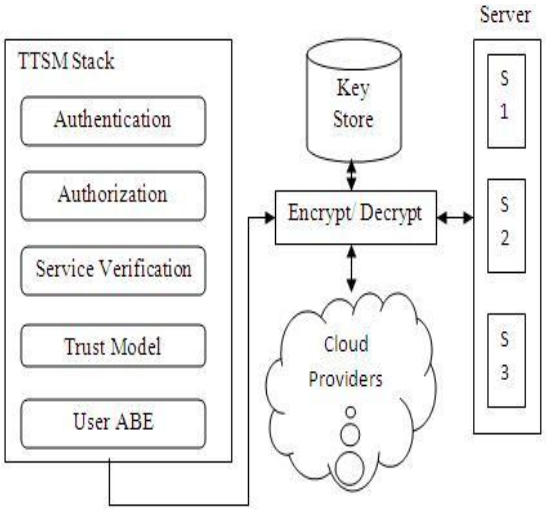

Figure 1: Process Model of Proposed TTSM Approach

At the time of user request to its stored data the encrypted data can only be decoded after applying the key which can be generated by user behavioral elements and its access areas like credential information, existing history of content type, session information, number of failed logins, timestamp, time of working session, type of service used, and number of time password changed. From these values a trust model is derived which prefers the access of data to user or not. If the key element matches it will be shown or else again trust is calculated. Initially the trust value is zero but as the process increases it value is also incremented. At the time of encryption these values can generate different key pairs like K1, K2, K3, and K4 to make the final key K. These K can be passes at the time of encryption and stored in a key database for next time decryption. The above element will automatically do the encryption without the uses knowledge.

After this step even cloud doesn't knows the type of data which the user had stored in the storage. After this the cloud [provides the user an access ID for a data storage session to the users so as to interact directly with the storage. When the client demanded for its stored data same behavioral element works as a decryption key. After applying such mechanism the problem related to data isolation & incorrect data display to the user is also solved. It is a onetime key. Once the data is successfully retrieved then the key is deleted from the data table. These key store is reside s at the third party location.
Steps Involve in TTSM Design

Step (1) Authentication:

In this the type of user access & file required is achieved through a authentication phase at application server. Initially new user creates the account at server side from which zero trust is calculated which later on incremented as per its uses.
Step (2) Authorization:

The user category & its attribute are authorized from a user database which is stored at third party. This step executed each time when the user demanded the data.

Step (3) Service Verification:
In this step the service provided by cloud is verified in browser & gives an identification value of integrity. It can be achieved by the certificates issues by the trusted third party to both user and cloud provider.

Step (4) Trust Calculation:
In this step each user has to reach a unique trust value which is more that a specific threshold which is defined by the user policies. It gives an insight to user activities which is defined after its trust verification. These step comes under the user behavior analysis through trust model which depends upon its historical data access & type of files required. It is based on user categorization and access control policies.

Step (5) User Attribute Based Encryption:
It is the final process of TTSM in which a specific ABE encryption methodology is used to encrypt & decrypt the file for user access. It is based on above trust & behavior analysis. In this each encryption is done by passing the value of user attribute as a key. In this the size of key is based on number of attribute used.

In this proposed work, an effective and flexible distributed scheme is given with explicit dynamic data support to ensure the correctness of users' data in the cloud with more security. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the certificates and ABE the scheme achieves the storage correctness insurance. AT the initial level of research the approach seems to give effective results in near future.

6. EXPECTED BENIFITS

In order to measure and compare the performances of the proposed BBACE scheme, the work continues to adopt the various comparison metrics, First is key size & generation is very effective and very less in case of existing encryption standard. Second is secure data access mechanism. The work makes the following observations about the proposed work

- Improved security and data access can be implemented in efficient manner. It will also ensure the successful satisfaction of various integrity rules for correctness of data.
- Data isolation and access control can be guaranteed by using access and key policies for various types of user. Policies are used here to define the fine grained access control.
- Dynamic operations on data block are supported like update, delete and append. This mechanism will improve the efficiency of system due to parallel processing of data updations and its encryption.
- New key combination approach is developed to further increasing security through key policy using attribute based encryption. Multiple attribute of user is combined together to generate a new key in this.
- User behavioral elements can be easily calculated which decrease the user effort. It causes reduction of efforts because user doesn't know about its security process, key calculation and data transfer.
-
- Effective trust model is used for continuous monitoring the user behavior. This trust model regularly measuring the user behavior & recognizes any changes in it very soon to prevent any data loss.

7. PERFORMANCE EVALUATION

The security and performance requirements are summarized as follows:

- *Data confidentiality.* Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a record document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.
- *On-demand revocation.* Whenever a user's attribute is no longer valid, the user should not be able to access future record files using that attribute. This is usually called attribute revocation, and the corresponding security property is forward secrecy. There is also user revocation, where all of a user's access privileges are revoked.
- *Write access control.* We shall prevent the unauthorized contributors to gain write-access to owner's record, while the legitimate contributors should access the server with accountability. The data access policies should be flexible, i.e. dynamic changes to the predefined policies shall be allowed, and especially the records should be accessible under emergency scenarios.
- *Scalability, efficiency and usability.* The records system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

