International Journal of Research in Advent Technology, Vol.2, No.7, July 2014
E-ISSN: 2321-9637

Data Encryption by Blowfish Encryption Algorithm to Protect Data in Public Cloud

Mr. Bhavesh Rahulkar[#1], Mr. Praveen Shende[#2]
CSE, Chhatrapati Shivaji Institute of Technology Durg, CSVTU Bhilai, India
[1]*er.bvsbvs@gmail.com*
[2]*praveenshende@csitdurg.in*

Abstract— Modern trends have set grow to the status and achievement of cloud computing. Cloud computing tool gives facility of data storage and access for cloud users, but when outsourcing the data to a third party causes safety issue of cloud data so data is protected by restricting the data. Proposed idea is encryption of data to defend and for safe delivery of data in public cloud. Encryption of data is done by Blowfish algorithm of symmetric key technique to protect data from external attacks. In this scheme there is registration for the user to use the data of cloud, with no registration there is no authority for user to use data of cloud because without registration any malicious user can use the data. Encryption is done by the Blowfish algorithm by this technique the data is encrypted/decrypted fast. Aim of this system is "Protecting the Data of public cloud by encryption of data by applying symmetric key algorithm".

Index Terms— Encryption; cloud computing; Blowfish; Symmetric key; data security; BE.

1. INTRODUCTION

Cloud computing development has taken the entire attention of several communities like researchers, student, end user, trade, industry, and government business. Huge data is the most important cause for coming of cloud computing in the time-consuming, everyday lots of data of big amount are uploaded in the digital world which required lots of storage space & computing resources [13]. The word cloud is analogical to internet, the name cloud computing is based on cloud drawings used in the earlier period to be a representation of telephone networks and afterward to symbolize internet in [10]. Nowadays, cloud computing is very famous in Information Technology; it provides enormously huge storage to all variety of data. Cloud computing is the technology that many companies are shifting toward and it is becoming very essential for the IT business [9], around all the companies are adopting this to grip their effort competently.

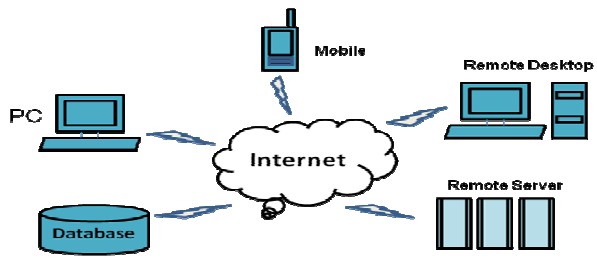

Fig. 1. Cloud Computing

But security issue is most significant concern to protect data in the cloud. The concerns of data security are growing because the existing progress of the internet and the simplicity of data delivery and communication. Data safety is serious in every aspects of our lives; banking information, private documents and businesses. Nearly all of those are processed with technologies and all through network communication. A very essential cause safety concerns are raising is as companies are running core and non-core business functions from side to side other companies [9]. To guarantee confidentiality of responsive data stored in public cloud; a frequently adopted scheme is to encrypt data previously to uploading it to the cloud. As the cloud does not see the keys used to encrypt the data, the privacy of the data as of the cloud is protected [1]. Cryptography is the procedure of achieving security by encrypting/encoding data to make them non-readable, the method of encoding plain text messages into cipher text messages is called as Encryption, there are a number of methods to encrypt the data. Encryption of the data is the way to defend the data from malevolent and not permitted users, encryption of the data can be more than one level, and several levels of the encryption improve the security of the data but increase the encryption charge for the owner. So, there are a number of scheme to care for the data items, and 'Encryption of the Data' is one of them.

Two kinds of encryption system is used in cryptography i) Symmetric key, ii) Asymmetric key. To encrypt/decrypt the data secret or public/private key is used, in symmetric key approach single key is used to encrypt and decrypt the data but in asymmetric key approach dissimilar keys are used to encrypt and decrypt the data. Symmetric key technique is quicker than asymmetric key technique in encryption and decryption of the data. But asymmetric key system is better than symmetric key in security, key management & distribution

standpoint. Asymmetric key is accepted for security of the data since asymmetric key system provides more protection than symmetric key system. This paper proposes the certification of the users and revocation of the malevolent users, revocation of the spiteful users is very much important to defend the data from malicious use; for that cause in this system cloud does revocation of the malevolent users and it is set for the aim that registration of the users. In symmetric key system secret key must be kept private and this key only accessible for two mutual users but in asymmetric key system it is not necessary of the public key to be kept confidential because public key is used to show anyone who gives data to the private key owner. There are several symmetric key algorithms, Blowfish is used for fast encryption/decryption of data [11] and it is symmetric key method thus there is no need of maintaining the public and private key both.

