Digital Signature based Improved SECO Environment to Enhance Data Security in Cloud Computing

Swaranjeet Kaur
M.Tech Research scholar
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab

Amritpal Kaur
Assistant Professor
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab

ABSTRACT
Cloud computing itself is as a Service Model which means that everything is available on-demand over the internet. Every type of resources such as hardware and software resources can be accessed from anywhere by just connecting any network device to the internet. As it is based on internet services, security becomes major issue in this. Number of algorithms has been introduced to make secure user's outsourced data on cloud. To solve this security issue, a secure and efficient data collaboration scheme SECO was introduced in cloud computing. This scheme resolves the security issue at a large extent but security needs to be enhanced more as security in itself is a vast area for research. In this paper, a Secure SECO Technique is proposed. The purpose of this technique is to enhance security by implementing digital signatures scheme in SECO scheme. This proposed technique helps to maximize the security of user's outsourced data on cloud.

General Terms
Cloud Computing, Digital Signatures.

Keywords
Cloud Computing, SECO environment, Secure SECO environment, Certification Authority, Digital Certificates and Security Analysis.

1. INTRODUCTION
There is numerous definition of Cloud Computing. According to U.S National Institute of Standards and Technology (NIST) — Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [1].Cloud computing is made up of two words cloud or computing. The word cloud is used to represent the network whose internal setup is not known to you. For example, in network diagrams, the network of Internet Service Provider (ISP) is represented by cloud. Any simple internet or virtual private network (VPN), all networks are represented by cloud. The word computing means to calculate. Computing comprises data processing and calculations which are performed by using computers. This computing can be done on your local computer or on a centralized server or it can be done on both local and centralized server in distributed form according to your design. There can be one server or group of servers to provide network services. There can be different storage systems and database systems according to network size. Number of applications or services such as mail services can be deployed on these servers. That means, computing is done by client devices such as computers or laptops to use these applications or services and computing is done by network servers to provide these applications or services. Now by combining these two words, cloud or computing, it can be concluded that data related processing and calculation or computing is done on the cloud. It means this computing takes place on such a network about which there is no information known to you, i.e., number of servers providing services, configuration of these servers, where data is to be stored etc all these type of information is not available to you. It is the responsibility of cloud service provider. Cloud computing is pay-as-you-go model in which users are charged on the basis of usage. The basic requirement in cloud computing is network connection. It does not matter where you are, if internet connection is available then connect your network device such as mobile phone, laptop, tablet and desktop to the internet and enjoy the cloud services according to your demand. In other words, cloud computing can be defined as Computing as a Service where client computers or other devices access shared resources, software or information by connecting to the internet. The biggest advantage of outsourcing data to cloud is that user can access data whenever and wherever using any network device [2].

1.1 Cloud Computing Services
There are three types of services which are provided by cloud service provider.

1. Software as a Service (SaaS) in which software is provided over the internet and there is no need to install the software by the customers [3].
2. Platform as a Service (PaaS) in which operating systems and middleware services are provided over the internet and customers can build their own applications [4].
3. Infrastructure as a Service (IaaS) in which computational resources; storage systems and network systems are provided over the internet as a service [5]. This model is based on virtualization technology.

1.2 Five characteristics of cloud computing
1. Broad Network Access – It means you can access cloud services from anywhere in the world.
2. Rapid Elasticity – Cloud is scalable or elastic, i.e., whenever you need it, it is able to scale up or down as per your requirements.
3. Measured Service (pay as you go) – It means whatever amount you are using, it will be charging you only for that amount.
4. On-Demand Self Service – Cloud computing is available on demand so whenever you need it, it is immediately available to you within two or five minutes.
5. Resource Pooling – Number of resources are pooled in cloud computing for multiple consumers.

There are many issues in cloud computing but the major concern is security as user's data is outsourced on the cloud. When user wishes to upload the data on cloud and if there is no security then user's critical data is at risk because without security any unauthorized user can trace the personal data of cloud user. So security becomes the important factor in cloud. There are number of security issues or concerns associated with cloud computing. The issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. Cloud providers must ensure that their infrastructure is secure and customer's data and applications are protected. Customers must ensure that provider has taken correct security measures to protect their information.

2. RELATED WORK

Data security in cloud computing is major area of research. The survey shows that from time to time, the researchers are providing efficient algorithms and many encryption techniques to enhance the data security on cloud.

Shashank Bajpai, et al. [6] proposed a model called Fully Homomorphic Encryption on cloud computing to enhance its security. This model accepts encrypted input and blind processing is performed on encrypted input without being aware of its contents. Then retrieved encrypted data can only be decrypted by the user who initiates the request.

