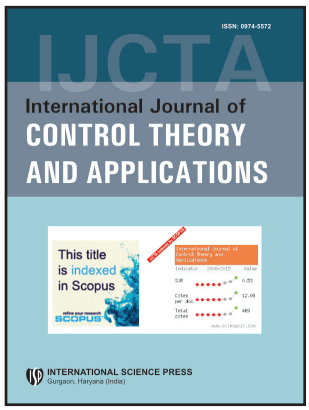

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 12 • 2017

Three Level Security System for Multiple Users in Cloud Computing

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

[a]*Research Scholar, CSE Department, St. Peter's University, Avadi, Chennai – 600 054, Tamil Nadu, India*
[b]*Professor and Head, Department of IT, St. Peter's College of Engineering and Technology, Avadi, Chennai – 600 054, Tamil Nadu, India*

Abstract: Cloud allows possible access to the information from anywhere at any time. Generally, the data is stored in physical data storage device from the same location where as this step is not required in cloud. This paper explains about the how the cloud user can safely upload and download their data. In cloud, data stored encrypted manner. The authenticated person can only decrypt the data by using the password. The proposed method is to maintain data integrity and to secure data storage without data loss. A particular person can receive One Time Password (OTP) to their respective mail-Id. High secure encryption algorithms ABE and AES used before uploading the data to the cloud. The authenticated person can only access the data from the cloud. The authenticated person access the data use by OTP generated randomly by using random key generation algorithm. After entering the password, the data can be viewed by the user. It is a secure method and no one can guess the password. The decrypted data by using ABE and AES algorithms downloaded to the user. Hence, in this proposed method there three level security systems are followed.

Keyword: Cloud, Security, Authentication, Access.

1. INTRODUCTION

Cloud computing resources are delivered on-demand as a service for customers over the internet. The management of information security operations is a complex task, especially in cloud environment. When cloud computing service models were first developed, more focus was given on performance, convenience, on-demand deployment and functionality. Cloud services are delivered through the internet and these services can be accessed anywhere and anytime. Thus these services are prone to cyber-attacks [1]. Cloud avail remote services through a network using various resources. It enables the users with minimum resources to get maximum computing and storage capability. This is achieved through this technology which requires and utilizes its resources in the efficient way [2].

Security is a crucial factor that affects most of the computing technologies like cloud technology due to its pervasive nature. Cloud computing infrastructure utilizes many innovative technologies and services and most of them were not completely assessed in terms of security aspects. Cloud Computing suffers from numerous security challenges like data security, trust, confidentiality and performances issues [2].

A. Cloud Computing Service Types

The three types of services offered by cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS). IaaS, also known as resource clouds offers manageable resources as services and virtualization capabilities to users. Some of examples of IaaS are Amazon EC2, vCloud [3]. PaaS offers services for developing and deploying the consumer application onto the cloud infrastructure using the service provider's tools and provides web applications and services on the Internet. Examples of PaaS are Microsoft Azure and Google App engine. Google App Engine allows developers to create customized apps [3]. There are numerous application offered by cloud service that are hosted by SaaS otherwise known as Application Service Provider (ASP) that can be accessed through the internet. SaaS cost less when compared to buying application which is one of the main benefits of using SaaS. Some of the examples of SaaS are Gmail, Google Groups and Online tax filing [3].

B. Types of Cloud Computing

There are different types of cloud computing they are private, public, community and hybrid cloud. Private cloud is deployed within the organization and the information can be accessed only by the employees or the members of that organization. Moreover, the infrastructure is operated and managed by the organization. In community cloud the information is shared between communities having similar concerns or interest, where as in public cloud the information is made available to general public and also to large scale industries. This is deployed in an organization in order to access various resources and web based applications. Hybrid cloud is a mix of at least two or more different types of clouds existing as unique entities but these entities are bound together by technology.

2. SECURITY ISSUES AND CHALLENGES OF CLOUD COMPUTING

Cloud storage is based on web technology that allows access to high quality on-demand cloud application by utilizing limited hardware and software resources. Moreover, the user information and data are stored in remote locations. The cloud users face many security challenges and issues in accessing services through internet as shown in Figure 1.

