On Cloud Security using Biometric Cryptographic Techniques

Sunil Kumar  
Computer Science & Engineering  
CGC - College of Engineering, IKG-PTU, Jallandhar, Punjab, India

Vijay K. Lamba  
Electronics & Comm. Engineering, Global College of Engg. & Tech., Anandpur Sahib, Punjab, India

Surender Jangra  
Computer Science & Applications  
Guru Teg Bahadur College, Sangrur, Punjab, India

Punit Soni  
Computer Science & Engineering  
HCTMTC, Kaithal, Haryana, India, IKG-PTU, Jallandhar, Punjab, India

ABSTRACT
Cloud computing is one of the best on-demand network access service to large shared pool of computing resources in today’s world. There are several widely recognized economic benefits of cloud computing. Cloud computing helps users avail combined benefits of three computing models storage (Infrastructure as a Service), operating system (Platform as a Service) and software(s) (Software as a Service) at their own premises without need to have them at their own hardware level. Apart from these economic benefits, public clouds still haven’t seen widespread adoption, especially by enterprises. Most large organizations today run private clouds, in the sense of virtualized and geographically distributed data centers, but rarely rely primarily on externally managed resources [2]. The major reason behind this is the security concerns involved in existing cloud infrastructures which includes hardware failures, software bugs, power failures, mis-configuration of servers, malware and insider threats[2]. The paper focuses on various biometric cryptographic techniques for cloud security and to compare them on various parameters possible.

Keywords  
Cloud computing, Cloud security, authentication, biometrics, cryptography.

1. INTRODUCTION
The research area of cloud computing is relatively young. The use of cloud computing has increased at a rapid pace in past decade. NIST [1] defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Ensuring security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may not be completely trusted. Cloud computing provides features like low cost storage, easy accessibility of data, flexibility (anytime / anywhere / any resource) and mobility (on the go) to its users, thereby increasing their benefits. It acquires a large number of users which require either infrastructure (servers, storage space, bandwidth etc. Infrastructure as a Service) or operating system (Platform as a Service) or some licensed application software(s) (Software as a Service). Clouds may be broadly classified in following three ways:

a) Public Cloud  
b) Private Cloud  
c) Hybrid Cloud

<table>
<thead>
<tr>
<th>Type of Cloud</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Cloud</td>
<td>Computing Infrastructure is at third party’s premises and is not visible to the user. Moreover, user doesn’t have any control over the shared computing infrastructure.</td>
</tr>
<tr>
<td>Private Cloud</td>
<td>Computing Infrastructure is dedicated to the particular organization and is not shared with other organization. Private clouds are more expensive and more secured.</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>Being the combination of both the public and private cloud, hybrid cloud enjoys the advantages of both.</td>
</tr>
</tbody>
</table>

1.1 Cloud Computing Components
The cloud computing model consists of five characteristics, three delivery models, and four deployment models [1]. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured services [6]. However, security concerns related to confidentiality and integrity puts hindrances in path of users to go for cloud computing. As the center security element, authentication plays a vital role in an advanced computing model. Hence, identity theft is one of the major issues in the cloud systems [2]. In past, confidential data stored on personal computer has been physically protected and checked for authentication physically as well as using username and passwords. However in today’s world of cloud computing since the data is stored at third party’s server where physical security is not possible, moreover username and passwords can also be hacked or forgotten. To many consumers, the most recognized model of cloud computing is public cloud, where services are provided in a virtual environment using shared physical resources and are accessible over a public network such as the Internet.
While the cloud may be flexible and cost-efficient, a lack of data safeguards and compliance standards makes security the largest obstacle to leap, therefore, the most important challenge to cloud is security. There are no possible instances where data can be allowed to leak to the unauthorized parties and the purpose can only be fulfilled by deploying an effective and efficient authentication mechanism that can ensure the security of data stored over cloud by the user.

Once an authentication module is created, user can be ensured about the safety of the important data. The major security issues with cloud are:

1. Privacy and Confidentiality - Once the users outsource data to the cloud, there must be some assurance that data is not accessible to unauthorized users at any cost. The cloud user should be confident enough that data stored on the cloud will be confidential. Only rigid security policies at cloud service provider level can guarantee this.

2. Security and Data Integrity - Data security can be provided using some encryption and decryption techniques. Providing the security of the data, cloud service provider should also implement mechanism to monitor integrity of the data at the cloud.