The extremely important thing is that, if more than one user are accepted and they want to get the same document then encryption rate will be enormously high for data owner since owner has to encrypt the same document several times for different users using the user's public key in prior mCL-PKE scheme [1]. To overcome this trouble the extended mCL-PKE system is, data owner encrypts the data only one time and sends the extra information to the cloud for certified users to decrypt the data [1]. But in this proposed system there is no need of extra information for the user to decrypt the encrypted data. Document is decrypted only by secret key given by the owner of the data. After getting the requested data from the cloud user has to decrypt encrypted data by secret key.

2. RELATED EXISTING SCHEME

The previous existing encryption system (mCL-PKE) is certificate-less approach consists of three main parts [1]:

(1) Owner
(2) Cloud
(3) User.

The cloud has three subordinate parts, Encrypted Content Storage, Key Generation Center (KGC), and Security Mediation Server (SEM). Encrypted Content Storage stores the encrypted data, Key Generation Center generates the KGC-key for encryption and Security Mediation Server partially decrypts the encrypted data [1].

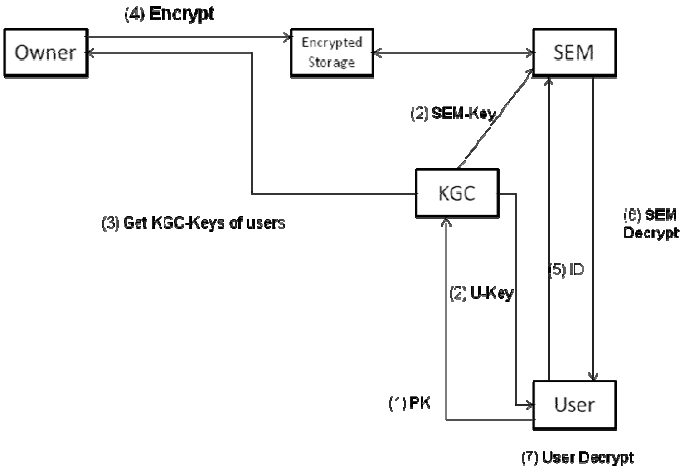

Fig. 2. The basic mCL-PKE scheme [1]

Earlier existing system of mCL-PKE projected single encryption on the data where data-owner encrypts the data and sends to the encrypted content storage with additional information for users now user requests for desired data to the cloud but cloud first checks the correlate information of the requested user if there is existing information then cloud fetches the requested data from the encrypted content storage, but before sending this data to the user cloud decrypts the encrypted data half (cloud partially decrypts the encrypted data not fully) and sends this partially decrypted data to the requested user now user decrypts this data finally by his private key. This process of decryption reduces the time required for decryption by the user, in public key encryption user generates the public & private key and sends public key to the KGC, now KGC generates SEM key for decryption and sends it to the SEM as well as generates KGC-key to send to the owner and owner encrypts the document by this KGC-key. This entire procedure reduces time of the user decryption but the weakness of this scheme is that data can be uncovered by the cloud because cloud has the extra information of the decryption which has to send to the user so cloud can decrypt the complete data as cloud partially decrypts the data and cloud is not fully trusted entity but in this paper cloud brings the data for user and data is still in encrypted form since the requested data is completely decrypted only by the user. The shortcomings of the existing scheme are:

1. There is no registration for the user, so unauthorized users also use the confidential data. Due to this cloud data is not safe.
2. Data is encrypted by the public key as already defined that public key encryption algorithm takes much time in encryption and decryption of the data, so whole process becomes very slow.
3. Here the encrypted data is partly decrypted by the cloud but cloud is not considered as trusted unit, so data is not safe in this way of this system.

Private data can be seen by the cloud that owner and user never want.

