Privacy Management in Cloud by making use of Homomorphic Functions

S. G. Sutar
Asst. Professor
Department of CSE
Annasaheb Dange College of Engineering and Technology, Ashta- India

G. A. Patil
Asst. Professor
Department of CSE
D. Y. Patil College of Engineering and Technology, Kolhapur- India

ABSTRACT
Cloud computing is new era, attracting peoples for different services providing in cost effective manner. Privacy management is one of the critical issues in cloud when these services accessed through untrusted service provider or third party. There is risk with sending personal information to such parties. We proposed a strong privacy preserving scheme for processing of personal information at untrusted service provider or third party end in the cloud. With making use of homomorphic encryption function on personal information, the proposed scheme maintains confidentiality of personal information sent by the cloud users to untrusted service provider or third party. While registering to a cloud, the personal information sent by cloud user is encrypted by making use of homomorphic function. cloud server receives this information in encrypted form and decrypts it by using homomorphic decryption function. The personal information of cloud user is stored at cloud server database and general information is created like registration ID. When it requires to access the services from untrusted service provider or third party, it need to login to cloud through such parties. In this, first, information sent by cloud user is encrypted using a homomorphic function and sent to the untrusted service provider or third party along with its general information. The service provider receives the encrypted information and request to cloud server for personal information by providing the received general information. Cloud server encrypts the personal information related to received general information using another homomorphic function and sends it to the untrusted service provider or third party. Now, untrusted service provider or third party compares the personal information received from both, client and server in encrypted form. Moreover, the proposed scheme condenses computation at cloud server by eliminating process of authentication. Theoretical analysis and simulative evolution demonstrate the soundness and effectiveness of the proposed privacy management scheme in cloud computing.

General Terms
Personal Information, Homomorphic Cryptosystem, Cloud.

Keywords
Cloud computing, Homomorphic encryption, Privacy management, Third party in cloud.

1. INTRODUCTION
Cloud computing provides different services like, Software-as-Service (SaaS), Platform-as-Service (PaaS) and Infrastructure-as-Service (IasS) to its users with diminutive cost and effective manner. The reason to become trendier is its ability to create a virtual office that can be run from anywhere.

While using the cloud services it requires to register with personal information that may be used while authentication and authorization process. Also, Cloud is a great target for attackers who may get or examine the personal information during sending and receiving such information, which causes to harm on privacy protection. When third party comes in focus it becomes more crucial to manage it.

Privacy is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights and the European Convention on Human Rights.Personal sensitive information is key factor of privacy [3]. Privacy sensitive information that includes the following [3]:

1. Personally identifiable information (PII): any information that could be used to identify or locate an individual (e.g. name, address) or information that can be correlated with other information to identify an individual (e.g. credit card number, postal code, Internet Protocol (IP) address)[3].
2. Sensitive information: information on religion or race, health, sexual orientation, union membership or other information that is considered private. Such information requires additional safeguards. Other information that may be considered sensitive includes personal financial information and job performance information. 3. Information considered being sensitive PII, e.g. biometric information or collections of surveillance camera images in public places [3].
4. Usage data: Usage data collected from computer devices such as printers; behavioral information such as viewing habits for digital content, users' recently visited websites or product usage history. - Unique device identities: Other types of information that might be uniquely traceable to a user device, e.g. IP addresses, Radio Frequency Identity (RFID) tags, unique hardware [3].

Privacy sensitive information can be considered as personal information. In this paper, we proposed a strong privacy preserving scheme for third party in cloud. By making use of homomorphic encryption function, the proposed scheme maintains confidentiality of personal information sent by the cloud users. The proposed scheme is consists of following modules:

1. A mechanism to categorize the personal information and encrypt it using a homomorphic encryption function.
2. A mechanism to decrypt the personal information by making use of homomorphic decryption function for store at cloud provider end.

3. A mechanism to process the personal information at third party with cipher text (i.e. there is no need to decrypt the personal information) by making use of homomorphism property.

Our objective is to achieve anonymous privacy while third party uses the personal information. The proposed scheme offers following significant features:

1. Enhanced privacy management: With the employment of homomorphic encryption functions, the confidentiality of personal information is effectively guaranteed, which makes it difficult for attacker to recover the encoded personal information.
2. Competency: As our proposed scheme does not allow third party to decrypt the personal information, third party process the information without knowing it which provides a high competency.
3. Reduced server side computation: The authentication process is carried out at third party. Server only provides information in encrypted manner.

