CLOUD OFFICE USING HOMOMORPHIC ENCRYPTION

Umamaheswari E.
Department of SCSE, VIT University Chennai campus, Chennai, Tamil Nadu, India
E-Mail: umamaheswari.e@vit.ac.in

ABSTRACT

The cloud computing has become the most promising innovation in computing world as it is an attractive solution to store and process the confidential data. Lately many users pool their data and application in cloud as it provides global access, confidentiality, provides lot of storage space and is easy to use. But the development of cloud computing is obstructed by many cloud security problem. The problem of data security in cloud computing is to be solved by using homomorphic encryption algorithm for an office management application which will manage the leave and salary details of the employee. The homomorphic encryption allows the user to store and manipulate their data in cloud confidential from the third party server. Re-encryption technique is used to prevent the system from chosen cipher text attack.

Keywords: cloud office, homomorphic encryption.

1. INTRODUCTION

The transfer of data between machines is common but how to secure it from the unauthorised person is the problem. To solve this problem we can encrypt the data and store it. However if we want to perform any operation on the stored data we should either provide the secret key to the cloud provider or retrieve the whole data and perform the operation. Providing the secret key to the cloud provider reduces the confidentiality and retrieving the whole data base for a single operation increases the computational overhead. Homomorphic encryption can be used to solve these problems as it performs operation on the stored data in encrypted form without revealing the original data providing only a function of the result of requested operation which can be decrypted by the user using the private key. The cloud office application is developed applying the homomorphic encryption technique to confidentially store the salary details of the employees.

2. CLOUD COMPUTING AN OVERVIEW

Definition [1]- Information technology (IT) model for computing, which is composed of all IT components (hardware, software, networking and service) that are necessary for development and delivery of cloud services via the Internet or private network.

The cloud service includes Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS) which can be deployed in private, public or hybrid cloud. The main advantages of cloud computing are flexibility, cost reduction, availability, disaster recovery, increased collaboration and easy disaster recovery.

Cloud office management is implemented using Platform as a service in public cloud for the convenience of the employees without compromising with the data security using homomorphic encryption algorithm with re-encryption technique.

3. SECURITY ISSUES IN CLOUD COMPUTING

The cloud computing platform is used by many organizations for their data operation, providing proper security for their data has become the priority for the organizations. The three basic operations in cloud are transfer, store and process. Illegal access to these operations can be avoided using encryption techniques. The top threats to the cloud computing and the service model which they affect are listed by Cloud Security Alliance (CSA) as follows:

Table-1. Top threats to cloud computing.

Threat	Service model
Abuse and Nefarious use of cloud computing	IaaS, PaaS
Insecure Application Programming Interface	IaaS, PaaS, SaaS
Malicious Insiders	IaaS, PaaS, SaaS
Shared Technology Vulnerabilities	IaaS
Data Loss/Leakage	IaaS, PaaS, SaaS
Account, Service and Traffic Hijacking	IaaS, PaaS, SaaS
Unknown Risk Profile	IaaS, PaaS, SaaS

We are addressing the problem of data loss or leakage when deploying our application on cloud using platform as a service.

4. HOMOMORPHIC ENCRYPTION

The term homomorphic is derived from Greek word for “Same structure”. Because the data in homomorphic encryption retain the same structure and identical mathematical operation whether they are carried out on encrypted or decrypted data will yield the equivalent result. Homomorphic encryption allows complex mathematical operation to be carried out on encrypted data without yielding the encryption.