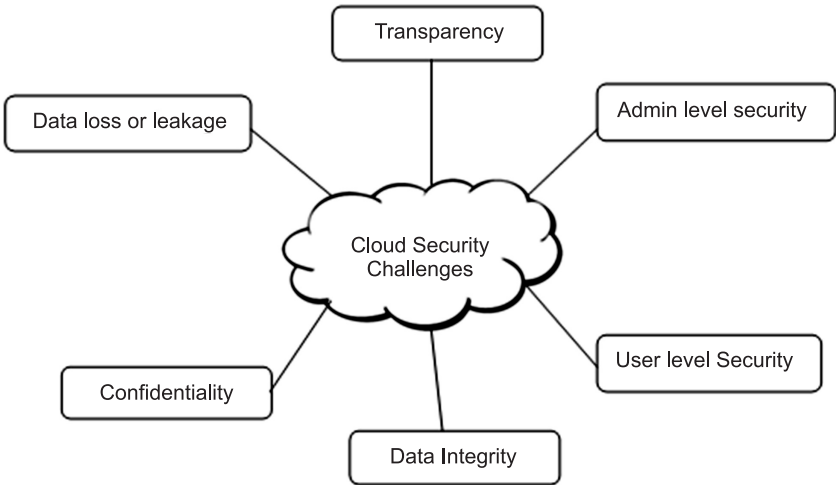

Figure 1: Security challenges in cloud computing

A. Confidentiality

Data confidentiality and security is identified as one of the main concerns for widespread adoption of cloud services. The service provider has concern over the privacy and security of the cloud user as they provide critical

and sensitive data. The data stored in the cloud are globally distributed in multiple third party servers which increases the risk of data leakage and privacy issues and also data exposure. The cloud service provider must make sure that user private data is protected from unauthorized discloser [4].

B. Data Loss or Leakage

Loss of data occurs when the user data is logically or physically detached from the organization or if the confidential information is misused that can be either intentionally or unintentionally. Some of the examples are leaking customer or patient information data, design specifications or source code, intellectual property, trade secrets *etc.* [5]. Loss of data can occur due to loss of encryption key, natural misfortunes like fire or earthquake, malicious attacks etc. Data breaching happens due to data deletion or modification of data without backup. In order to avoid unauthorized access of the confidential data there should be backup [3].

C. Data Integrity

Data integrity ensures that cloud data is not destroyed or altered in an unauthorized way and lack of appropriate security mechanism leads to integrity problems. [5].

D. Transparency

The cloud users are unaware that their data is been accessed and also have no knowledge on how to secure their data. Therefore, it is important for the service provider to maintain a transparency among their users and should ensure that the user trust the stability and the reliability of the data that are stored in the cloud. Public cloud is more transparent when compared to other cloud models such as private or hybrid cloud. Transparent security would prevent cloud providers from disclosing sensitive information about customer's security policies, design and practices [4].

E. Security on Admin Level

There is a lack of security at admin level. The admin is the one who uploads the data into the cloud and they are also responsible for securing the data from unauthorized users. There are number of security issues/challenges with cloud computing that fall under two broad categories namely (i) security issues faced by cloud admin or service provider (organizations that deliver software or application IaaS through the cloud) and (ii) security issues faced by the cloud user [6].

F. Security on User Level

There is lack of user level security in cloud and the data uploaded in the cloud are normally accessed by cloud user. Moreover, the cloud user must be able to access to their data easily and confidentially. The unauthorized users must not access to private data. So, the service providers must ensure that their infrastructure is more secure and the user's data and applications are also protected from unauthorized users. At the same time the users must ensure that the providers has taken the proper security measures to protect their data by taking proper security measures such as use strong passwords and authentication measures [6].

In this paper, the administrator provides data security by encrypting the data before uploading into the cloud and only the authenticated users download the decrypted data. In the proposed method, the users initially register them with their details in user form. After registration the user enter into login level. Upon successful login, the proposed security system generates a one-time numeric password to the authenticated user and sends it to their corresponding e-mail which would be valid only for that session.

