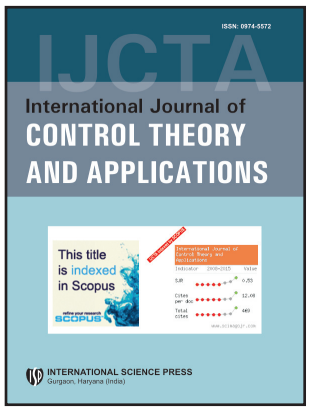

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 16 • 2017

Cryptographic Security System for Institutional Data Cloud

P. Umaeswari[a] and B. Shanthini[b]

[a]Research Scholar, CSE Department, St. Peter's University, Avadi, Chennai – 600 054, Tamilnadu, India. Email: umaeswari11@gmail.com
[b]Professor and Head, Department of IT, St. Peter's College of Engineering and Technology, Avadi, Chennai – 600 054, Tamilnadu, India. Email: bshanthini@gmail.com

Abstract: Big data institutional information is saved in a cloud environment. Big data stores large data in a cloud for easier access by the user anytime, anywhere. This paper analyses how multiple cloud users in an institution could use the cryptographic data in a secured manner. Encrypted data files are uploaded into the big data cloud with proof of ownership. Head of the institution, usually the principal would be the administrator. Security of the system is ensured by allowing only the registered and authenticated users and the others are prohibited from using it. The other registered users include the Heads of the departments (HoDs), teaching and non-teaching faculty, students and parents and only admin authenticated users can upload the files in an encrypted form with POW. Files can be downloaded by the registered users only through the verification of OTP sent by the admin/principal.

Keywords: Big Data Cloud, Institutional Information, Security, Authentication

1. INTRODUCTION

A. Cloud Computing

Cloud computing is a combined technology of web technology, Virtual machine, Grid computation and Autonomic Computation. Cloud achieves Storage and Computation services. Increased usage of access through internet with different devices, cloud service provider has permission to access various cloud services, which allows the use of new technology at a very less cost and it definitely is a boon to Information Technology [1].

Cloud computing utilizes optimum resources for its services in its best way and avails remote services through a network using various resources. Even if the end user has minimum hardware, cloud enables the maximum capability of computing. It gives maximum with the minimum resources like the end user is having the minimum hardware requirement satisfies the maximum capability of computing [2].

Cloud computing is the mixture of various computing entities that are globally separated but electronically connected. Cloud computation is moving towards corporate server which brings more issues such as distributed computing, identity management, virtualization, application security, authentication and access control [3].

B. Big Data

Big data computing has been operated by the construction of many next-generation sequencing based data sets, which are seeking to respond the queries about biological influences of human disease. It also provides various challenges of illustrating path to big data exposures has been paved with hazards the scientific community [4].

The problems of confidentiality, privacy, integrity and many other security issues are encountered in big data storage. Furthermore, these problems have been rectified with the convergent cryptography to secure the data duplication over network. As big data expands with the help of public clouds, traditional security solutions such as firewalls were found to be ineffective.

The design of security solution of big data should be capable of tackling specific big data characteristics such as variety, volume, velocity, value, variability, and veracity because these factors have a direct influence on information security [5]. The $5V^s$ of big data are as given below:

1. Volume of data: This is the most common descriptor of Big Data., i.e. the magnitude of data available is growing astronomically and handling such large data sets poses a serious challenge.
2. Velocity: refers to the speed of generation and transmission of data across the internet, i.e data collection from social networks, huge array of sensors from the micro (atomic) to the macro (global) level etc.
3. Variety: refers to the diverse data forms and in which model and structural data are archived.
4. Veracity: refers to the variety of quality, accuracy and trustworthiness of the data.
5. Value: All the above said Vs are important for reaching the value which focuses on specific research and decision-support applications to improve our lives, work and prosperity [6].