Akshay A. Pawle, et al. [7] proposed new face recognition system (FRS). There are many authentication techniques including traditional and biometric but has some drawbacks. This proposed technique has overcomed all drawbacks of traditional and other biometric authentication techniques. This proposed technique enables only authorized users to access data or services from cloud server.

Xin Dong, et al. [8] proposed a secure and efficient data collaboration scheme SECO. In SECO, a two-level hierarchical identity based encryption (HIBE) is employed to guarantee data confidentiality against untrusted cloud.

D.H. Patil, et al. [9] proposed a Two Factor Authentication Technique with the help of key generated using Diffie-Hellman key exchange algorithm. This generated key is sent to user's mobile device using the number which was provided during registration. First authentication requires user id and password to be matched and second authentication requires a key generated using Diffie-Hellman to be matched after it is entered by the user. The proposed work is highly efficient.

Sunita Rani, et al. [10] proposed an encryption technique called Hybrid Algorithm in order to provide privacy in the cloud. In this paper, Ceaser cipher, RSA substitution algorithm and Mono alphabetic method are combined to encrypt the data on cloud.

3. PROPOSED DIGITAL SIGNATURE BASED SECO ENVIRONMENT

3.1 Need and Significance of Proposed Work

The previous work which is taken under consideration proposed a secure and efficient data collaboration scheme SECO in which a two-level hierarchical identity based encryption is employed. In this scheme first level is Root Private Key Generator(R-PKG) and second level is Domain Private Key Generator (D-PKG). Each domain has number of users. The private keys for D-PKG are generated by R-PKG and D-PKG generates private keys for users. D-PKG has two private keys: a private key and master key and these two keys are used to generate private keys for all users. In this, each user has to provide a unique key or private key to upload data and then this key would be matched before downloading the same data. The main problem in this scheme is that if user id & password and unique key both are hacked then sensitive data of a user is at risk. So, the main focus of proposed work is to implement digital signatures to make SECO scheme more secure.

3.2 Proposed work

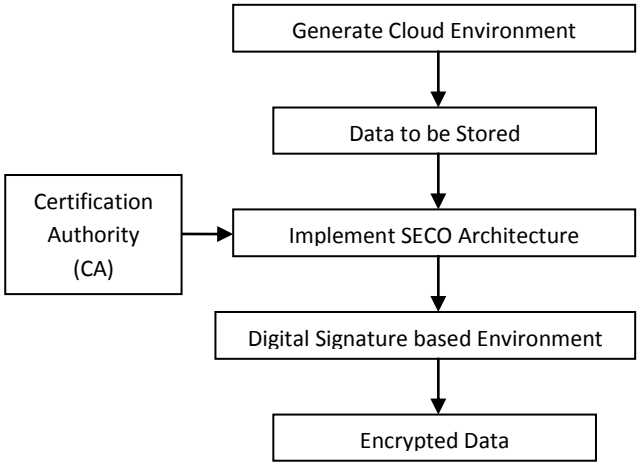

Figure 1: Flow of the Work

The proposed work is to implement digital signatures on SECO environment by using .NET environment to enhance data security.

In this work, a local client server environment is generated to implement cloud environment. This environment provides users to access the cloud with user id and passwords. Users can upload and download the data from cloud. In this work, double encryption is done by using SECO architecture and certification authority to encrypt the data.

3.2.1 Certification Authority & Digital Certificates

Certification authority is used to create the digital signatures of each user and issues digital certificates to the cloud users. Digital certificates provide complete security solution by assuring the identity of users. The contents of digital certificates are divided into two sections: Data Section and Digital Signature Section.

Data Section: It contains the following information:

1) The version number – It is based on standard supported by the certificate.

2) The serial number – Every certificate issued by certification authority (CA) has a unique serial number.

3) Public key information – It includes algorithm used and representation of keys.

4) Distinguished name (DN) of CA – It is considered as certificate issuers.

5) Time duration – It is the validity of certificate.

6) Certificate extensions – It is optional and contains the additional information..

Digital Signature Section: It includes the following information:

The cryptographic algorithm – This algorithm is used to create the digital signature. Digital signature for Certification Authority (CA) is obtained by hashing all the information in certificate and encrypting it with certification authority (CA) private key.

3.2.2 *Digital Signatures and how does they work*

Digital signature scheme is a mathematical process which is applied to an electronic document. This process generates a code (hash code) which is specific to a particular document and thus digital signatures can never be copied to any other documents. Digital Signature of a user varies from document to document thus authentication is assured. It involves two encryption keys: a private key to sign the message or document and a public key to verify signatures.

The sender's message can be first encrypted using encryption algorithm and then it can be digitally signed. Digital signature works as follows:

Step 1: A hash code or message digest of sender's message is calculated by using any hashing algorithm.