3. RELATED WORK

Allam Jyothi, Somasekhar. G, Prem Kumar. S [7] have suggest a security process for cloud. The author has proposed to combine signature and Convergent key encryption methods in order to attain a more secured cloud data sharing for more dynamic groups that are in the cloud. The group signature scheme has allowed anonymous use of the cloud resources and the convergent key encryption techniques allowed data owners to securely share their data files with others including new joining users. The high overhead and huge cipher text size hindered the adoption of broadcast encryption technique for users with limited resources. To handle this issue, the group manager computed the revocation parameters and made it as publicly available by uploading them into the cloud. This design considerably minimized the computation overhead of users while encrypting the files. The overhead and the cipher text size are fixed regardless of the revocation users.

Sathana. V and Shanthini. J [8] developed a secured data sharing system model for dynamic groups that are in an untrusted cloud. It consist of three, entities namely the cloud, a group manager (business manager) and group members (employees). The secure data sharing scheme enabled the individual users to share data with others in the group without disclosing identity secrecy to the cloud. It has supported efficient user revocation and new user joining. The group manager is responsible for system parameters generation, user registration and revocation. Revocation of users was performed using a public revocation list without updating the private keys of the continuing users and new users decrypt the files stored in the cloud.

Ramesh.K and Ramesh .S [9] presented an authentication scheme using OTP and an encryption technique using Advanced Encryption Standard (AES) to encrypt the owners Personal Health Record (PHR) prior to uploading onto the semi trusted cloud server. Fine grained access control was achieved using this technique.

Sunita R. Patil and Sandeep Kadam [10] have proposed a novel multiple owner data sharing method for dynamic group in the cloud. Group manager failure was maintained by increasing backup and the request are shared by the group managers. This method is immune to both the brute-force and shoulder attack that are from the user side. The system used a combined approach based on image authentication and OTP in order to increase the security. First, the user chooses a pre-selected image to login based on the chosen image from the grid. After this the OPT is automatically generated.

Indrajit Das [11] developed three diverse methods to allow easy and secure login to cloud service using OTPs and user's mobile phone as an authentication device. A two factor OTP authentication was used in cloud services. The data transmissions between the client and the server were configured to apply AES encryption. In the first method, OTP was generated on the mobile device on the basis of three factors components like 4-digit PIN code entered by user, secret arbitrary number and the present time. Then they are hashed using SHA-1. The second proposal is an OTP with challenge-response scheme similar to the previous type but an extra factor called challenge was added. Optical challenge-response is the third proposal in which the two-dimensional bar-codes were used as challenges and responses, rather than a combination of text and strings or numbers.

Geetanjali Choudhury and Jainul Abudin [12] proposed a novel authentication mechanism based on encrypted one time password (EOTP). This method used ID, PIN (static password) and encrypted one time password (EOTP) for login purposes. RSA algorithm was used for encrypting and decrypting one time password and the EOTP was directly transmitted to the user over the network. The system does not need any third party like GSM mobile number or email. The proposed authentication mechanism improved security, performance and eliminated third party dependency.

Sathana. V and Shanthini. J [13] designed a three level security system for group data shared in cloud. Data owners maintain their encrypted files in an untrusted repository and dispense the respective decryption

keys only to legitimate users. Therefore, illegitimate users and the servers were prevented from file access since they do not possess knowledge of decryption keys. An image based authentication was incorporated to offer a three levels of security. The advantages of this system are resistance to known attacks, maintaining seamless forward secrecy and security against disclosure of OTP, privacy, absence of sensitive verifier table and minimal computation and communication cost.

Vishal Paranjape and Vimmi Pandey [14] focused on various privacy and trust challenges issues in cloud environment. General design principles of a cloud were analyzed to manage the security threats and risks. Instead of conventional username-password authentication scheme, a dynamic code of mobile token was applied due to its robustness. Dynamic mobile token is an application to create a code by OTP mechanism and it can be applied only for a single session or transaction. In this method mobile device run a MIDLET that created OTP to authenticate the cloud user. Every mobile token contains a value for the secret variable to isolate one user access transactions or personal from another user.