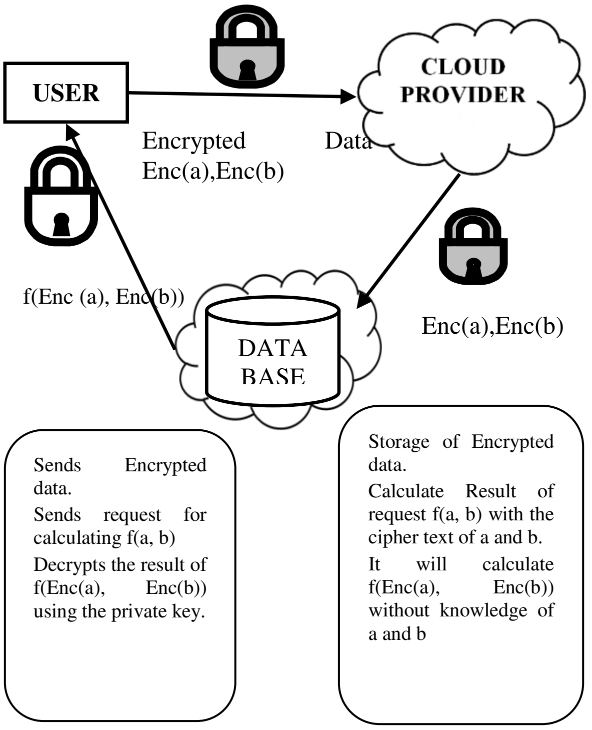

USER
CLOUD PROVIDER
Encrypted Data
Enc(a),Enc(b)
f(Enc (a), Enc(b))
Enc(a),Enc(b)
DATA BASE
Sends Encrypted data.
Sends request for calculating f(a, b)
Decrypts the result of f(Enc(a), Enc(b)) using the private key.
Storage of Encrypted data.
Calculate Result of request f(a, b) with the cipher text of a and b.
It will calculate f(Enc(a), Enc(b)) without knowledge of a and b

Figure-1. Homomorphic encryption architecture in cloud.

Homomorphic encryption is a form of encryption that allows computation to be carried out on the cipher text, thus generating encrypted result which after decryption matches the result of operation performed on the plain text.

Table-2. Homomorphic encryption characteristics.

Homomorphic algorithms	RSA	Goldwasser Micali	Pailler
Encryption Type	Multiplicative	Additive but can encrypt only a single bit	Additive
Platform	Cloud computing	Cloud computing	Cloud computing
Data Privacy	Is provided in communication and storage process	Is provided in communication and storage process	Is provided in communication and storage process

Homomorphic Algorithms	El Gamal	Boneh-Goh, Nissim	Gentry
Encryption Type	Multiplicative	Unlimited addition but only one multiplication	Fully
Platform	Cloud computing	Cloud computing	Cloud computing
Data Privacy	Is provided in communication and storage process	Is provided in communication and storage process	Is provided in communication and storage process

4.1 Multiplicative homomorphic encryption

A encryption is said to be multiplicative if $Encr(A \otimes B) = Encr(A) \oplus Encr(B)$
$Enc(\prod_{i=1}^{1} m_i)$=$\prod Enc\ (m_i)$
It involves 3 steps:

Key generation

Input: Choose two distinct prime numbers a and b.

Compute: mo=a*b which will act as modulo for both public and private key.
Compute $\varphi(mo) = (a-1)(b-1)$
Choose ex such that
$Gcd(ex, \varphi(mo)) = 1$
Choose d such that $d \equiv ex^{-1}\ mod\ \varphi(mo)$

Output: The output will be public key (pu) and secret key (se)
$pu = (ex, mo)$
$se = d$

Encryption

Input: m is the message to be encrypted where $m \in z_n$
Compute: the cipher text ci
$ci = m^{ex}\ mod\ mo$
Output: $ci \in z_n$

Decryption

Input: cipher text ci where $ci \in z_n$
Compute: The message
$m = ci^d\ mod\ mo$
Output: $m \in z_n$

Homomorphic property

Consider two cipher texts
$ci_1 = m_1^{ex}\ mod\ mo$
$ci_2 = m_2^{ex}\ mod\ mo$
$ci_1 . ci_2 = (m_1 m_2)^{ex}\ mod\ mo$
Hence it is homomorphic.

4.2 Additive homomorphic encryption

A encryption is said to be additive if
$Encr(A \oplus B) = Encr(A) \otimes Encr(B)$

$$Encr\left(\sum_{i=1}^{1} m_i\right) = \prod_{i=1}^{1} Encr(m_i)$$

It involves 3 steps:

Key generation

Input: Choose 2 distinct prime numbers a and b with similar bit length.

Compute: mo=a*b which will act as modulo for both public and private key.
Compute $\lambda = lcm(a-1)(b-1)$

Select integer g where $g \in z_n$ such that $(GCD\left(L(g^{\lambda} mod\ mo^2)\right)$ where L(u)=(u-1)/mo

Output: The output will be a public key (pu) and a secret key (se).
$pu = (mo, g)$
$se = (a, b)$

Encryption

Input: m is the message to be encrypted where $m \in z_n$

Compute

Choose random r where $r \in z_n$
Compute cipher text
$ci = g^m * r^{mo}\ mod\ mo^2$
Output: $ci \in z_n$

Decryption

Input: cipher text ci where $ci \in z_n$
Compute: plain text message m
$m = mod\ mo\ [L(ci^{\lambda}\ mod\ mo^2)/L(g^{\lambda}\ mod\ mo^2)]$
Output: $m \in z_n$

Homomorphic property

Consider two cipher text ci1 and ci2
$ci_1 = g^{m1}. r_1^{mo}\ mod\ mo^2$
$ci_2 = g^{m2}. r_2^{mo}\ mod\ mo^2$
$ci_1 . ci_2 = g^{m1+m2}(r_1 r_2)^{mo}\ mod\ mo^2$
Hence it is homomorphic.