Step 2:This hash code is encrypted using sender's private key and thus digital signatures are generated and attached to the encrypted message. At this step, the document is digitally signed document.

Step 3: When user wishes to upload the data on cloud then two types of uploading can be done: SECO and Secure SECO uploading.

a) In SECO uploading, information related to data uploading is filled out and data is encrypted using single encryption, i.e., only by Diffie-Hellman key exchange algorithm.

b) In Secure SECO uploading, information related to data uploading is filled out and data is encrypted using double encryption, i.e., firstly data is encrypted by Diffie-Hellman key exchange algorithm and then digital signatures are implemented of a particular user with encrypted data.

Step 4:Before encrypted data is uploaded successfully on the cloud, user has to provide a unique key or private key to upload the data on cloud.

Step 5: When user wishes to download the data from cloud then also two types of downloading can be done: SECO and Secure SECO downloading.

a) In SECO downloading, user has to provide his/her own unique key or private key which is matched with the unique key that has been provided before uploading and if both keys are matched then an encryption key is provided to the user on cloud server. By using this encryption key, user is able to download the data from cloud.

b) In Secure SECO downloading, user has to provide his/her own unique key or private key which is matched with the unique key that has been provided before uploading and if both keys are matched then message will be displayed that signatures have been sent to your Registered ID.

Step 6: Now user has to open his/her Gmail account and use the signatures to download the data from cloud.

4. RESULTS & COMPARISON

The analysis of proposed scheme has been done on the basis of different types of analysis**.**

4.1 Security Analysis

The security analysis of proposed scheme is done by analyzing the various security properties such as Data Confidentiality, Authentication and Integrity of data.

1) Data Confidentiality: Data Confidentiality of proposed scheme can be analyzed when it is compared with other encryption algorithms such as Advanced Encryption Standard which uses the symmetric key to encrypt the data.

In proposed scheme, data is double encrypted and any malicious user or cloud service provider can never access the cloud user's data because they do not have the sender's public key to decrypt the signatures of a valid sender and this key is only known to the data owner. Digital signatures can never be copied as written signatures can be copied to multiple documents because digital signatures are specific only to a particular document.

2) Authentication: Before having an access to encrypted data, the user's identity has been checked whether it is valid user or invalid. In proposed scheme, this authentication is done using digital signatures in which message digest is encrypted using sender's private key and decrypted using sender's public key. If any malicious user tries to access the cloud user's data then he/she would not be able to access the data because if sender's public key cannot decrypt the signature then it was not encrypted with the sender's private key. Thus Digital Signatures provide complete security by authenticating the exact user and malicious user would not be able to harm the cloud user's data.

3) Integrity: Integrity assures that digitally signed messages has not been tempered or modified during the transmission. In proposed scheme, if any malicious user changes or modifies the user's data then after decryption of data, the decrypted digital signature and hash code would not be equal to the original hash code and digital signature. Thus the valid user will come to know that his/her data has been modified by any unauthorized user or malicious user. So, in proposed scheme digital signatures provide complete security by assuring the integrity of data and data on the cloud is completely secure.

4.2 Analysis on the basis of Data Loss

1) SECO Environment: In SECO environment, if authentication system (user id and password) information (14%) of cloud user is hacked then there will be 86% data loss stored on cloud, i.e.,100% data loss. In other words, if any malicious user gets the user id & password and unique key of cloud user then malicious user can login successfully and the cloud user's data can be easily decrypted as a key for downloading the data is provided on the same cloud server. So, user's data is at risk.

2) Secure SECO Environment: In proposed Secure SECO environment, if authentication system information (14%) of cloud user is hacked then also the data loss will be 0%, i.e., only authentication information (14%) will be hacked and 86% of data stored on cloud is safe until Gmail account gets hacked. In this environment, signatures of a respective cloud user are sent to his/her registered ID instead of providing downloading key on same cloud server. Thus data is more

secure in this proposed scheme. This analysis has been done by conducting the following case study:

Case Study:

Let us consider, total number of users in cloud is 10 named as user1, user2 and so on up to user10 respectively. All the users saved their information to cloud using both SECO & Secure SECO Environment.

Out of 10 users, accounts of 6 users have been hacked by malicious users that mean 6 attacks are there under consideration. The following analysis has been done to measure the performance of secure environment.

Table 1: Attack Analysis

Users	Attack Information (Yes/No)	Authentication Successful (Yes/No)	Data Loss	
			SECO	Secure SECO
user1	No	Not Applicable	NA	NA
user2	Yes	Yes	100%	No
user3	No	Not Applicable	NA	NA
user4	Yes	Yes	100%	No
user5	Yes	Yes	100%	No
user6	No	Not Applicable	NA	NA
user7	Yes	Yes	100%	No
user8	No	Not Applicable	NA	NA
user9	Yes	Yes	100%	No
user10	Yes	Yes	100%	No

According to above analysis:
It is clear that when malicious users gets ID & password information then there is 100% chances for loss of information in SECO but there is no chance in Secure SECO because data will be accessed only when user have their signature information which already sent on the registered mail account while data is being uploaded. In the above analysis 60% attack is on the cloud environment out of 100%.