Richa Chowdhary and Satyakshma Rawa [15] examined OTP usage for authenticating services from multiple clouds at once. This paper gives a description on concept of cloud and use of multi-clouds organizations. At that point, it researched the security issues in cloud and OTP. This paper additionally discusses about confidentiality of the data, which ought to be kept up while information is transmitted over the cloud. In this way, different systems such as checksum, hash capacities were utilized. Moreover, Byzantine fault-blame tolerant replication protocol was executed in the cloud to maintain the privacy of data.

Sonia Arora and Pawan Luthra [16] discussed about data storage security model of cloud. The data model of default gateway proposed in this paper focused on providing high security to the platform. The gateway was used to encrypt the data completely with best encryption techniques before sending the data on cloud storage. Maintaining the security during transmission was the major concern, therefore secure OTP was proposed and various hashing techniques were used to sustain the integrity of data. The results demonstrate that AES, RC4 and Blowfish are the best algorithms as they take less time to encrypt or decrypt data. In addition to this data integrity was ensured by using hash algorithms.

4. PROPOSED WORK

The main aim of proposed work is to store the data in a secure manner and have a more safe and secured access to the data. An efficient security system provides three level authentications which are used for multiple users who can access data in cloud. Here, the data encrypted are stored in the cloud by admin. In any organization working people can register their details in the registration form, for example Name, login password, confirm password, mail Id, Phone No. *etc*. After registering into the system the user is allowed to login. Login into the system shows first level of authority. Use of registered details user get OTP to their respective email Id. Using ABE algorithm along with AES algorithm the admin encrypt the data and uploaded into the cloud. The admin uploads the secured data and permits the user to access the data. Then this permitted person is known authorized person who can access the data shows the second level of authority. Those who are authorized can access the securely stored encrypted data. OTP generated by random key generation algorithm. While downloading the data, user enter the OTP to get decrypted data using the algorithms ABE and AES downloaded to the viewer which shows the third level of authority. The below architecture explains detailed secure data access in cloud computing.

Figure 2 shows the process of Data owner/Admin encrypted the important data using ABE algorithm along with AES algorithm. The registration and login passwords are important to authorize. The number of user register into system, OTP sends it to their mail-Ids. Admin authorizes the user. Authorized person can only access/

download the data using OTP. Hence, it is safe from administrator side and also the user side. Unauthorized person cannot access the data.