2. RELATED WORK

Allam Jyothi, Somasekhar. G, Prem Kumar. S [7] has suggested a security process for cloud. The author has proposed to combine signature and Convergent key encryption methods to attain a more secured cloud data sharing for more dynamic groups that are in the cloud. The group signature scheme has allowed an anonymous use of the cloud resources and the convergent key encryption techniques allowed secured data sharing between the data owners and others including new entrants. The high overhead and huge cipher text size of broadcast encryption technique hindered the users with limited resources. In such cases, the group manager computes the revocation parameters and uploads the files in the cloud for public use.

Pancholi, Patel [8] presented a symmetric cryptographic algorithm called AES (Advanced Encryption Standard) which is based on several permutations, transformation and substitutions. On the other hand, the security of data in cloud database server has the key resources for the concern in the recognition of cloud.

Li Chen, Jiang [9] have proposed a vital security part of Attribute-Based Encryption (ABE). The security is through arrangement resistance, i.e. an opponent with numerous keys have the capacity to get information only when less than one individual key awards access. The idea of attribute based encryption was initially proposed by Amit Sahai and Brent Waters which is further advanced by Amit Sahai, Omkant Pandey, Vipul Goyal and Brent Waters. Few scientists have further proposed Attribute-based encryption with various powers that together produce user private keys.

Ramesh.K and Ramesh .S [10] presented an authentication scheme using OTP and an encryption technique using Advanced Encryption Standard (AES) which encrypts the owners' Personal Health Record

(PHR) before uploading onto the semi trusted cloud server. Fine grained access control was achieved using this technique.

Our proposed work uses Attribute-Based Encryption (ABE), Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA). ABE is a type of encryption that provides the Information Technology (IT) network with privacy and security through a policy between the attributes of the users in the system. ABE is of two types, Key Policy ABE (KP-ABE) and Cipher text- Policy ABE (CP-ABE). In CP-ABE, the sender's data access policy is embedded in the cipher text, and the recipient's attributes are associated with its private keys [11].

AES includes three block ciphers, such as AES-128, AES-192 and AES-256. Implying that encryption and decryption processes are done in block 128, 192 and 256 bits respectively. Symmetric or secret-key ciphers use similar keys for encrypting a decrypting process. So, every sender and the receiver must use and know the same secret key. All key lengths are believed to be satisfactory to maintain confidentiality of the information at the "Top-secret" level, and 192-bit or 256-bit key lengths are preferred for top secret information. Further, the number of rounds needed for 128-bit keys, 192-bit keys, and 256-bit keys are 10, 12 and 14 respectively. A round involves processing steps such as embrace replacement, transposition and mixing of the input plain-text and transformation into final output of cipher text. The encryption process of each round involves of the below steps [13, 14]:

- Sub Bytes – every byte non-linear substitution are replaced by another lookup table (S-box).
- Shift Rows – It is a transposition step of each row of the state is shifted cyclically a certain number of times.
- Mix Columns – a mixing operation operates the state columns and combines the four bytes of each column.
- Add-Round Key – Every byte of the state is united with round key; each round key is resulting from cipher key using a key program.

SHA reduces the message of arbitrary length to constant length message digest, which is very improbably equal to any other messages. The word "secure" shows that it is not possible to over a message but not create two messages for same hash value. The one-way hash functions are termed as "the workhorses of modern cryptography". The input data is usually known as the message, and the hash value is regularly termed as the message digest or simply the digest.

3. PROPOSED WORK

The main objective of the proposed work is secured data storage and safe access. An efficient security system provides multiple level authentications used for multiple users who access data in Big Data Cloud. Here, the data is encrypted and stored in a cloud by admin. In this case, the Principal, HoDs, teaching and non-teaching staff, students and parents can register their details, such as name, login password, confirm password, mail-id, phone No. etc in the registration form. The registration allows the users to login with OTP (one time password).

The admin encrypts data using ABE algorithm and AES algorithm and uploads it into the cloud and permits the authorized user to access the data. One Time Password generated by Secure Hash algorithm ensures the security of the stored encrypted data. While downloading the data, authorized user enters the one time password to get decrypted data using ABE and AES algorithms.