3. PROPOSED SCHEME

In this paper the proposed method is data encryption by blowfish algorithm and it is extended from the previous proposal of mCL-PKE, mCL-PKE system is based on certificate-less encryption and user is not certified by any authorized entity but in this plan there is registration for user, registration of the user also assures security of the data in cloud, accordingly only certified one can use the data. This scheme addresses the drawbacks of the mCL-PKE scheme. In this system user has to register first by the owner to get the confidential data. The elementary process is, owner encrypts the data by secret key and sends to encrypted storage, cloud fetches the requested data from encrypted storage and gives this document to the requested user.

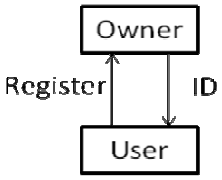

Fig. 3. Certification of the user

Now user decrypts that encrypted data which is still in encrypted form unlike decryption of the data by cloud of existing scheme since cloud does not decrypt the data i.e. user only decrypts encrypted data through the given secret key, after finishing the decryption by the user data is finally decrypted. Using blowfish encryption method the data is secured and entire practice becomes fast also since data is encrypted/decrypted by secret key and secret key encryption/decryption is extremely quick as compare to public key encryption. In this planned scheme there are three entities (1) Owner, (2) Cloud and (3) User, Cloud has two sub parts they are (1) Encrypted storage (2) Verification center.

Encrypted Storage is used as storage space for data, data is encrypted and sent in encrypted storage by the owner and Verification Center ensures requested user is authorized or not if user is registered by owner then only user is authorized for using data otherwise user is revoked by verified center. Cloud is divided into two units to lessen the time required for entire process. Storage of the encrypted data into encrypted storage and verification of the users by Verification center lessen the entire time of the complete method.

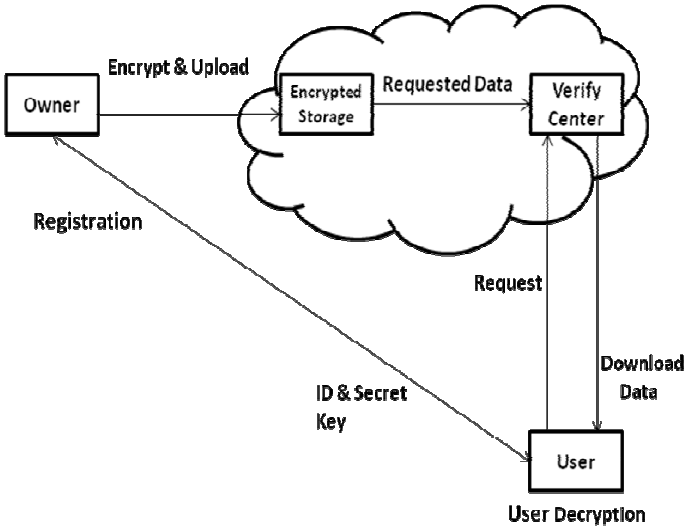

Fig. 4. Blowfish Encryption (BE) scheme

The fundamental method is Encryption of the documents means cryptography technique is applied on the data, for encryption secret-key method is used in this *BE* scheme and to apply secret-key approach blowfish algorithm is used in this system because blowfish algorithm is very fast in encryption & decryption as compare to other secret-key algorithms [11]. It is extended from the previous schemes of "Privacy Preserving Delegated Access Control in Public clouds" and the mCL-PKE scheme of "An Efficient Certificate-less Encryption for Secure Data Sharing in Public Clouds" but in *BE* scheme there is certification of the users which is not in mCL-PKE scheme. In this technique owner encrypts the data using secret key, here the encryption is done by only owner of data, and decryption is done only by the user. After encryption owner stores the documents to the Encrypted Storage, when user requests any document to the cloud, verification center first checks the user whether user authorised or not, if user is authorised then it fetches the requested document from the encrypted storage and sends this data to the user, now user downloads & decrypts that encrypted document. In this technique the Blowfish algorithm is used which supports symmetric key approach, Blowfish algorithm is very easy to implement and it enhances the speed of the complete process of *BE* scheme [11], here Blowfish algorithm is used for data encryption & decryption.