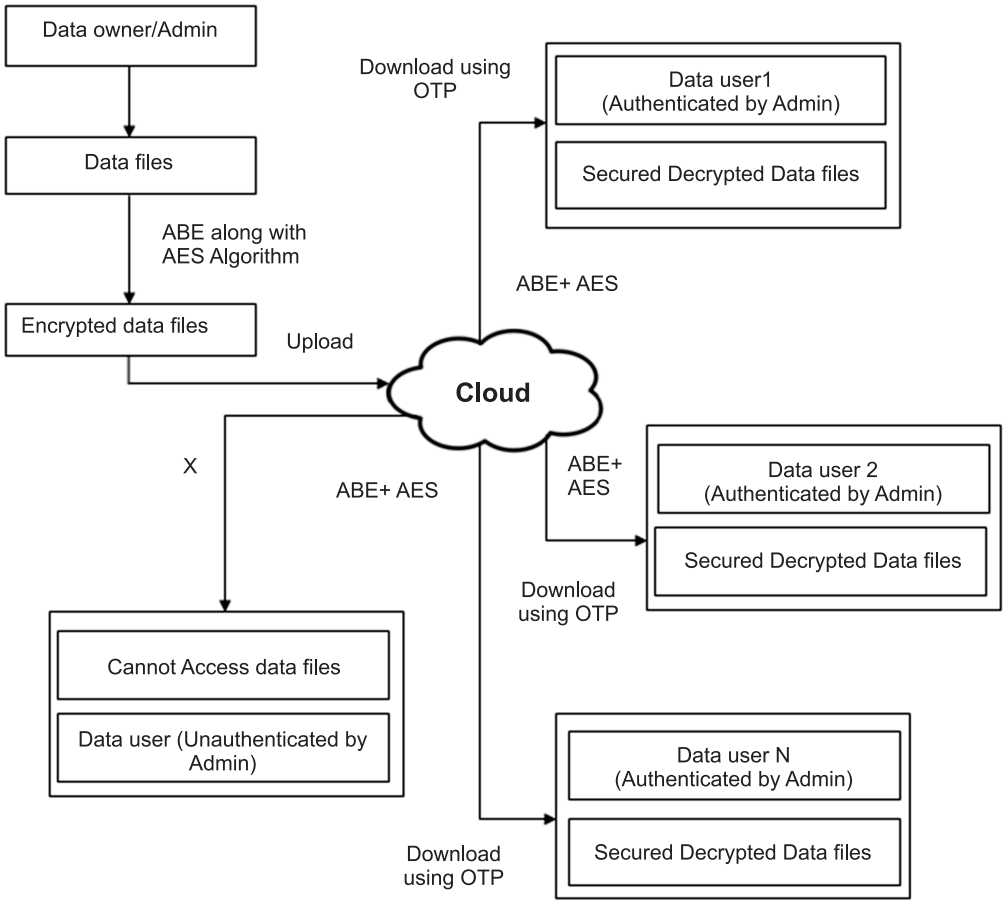

Figure 2: Architecture Diagram

The administrator has the rights to register the user into the system. In an organization the working people can be a user. The admin encrypt the data and upload into the cloud. The admin would decide on which users to download the data. Those people are called authorized persons.

Static password used to register into the system. User registration contains User Name, Password, Re-Type Password, Mail Id, Address, Phone Number and Role Type (User designation). After registering into the system the user receives OTP to their given mail Id. OTP will be 5 digit random valid number for one time, secret, this cannot be predictable by anyone, changeable whenever login into the system.

Those people who are registered to the system are allowed to login to the system with their passwords. Admin has rights to upload the data. Admin login to its encrypted data and uploaded into the cloud. Later, the data is uploaded by the admin and gives data access to authorized persons. Those who login to the system and authorized by the admin can download the data using their OTP passwords. For example, if the user is unauthorized they cannot access the data.

Administrator has rights to upload the data. The data encrypted by an Attribute Based Encryption (ABE) Algorithm and Advanced Encryption Standard (AES) algorithm and uploaded into the cloud by Admin.

The authorized person can download the encrypted data using OTP generated by random key generation algorithms that are send to the users respective mail Id, while the user register into the system.

5. DESIGN METHODS AND METHODOLOGY

In the proposed method the data encrypted and decrypted using Attribute Based Encryption and Advanced Encryption Standard algorithm which produces greater security and confidentiality in cloud computing atmosphere. The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. In Attribute Based Encryption method an attribute will be linked with cipher text. From master secret key, this will be derived. This secret key is used to decrypt the files merely if all its associate elements go after the rules.

Every cipher text connected with an attribute permitted by ABE (Attribute-based encryption) and the master-secret key holder can separate a secret key for a strategy of these attributes so that a cipher text can be decrypted by this key if it is related to attribute that follows the policy. The key size regularly increases linearly with the number of attributes it envelops, or the cipher text-size is not steady [17].

Advanced Encryption Standard (AES) encryption is a block cipher that uses an encryption key and a few rounds of encryption. A block cipher is an encryption that works on single block of data at a time. On thus account the standard AES encryption block is 128 bits or 16 bytes, long. The term round refers to the encryption that blends the data re-encrypting which is based on the length of the key. This AES encryption itself is not a computer program or source code. This is a mathematical description of a process of obscuring data. AES encryption is more secure, faster in both hardware and programming. The AES encryption itself is not a PC program or PC source code. It is a numerical portrayal of a procedure of darkening information. AES encryption is more secure, faster in both hardware and programming. Additionally the principle preference of the AES encryption is required by the latest U.S. and international standards [18]. ABE algorithm alongside AES algorithm is secure and safe; subsequently it is used for data encryption or decryption

In Registration Form the user fills up the details which are taken as attribute. The Attribute Based Encryption algorithm works with Advanced Encryption Standard algorithm to provide more efficient and faster encryption of the data. ABE and AES algorithms allows encrypt and decrypt the data based on user attributes makes the data perfect encryption and make it efficient. Data owner/Admin encrypts the data and uploads it into the cloud and permits the authorized user. The secure encrypted data uploaded into the cloud by admin, to provide secure data storage and avoid data loss. Authentication permission will ensure that user data confidentiality and integrity of the data is maintained.