5. ANALYSIS OF THE PROPOSED SYSTEM

The cloud office management is an application developed using homomorphic encryption protected against chosen cipher text attack using re- encryption technique. In our implementation we have encrypted the salary details of the employee using RSA and paillier cryptosystem. The system is safe because even if the attacker gets the key they have to decrypt using two different set of key which will make their job even more difficult.

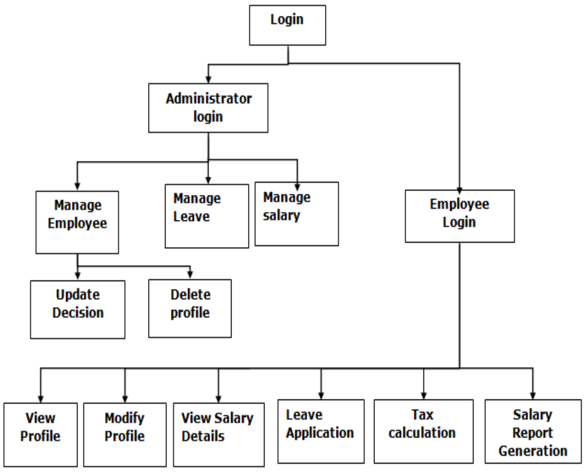


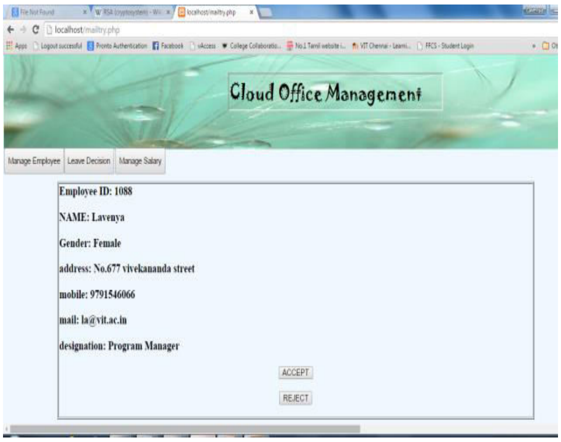
Figure-2. Analysis of the proposed system.

The users and the administrator will be provided with separate login.

The administrator can perform the following operations:

- Manage employee profile
- Manage leave decision
- Salary management

Manage employee profile: The administrator can view the modification request by employee and accept the changes or reject.



Cloud Office Management

Manage Employee | Leave Decision | Manage Salary

Employee ID: 1088

NAME: Lavenya

Gender: Female

address: No.677 vivekananda street

mobile: 9791546066

mail: la@vit.ac.in

designation: Program Manager

ACCEPT

REJECT

Figure-3. Profile update request.

Manage leave decision: The leave form Details will be visible to the administrator who can approve or reject the request. The status of leave form is updated to the employee through mail.

Salary management: The salary details can be modified and stored by the administrator.

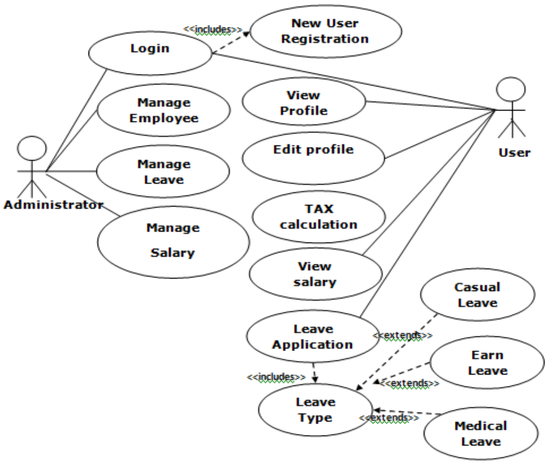


Figure-4. Use case diagram of the proposed system.

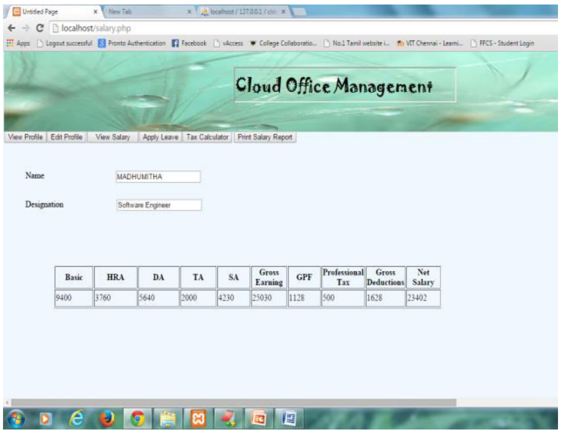
The employee can perform the following operations:

- View profile
- Update Profile
- View salary
- Tax calculation
- Salary report
- Apply leave

View profile: The employee can view their profile details.