2. PRELIMINARIES

2.1 Term- Cloud Computing

Key to the definition of cloud computing is the "cloud" itself. For our purposes, the cloud is a large group of interconnected computers. These computers can be personal computers or network servers; they can be public or private. This cloud of computers extends beyond a single company or enterprise. The applications and data served by the cloud are available to broad group of users, cross-enterprise and cross-platform. Access is via the Internet. Any authorized user can access these docs and apps from any computer over any Internet connection. And, to the user, the technology and infrastructure behind the cloud is invisible [8].

Cloud computing gets its name as a metaphor for the Internet. Typically, the Internet is represented in network diagrams as a cloud [9] which provides three types of services to its user as: software-as-a-service, platform-as-a-service and hardware/infrastructure-as-a-service. Offerings with as a service as a suffix include traits like the following [9]:
Low barriers to entry, making them available to small businesses, large scalability, Multi-tenancy which allows resources to be shared by many users, device independence which allows users to access the systems on different hardware.
It is essential to make service level agreement with the personal information, between cloud users and providers to guarantee the services and secrecy of the personal information. After which personal information will be stored in database of service provider and manipulated during authentication and authorization process.

2.2 Need of privacy management in cloud

Cloud computing is a topic on software and distributed computing based on Internet, which means user can access storage and applications from remote servers by web browsers or other fixed or mobile terminals. To provide access to users and/or such terminals it is essential to maintain private information for authentication purpose. Personal information may be stored to the servers within the Cloud through the network and used while processing user requests.

The personal information travels through the entire Cloud which is great target for attackers who may get or examine the private information which harms on privacy violations. By making use of personal information attacker may get the advantage of services allocated to a user or abuse the information which is an immense risk. So that, privacy management is an important issue for cloud computing.

2.3 Homomorphic Encryption function - HEF

For two algebraic systems (X, °) and (Y, *) of the same type in the sense that both ° and * are binary operations and a mapping g: X → Y is called a homomorphism if for any x1, x2 Є X,

$$G(x1° x2) = g(x1) * g(x2) \quad (1)$$

If such a function g exits, then it is customary to call (Y, *) a homomorphic image [5] of (X, °), although we must note that g(X) $\subseteq$ Y.

The property of homomorphism is used in our proposed scheme for Homomorphic Encryption functions, which means operations on plain-text, can be performed by operating on corresponding cipher-text. For example, suppose E (•) is a homomorphic encryption function. It is easy to compute E(x + y) and E(x) •E(y) from E(x) and E(y) without knowing the corresponding plaintext x and y. To be applicable in proposed scheme, it needs to satisfy following property:

$$E (x + y) = E (x) • E (y) \quad (2)$$

Paillier [6] cryptosystem is such system, where the addition on plaintext can be achieved by performing a multiplicative operation on the corresponding cipher text, i.e., E (x + y) = E (x) • E (y).

2.4 Security perspective

We consider the following two security threats:

A. An attacker can examine the personal information by analyzing and comparing the cipher text when sending to the cloud from user or sending to the third party from cloud.

B. Third party, who receives personal information may obtain decryption key and reveal message plaintext.

3. THEPROPOSED SCHEME FOR PRIVACY MANAGEMENT IN CLOUD

In this section, we propose a new scheme for privacy management in cloud, which can competently prevent scrutiny of personal information, followed by theoretical analysis and simulative analysis.

3.1 The proposed system architecture

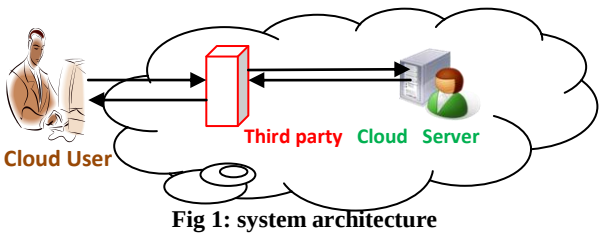

Fig 1: system architecture

As shown in fig 1, it is mandatory to store personal information at cloud provider end so that it can be used to authentication and authorization process.

While registration process, personal information will be categorized into following three parts:
1. Personally identifiable information (PII), e.g. user name (m1)
2. Sensitive Information (SI), e.g. password (m2)

3. General information (GI) which is not a personal and sensitive, e.g. registration number (m3).

When user sends private information, say m, will be encrypted using a function E as,

$$E(m) = g^m \cdot r^n \bmod n^2 \quad (3)$$

Where, r is random big integer value, n= pq, p and q are randomly generated large prime numbers and g is a random integer, the public (encryption) key [10] is (n, g).

This encryption function simulates the algebraic system (X, °).

By making use of this homomorphic encryption function we can send the personal information to the cloud database at the time of registration.