One Time Password is used as third level of authority to decrypts the data. Random key generated and 5 digits One Time Password send to the user Mail-Id to maintain confidentiality.

6. EXPERIMENTAL RESULTS

Comparison of Encryption time given in mille second with AES and ABE & AES algorithm of number of files uploaded on cloud is tabulated in Table 1.

Table 1
Comparison of Encryption time for AES and OTP ABE & AES algorithm

FILE UPLOADED	*ENCRYPTION TIME (ms)*	
	AES (ms)	*ABE & AES (ms)*
1	0.821	1.590
2	1.175	1.713
3	1.956	2.119
4	2.367	2.580
5	2.966	3.164

Figure 3 shows that the comparison encryption time required by the ABE & AES encryption algorithm requires considerably more time to encrypt compare with AES algorithm because of additional security. Hence it proved that the number of files uploaded into the cloud safe and secure by the admin.

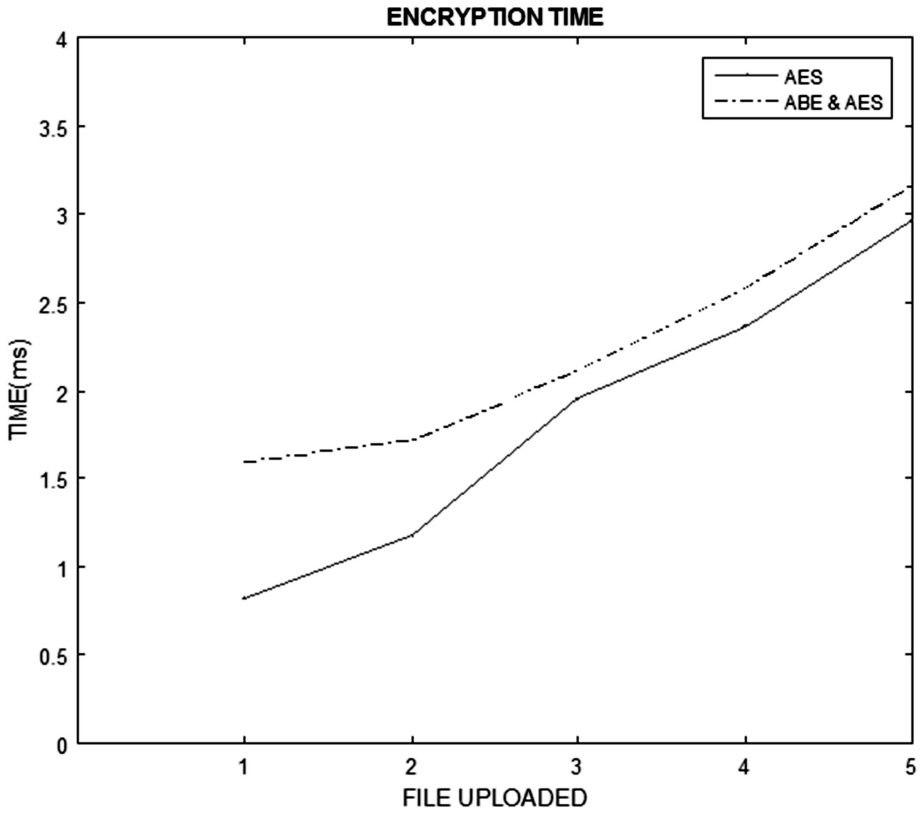

Figure 3: Encryption with AES and ABE & AES algorithm of number of files uploaded on cloud

Table 2 Results shows the comparison of Decryption time given in AES and OTP with ABE & AES algorithm of number of user authentication request on cloud. Figure 4 shows the comparison graph of decryption time required by the OTP with ABE & AES encryption algorithm requires considerably more time to decrypt compare with AES algorithm depends on user authentication request so as to get downloaded from the cloud.