In this experiment Principal, HoDs, Teaching Staff, Non-Teaching Staff, student and parents of the institution access the data from Big Data Cloud. Head of the institution, usually the Principal is an Admin. HoDs, Teaching Staff, Non-Teaching Staff, Students and Parents act as users.

The architecture given in Figure 1 explains the secured data access from Big Data Cloud.

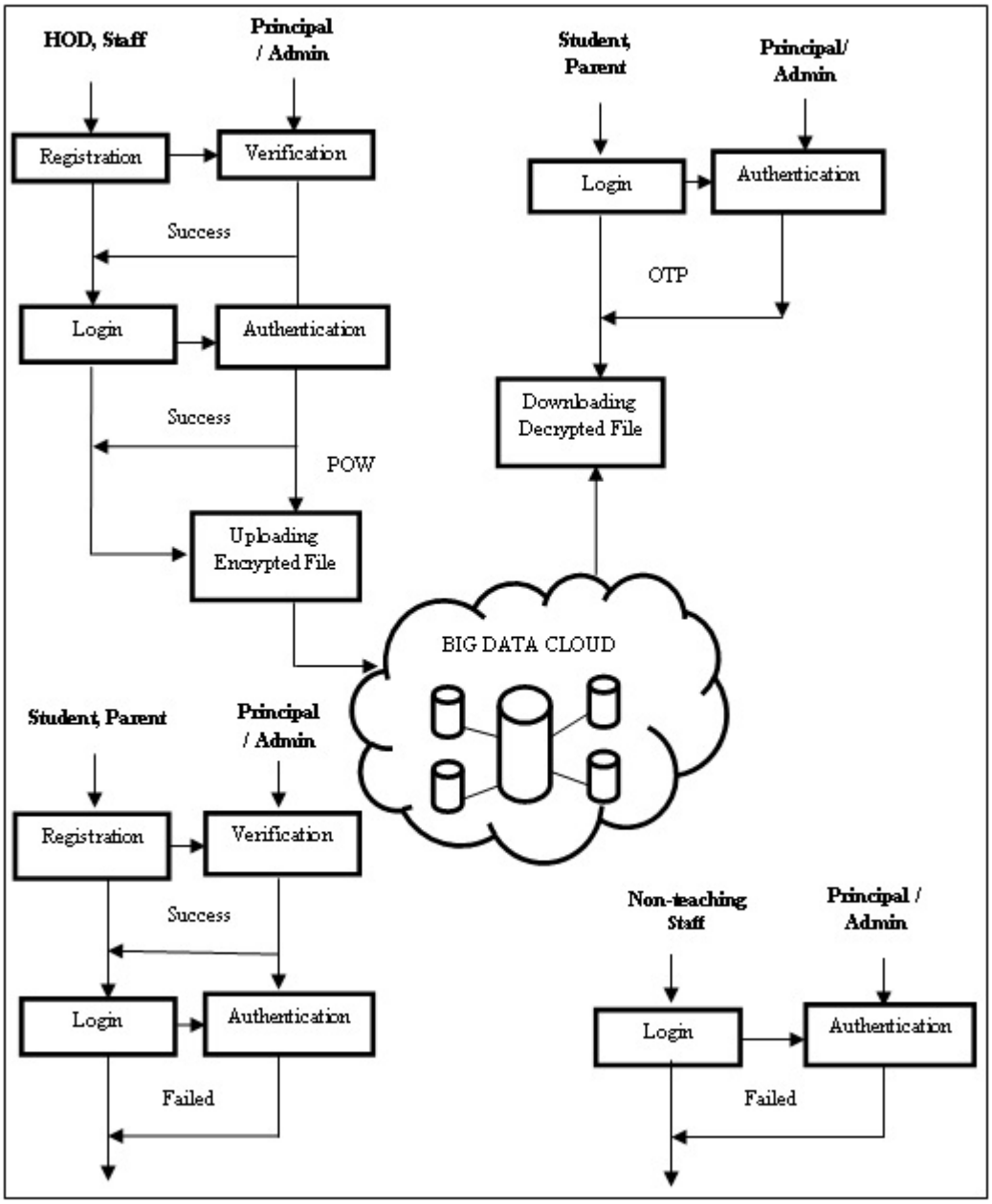

Figure 1: Uploading and Downloading Process of the Institution in Big Data Cloud

Figure 1 shows the encryption process of Admin/User of the data using ABE and AES algorithms. Registration process is a key for Principal, HoDs, Teaching Staff, Non-Teaching Staff, Students as well as Pparents. Each registration is verified by the Principal (Admin).

The registration and login passwords are important to authorize the access. The number of users like Principal, HoD, Teaching Staff, Non-Teaching Staff, Students and parents register into the system. After login to the system, the Principal (Admin) verifies the user login details with registration details and permits the access of data by the users. Access permission includes authorization to upload the files like institutional details, infrastructure, lab facilities, departments, fees structure, faculties, results, exam dates etc. Proof of ownership (POW) is needed

to identify the resource person who uploaded the file the Big Data Cloud. Admin/Principal gives authorization to the Principal (Admin), HoD and Teaching Staff to upload the files. Principal (Admin), HoD and Teaching Staff are authorized persons whereas Non-Teaching Staff, Students and parents are unauthorized to upload the files.

For downloading the data/files, Principal (Admin) authorizes multiple users. The number of users like Principal, Teaching Staff, Non-Teaching Staff, Students and parents can login into system. Principal (Admin) gives authorization to Students and parents. Admin sends One Time Password to their mail-ids. Authorized person can only access/download the data using the OTP received from the admin. . Hence, it is safe from administrator side as well as the user side. Unauthorized persons like non-Teaching Staff cannot download the data.

In this proposed system, POW is generated using AES algorithm. Before uploading, the files are encrypted by ABE and AES algorithm to provide more security and OTP is sent by the admin using SHA algorithm. The files are decrypted by ABE and AES algorithm for downloading.