The result of an encryption operation will be as:

$$E(m1)= g^{m1}\cdot r^n \bmod n^2$$
$$E(m2)= g^{m2}\cdot r^n \bmod n^2$$
$$E(m3)= g^{m3}\cdot r^n \bmod n^2$$

Note that, general information may be generated after completion of registration process.

When server at cloud provider end receives the encrypted personal information and retrieves plain text by using homomorphic decryption function as:

$$m = L(E(m)^{\lambda} \bmod n^2) \cdot \mu \bmod n \quad (4)$$

Where λ = lcm (p – 1, q – 1), $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, function L is defined as $L(\mu) = (\mu - 1)/ n$. The private (decryption) key [10] is (λ, μ).

Prior to store the personal information, server will categorize the personal information into PII, SI, and GI. In the similar way, server will retrieve m1, m2, m3.When user needs to access the services, it has to go through authentication process which will be carried out by a third party. In this process user submits the personal information by using homomorphic encryption function to the third party. After which, third party requests the same personal information to the cloud server. Now, it becomes crucial to hide the plain text from the third party. To achieve the secrecy user will send personal information by using homomorphic functions (discussed previous) as below

$$D(E(m1) \cdot E(m2) \bmod n2) \quad (5)$$

On other hand, server will send the personal information of user by making use of another homomorphic functions as below:

$$D(E(m1).g^{m2} \bmod n^2) \quad (6)$$

Note, both functions satisfy the property of homomorphism as below:

$$D(E(m1) \cdot E(m2) \bmod n^2) = m1+m2 \bmod n =$$
$$D(E(m1).g^{m2} \bmod n^2) \quad (7)$$

3.2 Mechanism to categorize and encrypt PI using a homomorphic encryption function

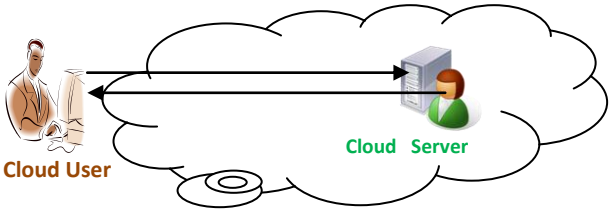

Fig 2: cloud user sends PI using HEF

This module, categorizes the personal information into following three parts:

1. Personally identifiable information
(PII), e.g. user name (m1),
2. Sensitive Information (SI), e.g. password (m2),
3. General information (GI),
4. Sensitive information, e.g. Registration number (m3).

After which, it encrypts the personal information by making use of homomorphic function E as:

$$E(m) = g^m \bullet r^n \bmod n2$$

Let, the personal information m1= v (ASCII value= 115) and m2= k (ASCII value= 107), randomly generated p = 61 and q= 47, random integer g= -621798935then n=2867, λ = 1380, μ= 2025, let r= 1628. So, E (m1) = 3169598 and E (m2) = 534758. These cipher texts will be sent to the server.

3.3 Mechanism, to decrypt the PI by making use of homomorphic decryption function, to store it at cloud provider end.

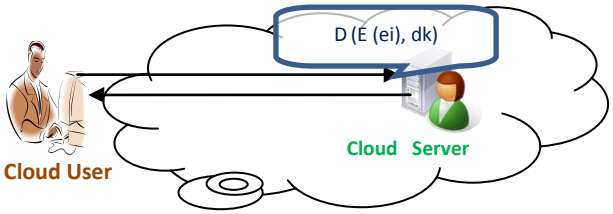

Fig 3: A Cloud provider receives the encrypted PI and decrypts it using homomorphic decryption function.

The cloud providers will receive the encrypted personal information in the form of E (m1), E (m2), E (m3)…

To store the personal information cloud providers categorizes it into PII, SI, and GI like: PI= E (m1), SI = E(m2) and GI = E(m3). By making use of homomorphic decryption function (4) and private key, it retrieves the plain text as:

$$m1= D(E(m1)) = L(E(m1)^{\lambda} \bmod n^2) \cdot \mu \bmod n$$
$$m2= D(E(m2)) = L(E(m2)^{\lambda} \bmod n^2) \cdot \mu \bmod n .$$

3.4 Mechanism to process the personal information at third party by making use of homomorphism property.

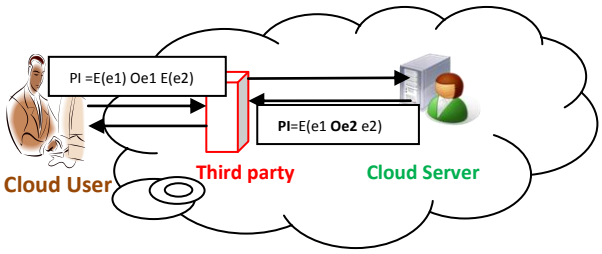

Fig 4: Third party (authentication) process uses cipher-text without knowing the plaintext.