1.2 Parameters affecting Cloud Security

There are several security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [8]. Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

1.3 Security Issues faced by Cloud Computing

Whenever a discussion about cloud takes place, there is always much to do regarding its security. There may be chances that users sensitive data stored on cloud may be lost or hacked. There is also a possibility where a malicious user can penetrate the cloud by imitating as a genuine user, there by infecting the entire cloud. This leads to affect many customers who are sharing the infected cloud. There are four types of issues raise while discussing security of a cloud. These are Data issues, Privacy issues, Infected applications and last but not the least Security issues. Clients always keep their significantly valuable data on clouds that require authentication at the login interface of the cloud which can be done more reliably using physiological and behavioural biometric traits of a human being like fingerprints, face, iris, gait, ear, palm-prints, signature etc. instead of using passwords and PINs. Advancing one step further towards having secure clouds, [4], [6], [13], [14], and [21] have used these biometric traits to crate biometric cryptographic keys to provide encryption based security in a cloud computing environment. DES, Blowfish, Triple-DES, DSA, RSA and SHA-1 are the algorithms that can be employed for deployment.

1.4 Data Security Techniques

1.4.1 Symmetric Techniques

DES: DES stands for Data Encryption Standard. It applies a 56-bit key to each 64-bit block of data. It was the first encryption standard to be approved by NIST [1]. This Method can run in number of modes and requires 16 rounds or controls, even though this is designed with “strong” encryption. We have used DES algorithm with destruction-editing approach for providing data security with integrity [17]. Each round in the deals with uses a separate 48-bit round key which is produced from the consistent cipher key according to the DES techniques. The Data Encryption Standard (DES) is a formerly transcendent symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of present day cryptographic systems.DES is the block cipher an algorithm that takes a fixed length string of plaintext bits and changes into a series of muddled operations into another cipher-text series of bits with the same length. On account of DES, for the most part, the block size is 64 bits. DES additionally utilizes a key to altering the change, so that decryption must be performed by the individuals who know the specific key used to encrypt. At the present DES issued to be unconfident for multiple applications, and therefore it has been replaced by the Advanced Encryption Standard (AES) [18].

BLOWFISH: It is symmetric encryption algorithm. It have 64 bit block cipher developed by Bruce Schneider; enhanced for 32-bit mainframes with huge data stores, it is greatly faster than DES on a Power PC-class machine. Key lengths can differ from 32 to 448 bits in range. Blowfish, having 16 rounds, is easily accessible and is developed as an alternate for DES or IDEA [18].

3DES: In Triple DES (3DES) Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher encryption is discussed with the development of the Data Encryption Standard (DES) cipher techniques. TDES uses a block size of 64 bits and operate 48 processing round corresponding to DES. In 3DES three times iteration is produced to improve the encryption and security level [18]. It makes three encryption and decryption permits done the block using DES 56 bit keys.

1.4.2 Asymmetric Techniques

RSA: Ronald Rivest, Adi Shamir and Leonard Adleman designed the RSA algorithm 1977 cryptosystem uses the properties of the generative homomorphism encryption. RSA key size is having 1024 bit. RSA is generally used in public key techniques and is accomplished to maintain encryption and digital signatures. RSA provides the best security plan by encrypting the data that is confidential; this is the motivation behind why the enormous administration suppliers like Google mail, Yahoo mail and many others are using this algorithm to providing security to their clients [19].

DSA: It presents an autonomous investigation of security algorithms in cloud computing which provides the particular technique to secure data on cloud computing. The DSA (Digital Signature Algorithm) technique gives digital signature capabilities employed for the authentication of messages [11]. DSA is a Federal data processing Standard for digital signatures, DSA was introduced by the NIST. It is used to detect the unauthorized alterations to the data send by the source to the receiver.
**Diffie-Hellman Key Exchange:** Diffie-Hellman introduces secret-key exchange protocol only. It is not for authentication or digital signatures and it is public key exchange methods, it uses of the discrete logarithm problem. Actually the sender and receiver set the secret key [12]. These techniques protect the data confidentiality and safe and security, Diffie Hellman Key Exchange method to link organization and Elliptic curve cryptography for data encryption

The rest of the paper is organized as follows. Related Work is given in section II. Comparative analysis of security techniques is presented in section III. Section IV presents concluding remarks followed by Acknowledgements in Section V and References in Section VI.

### 2. RELATED WORK

Sugumaran et al [10] discussed techniques that are implemented to protect data and proposed architecture to protect the data in the cloud. Their architecture was developed to store data in the cloud in encrypted form using a block cipher based symmetric key cryptography technique which gives faster speed of access.