4. DESIGN METHODS AND METHODOLOGY

In the proposed method, the data is encrypted and decrypted using Attribute Based Encryption (ABE) and Advanced Encryption Standard (AES) algorithm which provides greater security and confidentiality in cloud computing environment. Encoding the plaintext into cipher text is called Encryption and the process of decoding ciphers text to plaintext is called Decryption. In ABE algorithm an attribute will be connected with cipher text. The secret key will be derived from master secret key. This secret key is used to decrypt the files only if all its associate elements follow the rules. For each cipher text to be associated with an attribute as allowed by ABE, the master-secret key holder can mine a secret key for a strategy of the attributes, provided its related attribute follows to the policy [9].

Advanced Encryption Standard (AES) encryption is a block cipher that uses an encryption key and numerous rounds of encryption. Standard AES encryption the block is the length of 128 bits, or 16 bytes. The encryption mixes the data re- encrypting through rounds. The AES encryption algorithm is not a computer program or source code. It is a mathematical description of a process of ambiguous data. The principle of the AES encryption is needed by the most and new to United States and international standards [10]. ABE algorithm along with AES algorithm is safe and secure, hence it is used to encrypt and decrypt the data.

Attribute-based encryption is a comparatively current approach that re-examines the concept of PKC - Public-Key Cryptography. A message is involved during the encryption process for specific receiver's public key in traditional PKC. In the Identity-based cryptography and in particular IBE has changed the traditional understanding of PKC by allowing the public-key to an arbitrary string, for example, the receiver's email address. ABE uses one step to define the identity, but it is not an atomic. Derived set of attributes and the messages will be encrypted with respect to subsets of attributes such as KP-ABE, CP-ABE. AES is more suitable for encryption but ABE is considered to be more expensive, so the data is not directly encrypted using ABE. Generally symmetric key is used for encrypting bulk of the data and asymmetric key is suitable for encrypting short key value. First, data is encrypted using AES with 128 bits keys and the AES keys are again encrypted/decrypted using ABE and are sent together with cipher text [11].