8. CONCLUSION

As the number of user is increasing very rapidly the issues related to cloud and data security is also raising its strong presence. It needs to handle carefully to make the system more reliable and fault tolerant. Also as the users data is quantitatively increased the isolation issues is also abruptly gets into existence. Thus some improved mechanism can be designed which provides greater security and user assurance about its data. To resolve the mentioned issues related to data security, client assurance and isolation this work proposes a novel TTSM approach. It modifies the access mechanism through some existing trusted third party which verifies both the user information and service confirmation. It also helps the user to calculate their behavioral element to generate a trust model for attribute based encryption. Same process can come at the decryption time. It also monitors the user working continuously and its value must be greater than a specified threshold. If it is not above that then the user gets logged out. Thus in this way an improved secure data access mechanism can be developed. At the initial level of our work great futuristic results is assured can be handle

9. FUTURE WORK

Taken security as a major concern in this work has generated so many integration issues. While applying the above proposed architecture component must be placed in correcting order for better results. The security breaches identification can be done as a real time entity. Behavior based encryption, access control, data isolation & key handling issues can also be improved effectively by using KMIP protocol standard. Hence some problems and concepts that remain unaddressed can be performed. The implementation of the above proposed mechanism is configured in Aneka 3.0 cloud platform tool in near future.

10. ACKNOWLEDGMENT

The authors wish to acknowledge LNCT administration for their support & motivation during this research. The authors would also like to thank the anonymous referees for their many helpful comments, which have strengthened the paper. Many thanks to all the dignitaries for their discussions regarding the cloud security policies & for producing the approach adapted for this paper.

11. REFERENCES

[1] Ming Li, Shucheng Yu, Yao Zheng, Student, Kui Ren, and Wenjing Lou, ―Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption, in IEEE Transactions on Parallel and Distributed Systems, Vol. xx, No. xx, 2012.

[2] Changji Wang & Jianfa Luo, ―An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length in Mathematical Problems in Engineering Volume 19 , Article ID 810969, 2013..

[3] Shucheng Yu, Cong Wang, Kui Ren & Wenjing Lou, ―Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, in Proceedings of IEEE Infocomm., ISSN: 978-1-4244-5837-0/10, 2010.

[4] Dongyoung Koo, Junbeom Hur & Hyunsoo Yoon, ―Secure and efficient data retrieval over encrypted data using Attribute-based encryption in cloud storage, in Computers and Electrical Engineering Journal of Elsevier, ISSN:0045-7906, doi:10.1016/j.compeleceng.2012.11.002, Vol. No 39, Jan 2013. pp 34–46

[5] Guojun Wang, Qin Liu, Jie Wu & Minyi Guo, ―Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, in Computer & Security Journal of Elsevier, ISSN: 0167-4048, doi: 10.1016/j.cose.2011.05.006, Vol. No. 30, July 2011. pp 320-331

[6] Mohemed Almorsy, John Grundy & Amani S. Ibrahim, ―Collaboration-Based Cloud Computing Security Management Framework‖, in 4th International Conference on Cloud Computing, IEEE Computer Society, ISSN: 978-0-7695-4460-1/11, doi:10.1109/Cloud.2011.9, 2011.

[7] Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta & Manoj Diwakar, ―Effective Ways of Secure, Private and Trusted Cloud Computing‖, in International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 8, Issue 3, No. 2, May 2011.

[8] Seny Kamara & Kristin Lauter, ―Cryptographic Cloud Storage‖, in Microsoft Research Article at http://

[9] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi & P. Samarati, ―Encryption-based Policy Enforcement for Cloud Storage‖, in IEEE Transaction, at Universita degli Studi, di Milano, 2010.

[10] Nishant Doshi & Devesh Jinwala, ―Updating Attribute in CP- ABE: A New Approach‖ in IJCA proceedings of ICDCIT, ISSN 0975 – 8887, 2013.

[11] Kan Yang, Zhen Liu, Zhenfu Cao, Xiaohua Jia, Duncan S. Wong & Kui Ren, ―TAAC: Temporal Attribute-based Access Control for Multi-Authority Cloud Storage Systems‖, in IEEE Transaction, 2011.

[12] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Xiaorui Gong & Shimin Chen, ―POSTER: Temporal Attribute-Based Encryption in Clouds‖, in ACM Journal, ISSN:978-1-4503-0948-6/11/10, Oct 2011.

[13] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, ―DACC: Distributed Access Control in Clouds‖, in International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-1, ISSN: 978-0-7695-4600-1/11, doi:10.1109/TrustCom.2011.15, 2011.

[14] Pratap Chandra Mandal, ―Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish, Journal of Global Research in Computer Science, ISSN: 2229-371X, Volume 3, No. 8, August 2012.

[15] Craig Gentry, ―Computing Arbitrary Functions of Encrypted Data‖, in ACM Journal, ISSN: 0001-0782/08/0X00, 2008.

[16] Bharath K. Samanthula, Gerry Howser, Yousef Elmehdwi, and Sanjay Madria, ―An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud‖, in ACM Journal, ISSN: 978-1-4503-1596-8/12/08., 2012.

[17] Farhan Bashir Shaikh & Sajjad Haider, ―Security Threats in Cloud Computing‖, in 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates Dec 2011.

[18] Farzad Sabahi, ―Cloud Computing Security Threats and Responses‖, in IEEE Transaction, ISSN: 978-1-61284-486-2/11, 2011.

[19] Wentao Liu, ―Research on Cloud Computing Security Problem and Strategy‖, in IEEE Transaction, ISSN: 978-1-4577-1415-3/12, 2012.

[20] Amit Sahai & Hakan Seyalioglu, ―Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption‖ in DARPA N11AP20006, University of Texas, Aug 2012.