4. EXPECTED RESULTS

In this section, first presents the basic mCL-PKE scheme and compares with improved *BE* scheme, the existing scheme of public key encryption is certificate-less scheme (mCL-PKE), in which user's certification is not necessary which reduces the management cost but this scheme compromises to the malicious users, any malicious user can access the data for malicious use. The shortcomings of this scheme is addressed by the improved scheme of *BE*

system, in which user must be registered by the owner then only is able to access the documents. So this ideology enhances the security of the data. The previous mCL-PKE scheme proposed the single encryption and half decryption is done by the cloud and remaining half is decrypted by the user, this scheme is proposed to reduce the decryption time of the user, but partially decryption of the data by cloud reduces the security of the contents, but in *BE* scheme there is registration is needed for using the cloud data and decryption of the data is done only by the user, hence security is high in enhanced *BE* scheme and overall process is very easy and fast to execute. The overall result comes that security is very high as well as complete process is fast in this proposed *BE* system as compare to previous mCL-PKE scheme.

5. CONCLUSION

In scheme of blowfish encryption the certification of the user offers high security to the data, and symmetric key approach (Blowfish Algorithm) is very easy to implement and also offers high speed to the whole process [11]. The future enhancement of this scheme is that blowfish algorithm can also be used for large size of data for fast encryption and decryption, so it will be helpful for improving the speed and security of the big size data. *BE* scheme offers security as well as fast encryption & decryption in which Blowfish algorithm is used to encrypt/decrypt the data because this symmetric key algorithm is so fast [11], so *BE* system uses symmetric key algorithm to provide security and reduce the overall process time.

REFERENCES

[1]. Mohamed Nabeel, Elisa Bertino, Seung-Hyun Seo, Xiaoyu Ding Members of IEEE "An Efficient Certificate-less Encryption for Secure Data Sharing in Public Clouds" June 2013.

[2]. Zhiguo Wan, Jun'e Liu and Robert H. Deng. Senior Member, IEEE "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" April 2012.

[3]. Mohamed Nabeel, Student Member, IEEE, Ning Shang, Elisa Bertino Fellow, IEEE "Privacy Preserving Policy Based Content Sharing in Public Clouds" 2013.

[4]. Mohamed Nabeel, Elisa Bertino Fellow, IEEE "Privacy Preserving Delegated Access Control in Public Clouds" 2013.

[5]. Yang Tang, Patrick P.C. Lee, Member, IEEE, John C.S. Lui, Fellow, IEEE, and Radia Perlman, Fellow, IEEE "Secure Overlay Cloud Storage With Access Control and Assured Deletion" November/December 2012.

[6]. Sushmita Ruj, CSE, Indian Institute of Technology, Indore, India, Milos Stojmenovic, Singidunum University, Belgrade, Serbia, Amiya Nayak, SEECS, University of Ottawa, Canada, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" 2013.

[7]. Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud" March 2012.

[8]. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng "Attribute-Based Encryption with Verifiable Outsourced Decryption" 2013.

[9]. Amal AlKadi, Hanouf AlYahya, CIS Department, Prince Sultan University, Riyadh, Saudi Arabia, "Data Security in Cloud Computing".

[10]. Luit Infotech Private Limited Bangalore, India, "Luit Infotech SaaS Business Software".

[11]. Diaa Salama, Hatem Abdual Kader, Jazan University, Kingdom of Saudi Arabia, and Mohity Hadhoud, Minufiya University, Egypt, "Studying the Effects of Most Common Encryption Algorithms".

[12]. Atul Kahate, Tata McGraw Hill Education Private Limited, Second Edition, "Cryptography and Network Security".

[13]. Ajith Singh. N, Department of computer science, Karpagam University, Coimbatore, India, M. Hemalatha, Department of software systems & research, Karpagam University, Coimbatore, India, "Cloud computing for Academic Environment".

First Author

Mr. Bhavesh Rahulkar received the BE (Computer Technology) From RTM Nagpur University, Nagpur (M.H.) in 2008 and pursuit for M.Tech. (Computer Science) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India. He is now attending the M.Tech.-CS course in CSIT and his research interest include Computer Networks, with Cloud Computing and programming languages (JAVA, PHP, **.**NET) and Web Development, DBMS.

Second Author

Mr. Praveen Shende, Asst. Prof. CSE Dept. C.S.I.T. Durg, India, received B.E. (Computer Sc.) in year 2009 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, His interests are Programming Languages (Java, PHP, Joomla) Cloud Computing and DBMS, Computer Networks, Computer System Architecture.