Registration form filled by the user details serve as attribute and ABE algorithm work with Advanced Encryption Standard algorithm to provide more security, efficient and faster encryption of the data. ABE and AES algorithms allow encryption and decryption of the data based on user attributes, makes the data perfect for encryption and makes it efficient. Data owner/Admin encrypts and uploads the data into the cloud and permits access to the authorized user. The secure encrypted data uploaded into the cloud by admin, provide secure data

storage and avoid data loss. Authentication permission is given to the user to provide confidentiality and data integrity.

While AES is more suitable for encryption/decryption of data, ABE is considered to be more effective. Generally symmetric key is used for encrypting bulk of the data and asymmetric key like ABE is suitable for encrypting/decrypting short key value. Firstly, data is encrypted/decrypted using AES with 128 bits keys and the AES keys are again encrypted/decrypted using ABE and are sent together with cipher text making the encryption/decryption more efficient compared to the other algorithms [12].

SHA algorithm has been proposed for providing separate key to each user requesting the authentication of necessary files posted by the file owner. The OTP is created with the help of proposed algorithm and it should be used once to decrypt the required information.

One Time Password is used as the third level of authority to decrypt the data. Secure Hash Algorithm is used to generate One Time Password sent to the user's mail-id to maintain confidentiality for downloading the data.

The model of ABE with subcontracted decryption consists of the following constraints: Setup, KeyGen, Encrypt, Decrypt, $GenTK_{out}$,$Transform_{out}$,$Decrypt_{out}$. An important party generates the public parameters and a master secret key(MSK) by Setup algorithm, private key generated by the trusted party running KeyGen [13].

After taking the cipher text, the user selects the outsource decryption of the cipher-text. If the user desires to select outsource decryption, he needs to execute the **$GenTK_{out}$** algorithm and use private key to generate the transform key by the particular use [14]. Proxy is able to covert the variable size cipher text into constant size cipher-test by **$Transform_{out.}$** **$Decrypt_{out}$** algorithm which is used to recover the plain text from transformed cipher-text.

Concept of ABE scheme with decryption process is as given below:

- **Setup** *(1^{λ} U)*: The algorithm works at the Setup points *(1^{λ},U) →(PK, MSK)*, and selects the key derivation function of KDF with 'l' - output length , then publishes the public parameters *PP = (PK,*KDF, *l)&MSK.*
- **KeyGen** *(PP, MSK, I_{key})*: The key generation algorithm runs KeyGen *(PK, MSK, I_{key})→ SK*, and outputs *SKI = (I_{key} , SK)*.
- **Encrypt** *(PP, M, Ienc)*: Parse *PP = (PK,* KDF, *l)* the encryption algorithm runs Encrypt *(PK, I_{enc}) → (*DK, *C)*. It selects a random coin *r*, sets _ *C* =$Commit_r$ *(M)*, and runs Enc *(*KDF (DK,*l), M* ‖ *r)→C*, outputs of the cipher text *CT = (I_{enc}, C, C,_C)*.
- **Decrypt** *(PP, SKI, CT)*: Parse *PP = (PK,* KDF*)*, *CT = (Ienc, C, C,_C)* and *SKI = (Ikey , SK)*.

5. EXPERIMENTAL RESULTS

Figure 2 explains the results of comparison of Encryption time (mille second) with ABE or AES and ABE & AES algorithms for the fixed number of files uploaded by multiple users on cloud.

The results show that the encryption time required by the ABE with AES encryption algorithm is more compared with ABE algorithm or AES algorithm because of the additional security. i.e. Using AES algorithm for s encryption and the encrypted files get re encrypted by ABE algorithm. It takes more encryption time when compared to other algorithms. Depending on the number of files, the encryption time is increased or decreased. Hence the number of files uploaded into the cloud by the multiple users using the algorithms ABE with AES produces good results to encrypt the data files.