Table 2
Comparison of Decryption time for AES and OTP with ABE & AES algorithm

USER AUTHENTICATION REQUEST	*DECRYPTION TIME (ms)*	
	AES(ms)	*OTP with ABE & AES(ms)*
1	0.416	0.796
2	0.897	1.055
3	1.117	1.371
4	1.623	1.972
5	2.266	2.519

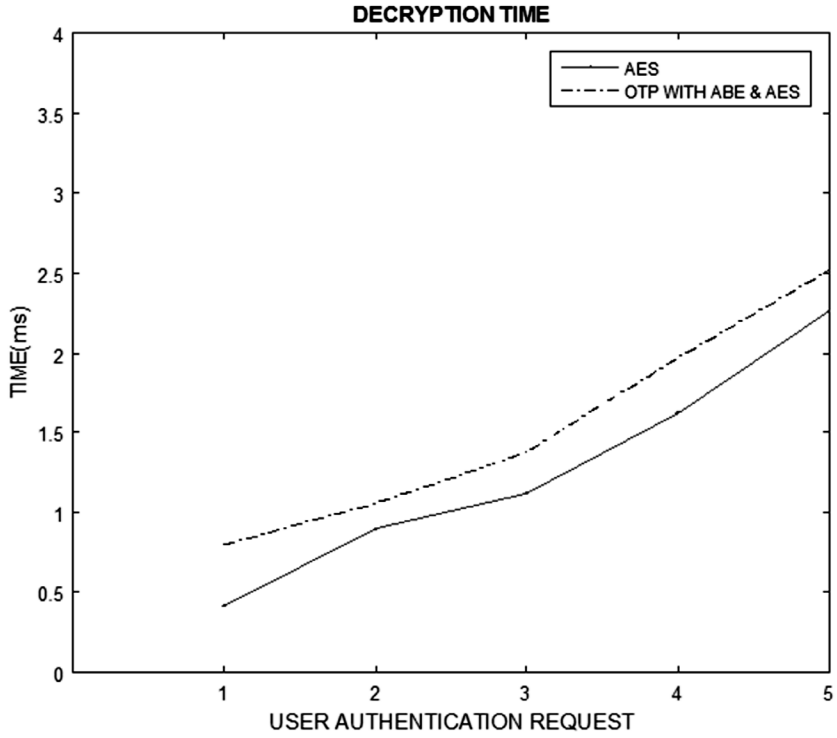

Figure 4: Decryption time of AES and OTP with ABE & AES algorithm for the number of user authentication request

Table 3
Security Issues Handled by Proposed Work

	Registration	*Login*	*Access Permission*	*Upload the Data (Encrypted)*	*One Time Password*	*Download the Data (Decrypted)*
Data Owner/ Administrator	Transparency	Transparency	Security and Confidentiality	Secure Storage Data Integrity	Data Integrity	√ Security on Admin Level
Authorized Data User	Transparency	Transparency	Security and Confidentiality	Authorized	Data integrity	√ Security on User Level
Unauthorized Data User	Transparency	Transparency	Not Authorized	Not Authorized	Not Authorized	X Unsuccessful Access

The below Table 3 explains the proposed system of highly secure and safe for both admin side and user side. Attribute Based Encryption Algorithm and with Advanced Encryption Standard algorithm used to encrypted and decrypt the data. It is secure algorithm to encrypt and upload the data. Authorized person can access permission from admin side and OTP are used to secure the data from unauthorized person. The cloud security challenges are faced by this proposed method. Also, Table 3 explained the security issues like transparency, confidentiality and data integrity, security without data loss or leakage are handled by proposed system.

7. CONCLUSION

This proposed method safe for cloud user. The data uploaded into the cloud by the admin and he permits the authorized one. In a cloud environment data stored in encrypted manner. The authenticated person can only

decrypt the data by using the password. The proposed method have data integrity, high secure data storage are achieved without data loss. A particular person can authenticate by receiving one time password to their respective mail-ID at the time of access request to the cloud. High secure encryption algorithm used before upload the data to the cloud. The authenticated person can only access the data from the cloud. The authenticated person access the data only use by one time password to decrypt the data with effective decrypted algorithm from the cloud.