The below figure 2 shows the percentage analysis based on authentication information loss and uploaded data loss by comparing the SECO Environment and proposed Secure SECO Environment.

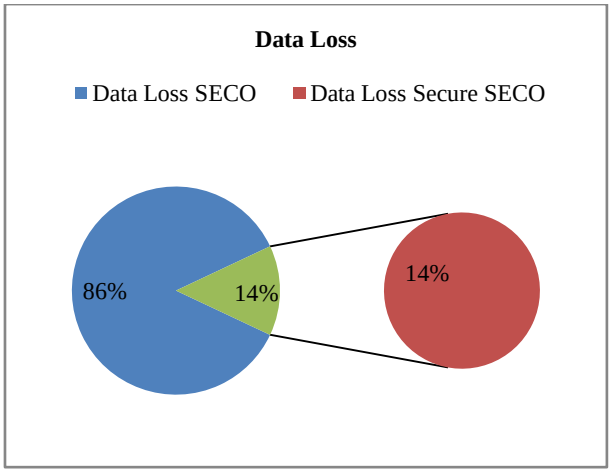

Figure 2: Analysis based on Authentication & Data Loss

5. CONCLUSION & FUTURE WORK

As the usage of cloud computing still continues to rise, the need for data security on cloud is increasing. In this thesis, a Secure SECO Environment using Digital Signatures has been proposed to enhance the security of data stored on the cloud. In this proposed work, data gets double encryption and it is difficult for malicious user to gat easily access to cloud user's data until signatures are not matched. So, proposed technique is more secure. Result analysis also shows that proposed technique can effectively improve the security of user's data on the cloud.

In future, file type can be explored further. As video encryption is not included in this thesis work or video files cannot be uploaded on cloud in this proposed work. So, any encryption algorithm can be used to provide encryption for videos.

6. REFERENCES

[1] Mohsin Nazir, "Cloud Computing: Overview & Current Research Challenges", IOSR Journal of Computer Engineering (IOSR-JCE), ISSN 2278-0661, Vol. 8, Issue 1, pp. 14-22, 2012.

[2] Remya Rajan, "Efficient and Privacy Preserving Multi User Keyword Search for Cloud Storage Services", International Journal of Advanced Technology & Engineering Research (IJATER), ISSN 2250-3536, Vol. 2, Issue 4, pp. 48-51, July 2012.

[3] Ashalatha R, "A Survey on Security as a Challenge in Cloud Computing", International Journal of Advanced Technology & Engineering Research (IJATER), ISSN 2250-3536, Vol. 2, Issue 4, pp. 1-4, July 2012.

[4] Shobha Rajak, Ashok Verma, "Secure Data Storage in the Cloud using Digital Signature Mechanism", International Journal of Advanced Research in Computer Engineering & Technology, ISSN 2278 – 1323, Vol. 1, Issue 4, pp. 489-493, June 2012.

[5] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN 2278-1323, Vol. 2, Issue 2, pp. 652-661, Feb 2013.

[6] Shashank Bajpai, Padmija Srivastava, "A Fully Homomorphic Encryption Implementation on Cloud

Computing", International Journal of Information & Computation Technology (IJICT), ISSN 0974-2239, Vol. 4, No. 8, pp. 811-816, 2014.

[7] Akshay A. Pawle, Vrushsen P. Pawar, "Face Recognition System (FRS) on Cloud Computing for User Authentication", International Journal of Soft Computing and Engineering (IJSCE), ISSN 2231-2307, Vol. 3, Issue-4, pp. 189-192, September 2013.

[8] Xin Dong, Jiadi Yu, Yuan Luo, "Achieving Secure and Efficient Data Collaboration in Cloud Computing", Vol. 978-1-4799-0590-4/13/$31.00 ©2013 IEEE.

[9] Sunita Rani, Ambrish Gangal, "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", International Journal of Computer Science and Information Technologies (IJCSIT), ISSN 0975-9646, Vol. 3, No. 3, pp. 4302 – 4304, 2012.

[10] D.H. Patil, Rakesh R. Bhavsar and Akshay S. Thorve, "Data Security over Cloud", International Conference on Emerging Frontiers in Technology for Rural Area (EFITRA) , Proceedings published in International Journal of Computer Applications® (IJCA), pp. 11-14, 2012.