Monikandan et al [11] have described an encryption algorithm to address the security and privacy issues in cloud storage to protect the data from restricted access. Data can be attacked in two ways. An insider attack is an administrator having the possibility to hack the user’s data. Outsider attack is third party can access the user’s data. The Author proposed a symmetric encryption algorithm, integrating substitution cipher and transposition cipher, to protect the data stored in cloud storage from the unauthorized access. Their proposed technique is converting plain text into the corresponding ASCII text of each alphabet and the key size ranges from 1 to 256. Symmetric encryption has the speed and computationally efficient to handle encryption of large volumes of data in cloud storage.

Prashant et al [12] have proposed a “Three way mechanism” ensures all the three protection scheme of authentication, data security and verification at the same time. They have used digital signature and Diffie Hellman key exchange with AES algorithm to protect confidentiality of data stored in the cloud.

Sanjukta Pal et al. [13] have discussed cryptography combined with the fingerprint biometrics. They have generated the encryption key using fingerprints and deduced the information from the key using fingerprint matching algorithm. To implement the above concept, sender’s recent fingerprints have been used to construct the key. For decryption, the sender’s Database fingerprint images, which are already kept by receiver at receiver’s end, have been used.

S. Kavin Hari Hara Sudhan et al. [14] have discussed AES and RSA data security algorithms for cloud security. They have used two different algorithms, for asymmetric key encryption and decryption RSA is used and for symmetric key encryption AES algorithm is being used. They have proposed two-phase technique in Phase-1 user have to register on the cloud. During registration the biometric sample is given from the consumer side that is going to be encrypted by public key which is received from the authentication server where it is decrypted by the private key of its own. Then the decrypted template is once again encrypted by the server’s private key and stored in the database along with user name and password for further usage. In phase-2 while login after the first registration the same principle is followed.

Thakur et al. [15] discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings. The presented comparisons take into consideration the behaviour and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size, and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used.

Alanazi et al.[16] has done the comparative analysis of three Encryption Algorithms (DES, 3DES and AES) within nine factors such as Key Length, Cipher Type, Block Size, Security, Possible Keys, Possible ASCII printable character keys and Time required to check all possible keys at 50 billion keys per second etc. This study concludes that AES is better in performance as compared to DES and 3DES.

### 3. COMPARITIVE ANALYSIS

We have discussed various techniques that can be used for data security; all these techniques have their own pros and cons. We have compared these techniques based on some well established parameters, which will help us to understand the capability of different security methods available to authenticate data access. Also this will help in studying their effect on cloud’s performance. Following are some of the parameters we have taken to compare the above mentioned techniques:

- **Key Length:** Key length is the size (bits) of the key used in a cryptographic algorithm. The larger the key size, higher the security, but may decrease encryption/decryption speed.
- **Block Size:** Larger block sizes mean greater security but reduced encryption/decryption speed for a given algorithm.
- **Possible No. of Keys:** This depends upon key size. These are actually the possible permutations of a key.
- **Speed:** Speed of any cryptography algorithm is always a major concern and depends upon the key size, block size and number of rounds.
- **Key Type:** key type may be private key or public key depending upon the type of cryptography i.e. symmetric or asymmetric cryptography.
- **Cipher Type:** Cipher type may vary among block cipher, substitution cipher, transposition cipher etc.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>DES</th>
<th>3DES</th>
<th>AES</th>
<th>Blowfish</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Size</td>
<td>56</td>
<td>112,58</td>
<td>128, 182, 256</td>
<td>32-448</td>
<td>1024 to 4096</td>
</tr>
<tr>
<td>Number of Rounds</td>
<td>16</td>
<td>48</td>
<td>10(128), 12(192), 14(256)</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>Key Type</td>
<td>Private key</td>
<td>Private key</td>
<td>Private key</td>
<td>Private key</td>
<td>Public Key</td>
</tr>
</tbody>
</table>

The rest of the paper is organized as follows. Related Work is given in section II. Comparative analysis of security techniques is presented in section III. Section IV presents concluding remarks followed by Acknowledgements in Section V and References in Section VI.
4. CONCLUSION
We have discussed various techniques that can be used for data security with their respective advantages and disadvantages. A comparative analysis is given based on already established parameters, helping us to understand the capability of different security methods for cloud security. We have taken some parameters but there can be few more to be considered in future which may be power consumption, throughput, memory usage, flexibility and type of cloud. Also, MD5 and SHA-1 can be taken into consideration for implementing cloud security.

5. ACKNOWLEDGMENTS
Authors are really grateful to CGC College of Engineering and IKG-PTU, Jallandhar for providing excellent platform for the research.

6. REFERENCES