8. FUTURE WORK

Hence the proposed method provides secure data access, this method suitable for any one organization or one private sector only. In the future the proposed work developed for the multiple sectors also.

REFERENCES

[1] Fahad F. Alruwaili, Aaron Gulliver.T, " SOCaaS: Security Operations Center as a Service for Cloud Computing Environments", International Journal of Cloud Computing and Services Science (IJ-CLOSER), ISSN: 2089-3337, Vol. 3, No. 2, pp. 87-96, Apr. 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] Abinisha Sapanny, Kavya. K.V, Neha Nagaraj, Soumya. M, Sheetal .V.A, "Cloud Security Challenges and Recommended Solutions", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol. 5, No. 4, pp. 82-86, Apr. 2015.

[4] Bhavani.S, Ankit Hatwal, "Review on Cloud Computing and Security Issues in Cloud", International Journal of Advanced Engineering Research and Science (IJAERS), ISSN: 2349-6495, Vol-2, Issue. 5, pp. 21-24, May 2015.

[5] Rex Cyril.B, S. Britto Ramesh Kumar. S, "Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, p-ISSN: 2395-0072, Vol. 02, Issue. 04, pp. 848-857, July-2015.

[6] Vijayakumar.K, "Security Issues and Algorithms in Cloud Computing", Global Journal of Advanced Research, ISSN: 2394-5788, Vol. 2, Issue 3, pp. 569-574, Mar. 2015.

[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] Sathana. V, Shanthini.J, "Enhanced Security System for Dynamic Group in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Vol. 4, Issue 3, pp. 37-42, Mar. 2014.

[9] 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.

[10] Sunita R. Patil, Sandeep Kadam, "RS-MONA: Reliable and Scalable Secure Method to Store and Share Secrete Data for Groups in Cloud", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 102, No. 3, pp. 13-17, Sep. 2014.

[11] Indrajit Das, "Mobile Security (OTP) by Cloud Computing", International Journal of Innovations in Engineering and Technology (IJIET), ISSN: 2319-1058, Vol. 2, Issue 4, pp. 284-290, Aug. 2013.

[12] Geetanjali Choudhury, Jainul Abudin, "Modified Secure Two Way Authentication System in Cloud Computing Using Encrypted One Time Password", International Journal of Computer Science and Information Technologies (IJCSIT), ISSN: 0975-9646, Vol. 5, No.3, pp. 4077-4080, 2014.

[13] Sathana.V**,** Shanthini.J, "Three Level Security System for Dynamic Group in Cloud", International Journal of Computer Science Trends and Technology (IJCST), ISSN: 2347-8578, Vol. 1, Issue 2, pp. 23-28, Nov-Dec. 2013.

[14] Vishal Paranjape, Vimmi Pandey, "An Approach towards Security in Private Cloud Using OTP", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol. 3, Issue 3, pp. 683-687, Mar. 2013.

[15] "Challenges and Surveys in Key Management and Authentication Scheme for Wireless Sensor Networks" in Abstract of Emerging Trends in Scientific Research 2014-2015.

[16] http://econpapers.repec.org/article/pkpabetsr/Impact Factor: 0.119

[17] Published Paper in the title of "Biologically Inspired Intelligent Robots Using Artificial Muscles" ,International Journal of pharma and bio sciences, Impact Factor = 5.121(scopus indexed)

[18] Suhas Bachhav, Chetan Chaudhari, Nikhilesh Shinde, Poonam Kaloge, "Secure Multi-Cloud data sharing using Key Aggregate Cryptosystem for scalable data sharing", International Journal of Computer Science and Information Technologies (IJCSIT), ISSN:0975-9646, Vol. 6 , No. 5, pp. 4479-4482, 2015.

[19] Sivaprasad Manivannan, Muthuselvi, "Efficient Key Management for Enforcing Secure Role Based Access Control on Encrypted Data in Cloud Storage", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), ISSN (Online): 2319-8753, ISSN (Print): 2347-6710, Vol. 4, Issue 5, pp. 3478-3483, May 2015.