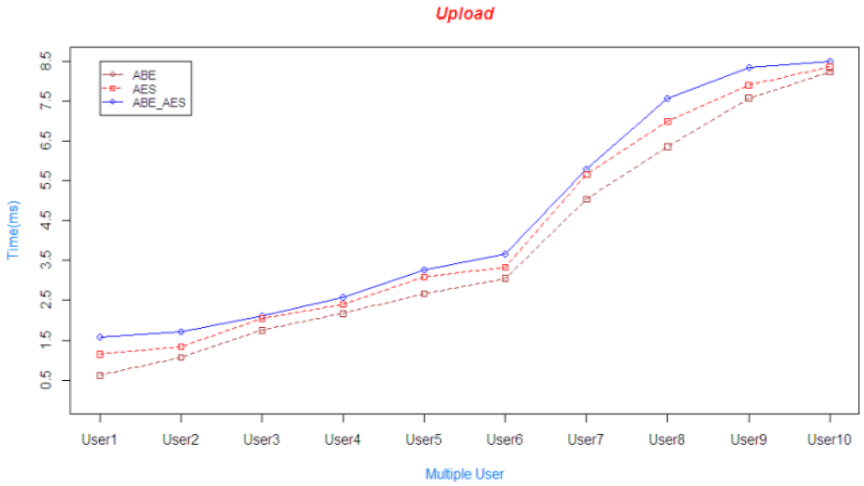

Figure 2: Encryption Time for Uploading the File by multiple users

Figure 3 shows the results of comparison of decryption time for downloading the number of files (milli seconds) with ABE or AES and ABE&AES&SHA algorithms for fixed number of user file requests on cloud.

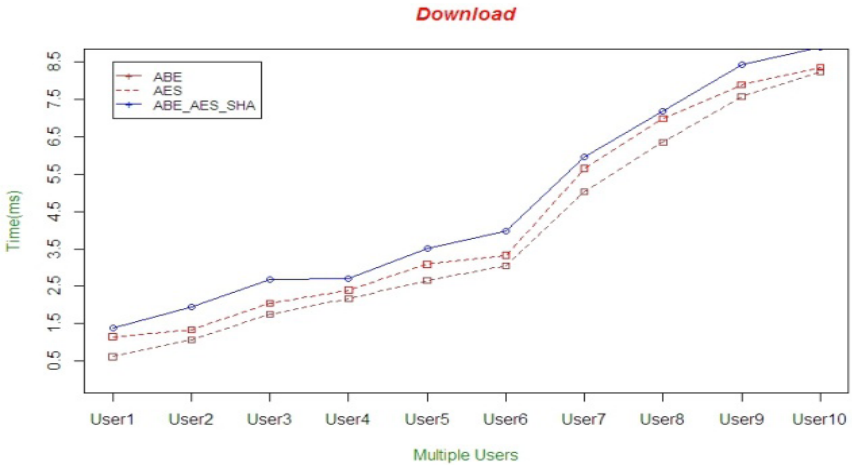

Figure 3: Decryption Time for Downloading the File by multiple Users

The given graph shows that the decryption time required by the OTP by SHA with ABE & AES decryption algorithm requires considerably more time to decrypt the number of files compared to that with ABE or AES algorithms depending on multiple user downloading fixed the number of files from the cloud.

SHA algorithm has been proposed for providing a separate key to each user requesting the authentication of necessary files posted by the file owner. The OTP was created with the help of the proposed algorithm and it should be used once to decrypt the required information. The user would provide a request to the cloud big data storage where 'N' number of files is stored by the '*n*' number of the users. Each user is given a specific access control to access the cloud big data.