As discussed in the proposed system architecture, this module will work as third party authentication process. In this module, user will send the personal information m1, m2 and m3 to the third party. m1 and m2 will be used to generate credential for authentication by using equation (5). m3 will be used to retrieve the personal information from server end which will again use m1 and m2 to generate credential by using equation (6). If both credentials match then third party processes the user request. To make the secrecy of personal information it uses homomorphism property of homomorphic functions.

In previous example, user sends the personal information by making use of (5) as:

$$(E(m1) \cdot E(m2) \bmod n^2) = +3170245 \quad (8)$$

In the other hand, server sends the personal information of user having GI=m3 by using equation (6) which in example:

$$D(E(m1).g^{m2} \bmod n^2) = +3170245. \quad (9)$$

Equation (9) simulates to equation (7). Hence, it hides the personal information from the third party.

4. RELATED WORKS

Ten major obstacles found in [1] which provides opportunities for work in cloud environment as below: Availability of service, Data Lock-In, Data confidentiality and Auditability, Data transfer bottleneck, Performance Unpredictability, Scalable storage, Bugs in large scale distributed systems, Scaling quickly, Reputation fate sharing, Software Licensing.

Some security challenges some cloud computing issues and some security benefits found in [2]. However, it identified seven security issues [2] as: Privileged user access, regularly compliance, Data location, Data segration, Recovery, Investigate support, Long term viability

It is important to take privacy into account when designing cloud services and found privacy threats and risks for cloud computing [3].However, some guidelines for designing privacy enhanced cloud and most six recommended privacy practices are found as [3]: Minimize personal information sent to and store in the cloud, Protect personal information in the cloud, Minimize user control, Allow user choice, Specify and limit the purpose of data usage, Provide feedback

A set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing architectures is provided in [4]. The mechanism allows for the secure storage and processing of users confidential data by leveraging the tamperproof capabilities of cryptographic coprocessors. Also, it [4] devises the some guidelines highlighted in reference [3]. The issues and obstacles mentioned in above survey needs the work to be extended. Our proposed work attempts to enhance these issues. It is found that homomorphic encryption techniques for allowing specific algebraic operations on encrypted data are still theoretical and lack of any pragmatic implementation [4].A practical fully homomorphic crypto system is still open research topic [7].

5. CONCLUSION AND FEATURE WORK

In this paper, we first identified the potential privacy issues in cloud computing. Then we proposed a strong privacy preserving scheme for third party in cloud. By making use of homomorphic encryption function, the proposed scheme maintains confidentiality of personal information sent by the cloud users. The proposed scheme offers three significant features, Enhanced privacy management, Competency, Reduced server side computation. We have implemented the scheme in Java with simulative results. We are using Paillier cryptosystem for privacy management. It is also possible to use another homomorphic functions for the same scheme. Our future work will attempt to enhance this issue with more results by implementing it in cloud environment.

6. REFERENCES

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Guntio Lee, David Patterson, Ariel Rabkin, Ion Stoica, and MateiZaharia, "Above the clouds : A berkely view of cloud computing", UC Berkely Reliable Adaptive Distributed Systems laboratory, February 10, 2009

[2] Train Anddrei, "Cloud Computing Challenges and related security issues", a project report, 2009

[3] Saini Pearson, "Taking Account of privacy when designing cloud computing services", in proceeding of ICSE-cloud 09, Vancouver, 2009.

[4] WassimItani, AymanKayssi, Ali Chehab, "Privacy as a Service: Privacy- Aware data Storage and processing in Cloud Computing Architectures", IEEE international conference on Dependable, Automatic and secure computing, 2009.

[5] J. P. trembly, R Manohar,"Discrete Mathematical Structures with Applications to Computer Science", book.

[6] P. Paillier, "Public-key Cryptosystems Based on Composite Degree Residuocity Classes", Proc. Of EUROCRYPT'99, LNCS,vol 1592, pp.223-238, 1999.

[7] Schneier on Security, available at: http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html

[8] Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", book.

[9] Anthony T. Velte, Toby J. Velte, Robert Elsenpeter, "Cloud Computing:A Practical Approach".

[10] Paillier cryptosystem, available at: http://en.wikipedia.org/wiki/paillier_crptoststem