Decryption time with ABE and AES algorithms is more compared with the other algorithms, because the data is decrypted using AES algorithm which files is decrypted. Again is re- decrypted by ABE algorithm. Depending on the number of files the decryption time is increased or decreased. The decrypted files are stored on Big Data Cloud. The OTP developed by SHA algorithm is given by the authorized user to download the data. Hence the number of files downloaded in decrypted form from Big Data Cloud to multiple users which takes

more time when compared with decrypted by ABE or AES algorithm. Hence the number of files downloaded into the cloud by the multiple users using the algorithms ABE with AES and OTP by SHA produce good result to decrypt the data files.

6. CONCLUSION

This proposed method is tested for a department in an educational institution. We can implement the proposed method in different sectors like library system, banking, employee details etc. Because Big Data Cloud enables the users to upload and download the data easily and efficiently. Proposed system involves the uploading of data file into the Big Data Cloud by the admin who in turn permits the authorized users. In a cloud environment data is stored in encrypted manner. The authenticated person can only decrypt the data by using the password. The proposed method has data integrity, highly secured data storage without data loss. A particular person can be authenticated by receiving one time password to their respective mail-ids at the time of access request to the Big Data Cloud.

7. FUTURE WORK

Hence the proposed method provides secure data access and this method is suitable for private cloud. In future this work can be extended for the public cloud.

REFERENCES

[1] Cecil Donald. A, L. Arockiam, "Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues", International Journal of Computer Applications, ISSN:0975 – 8887, Vol. 94, No. 1, May 2014.

[2] Rachna Arora, Anshu Parashar," Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.

[3] Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. A strong user authentication framework for cloud computing, In Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific (pp. 110-115). IEEE, Dec 2011.

[4] Flood, M. D., Jagadish, H. V., & Raschid, L., Big data challenges and opportunities in financial stability monitoring. Financial Stability Review, (20), 129-142, 2016.

[5] Wen, M., Yu, S., Li, J., Li, H., & Lu, K., Big Data Storage Security. In Big Data Concepts, Theories, and Applications (pp. 237-255). Springer International Publishing, 2016.

[6] Chaowei Yang, Qunying Huang, Zhenlong Li, Kai Liu, Fei Hu, Big Data and cloud computing: innovation opportunities and challenges, International journal of digital earth, volume 10,issue 1, 2017.

[7] Allam Jyothi, Somasekhar. G, Prem Kumar. S, "A Secure Multi-Owner Data Sharing Scheme for Dynamic Group in Public Cloud", International Journal of Computer Engineering in Research Trends, ISSN: 2349-7084 Vol. 2, Issue 8, pp. 475-480, Aug. 2015.

[8] Pancholi, V. R., & Patel, B. P., Enhancement of Cloud Computing Security with Secure Data Storage using AES. International Journal for Innovative Research in Science and Technology, 2(9), 18-21, 2016.

[9] Li, L., Chen, X., Jiang, H., Li, Z., & Li, K. C., P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds. In 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), IEEE (pp. 575-580), May 2016.

[10] Ramesh.K, Ramesh.S, "Implementing One Time Password Based Security Mechanism for Securing Personal Health Records in Cloud", Control, Instrumentation, Communication and Computational Technologies (ICCICCT), IEEE, ISBN:978-1-4799-4191-9, pp. 968 – 972, Jul. 2014.

[11] TK, A. K., Thomas, J. P., & Parepally, S. (2017). An efficient and secure information retrieval framework for content centric networks. Journal of Parallel and Distributed Computing.

[12] Smekal, D., Frolka, J., &Hajny, J. (2016). Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays. IFAC-PapersOnLine, 49(25), 384-389.

[13] Wang, Z., Cao, C., Yang, N., & Chang, V. (2016). ABE with improved auxiliary input for big data security. Journal of Computer and System Sciences.

[14] Yin, H., Qin, Z., Ou, L., & Li, K. (2017). A query privacy-enhanced and secure search scheme over encrypted data in cloud computing. Journal of Computer and System Sciences.