Update profile: The employee can modify the profile details and send for the administrator approval.

View salary details: The salary details of the employee are displayed in a tabulated format.



Cloud Office Management

View Profile | Edit Profile | View Salary | Apply Leave | Tax Calculator | Print Salary Report

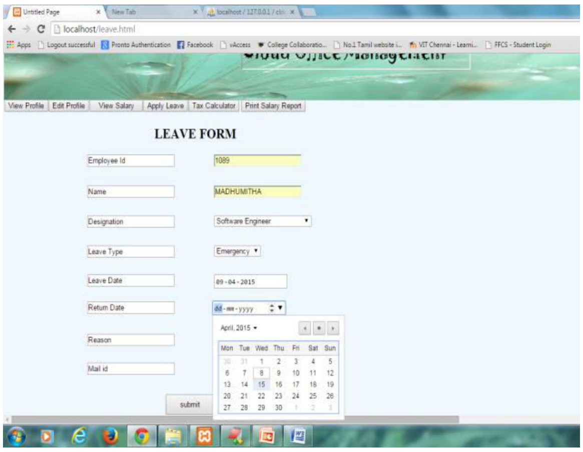
Name MADHUMITHA

Designation Software Engineer

Basic	HRA	DA	TA	SA	Gross Earning	GPF	Professional Tax	Gross Deductions	Net Salary
9400	3760	5640	2000	4230	25030	1128	500	1628	23402

Figure-5. Salary details of the employee.

Apply leave: The employee can apply for leave by entering the details. The leave form will be forwarded to the administrator for approval. The leave request status will be received through mail.



LEAVE FORM

Employee Id	1089
Name	MADHUMITHA
Designation	Software Engineer
Leave Type	Emergency
Leave Date	09-04-2015
Return Date	dd-mm-yyyy
Reason	
Mail id	

April, 2015

Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Figure-6. Sample leave form.

Tax calculator

Income tax of the employee is calculated after getting additional details. The employee is requested to enter their loan amount if the employee has take loan, policies if the employee has invested in any policy, Donation if the employee has donated. Tax is calculated based on the salary slab of employee. The salary details will be obtained from the database.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we have analysed the cloud computing security issues and presented the implementation of homomorphic encryption using re-encryption technique to avoid chosen chipper text attack which is the major attack on homomorphic encryption scheme for application in office management to manage the employee leave and salary details. If the salary details are encrypted and stored, the confidentiality of data can be achieved resulting in highly secure cloud computing environment.

As a future work we can try to reduce the key size and improve the existing algorithm to increase the efficiency of the system.

REFERENCES

[1] 2011. Securing the cloud (Cloud computing security techniques and tactics), JR Winkler.

[2] 2014. Homomorphic Encrypton method applied to cloud computing, Iram Ahmad and Archana Khandekar. International Journal of Information and Computation Technology. ISSN 0974-2239. 4(15): 1519-1530.

[3] 2011. Implementing Gentry's fully homomorphic encryption scheme, Craig Gentry, Shail Halevi, IBM Research.

[4] 2009. Fully homomorphic encryption scheme PhD thesis, C. Gentry, Stanford University.

[5] An analysis of security issues in cloud computing, Keiko Hashizume, David G Rosado, Eduardo Fernandez-medina, Eduardo B Fernandez. Journal of internet service and application.

[6] 2007. A survey of homomorphic encryption for nonspecialists, C. Fontaine, F. Galand, EURASIP Journal on Information Security.

[7] 2008. Post-Quantum Cryptography, chapter Lattice-based Cryptography, D. Micciancio and O. Regev. Springer.

[8] 2013. Effective Approach for Secure Storage Services in Cloud Computing, T. Deepika and T.R. Srinivasan. International Journal of Advanced Information Science and Technology (IJAIST), ISSN: 2319: 2682, 13(13).

[9] 2013. Providing a secure data forwarding in cloud storage system using threshold proxy re-encryption scheme, S. Poonkodi, V. Kavitha, K. Suresh. International Journal of Emerging Technology and Advanced Engineering. 3(Special Issue 1).

[10] 2012. New Directions in Cloud Computing: A Security Perspective, Alecsandru Patrascu, Diana Maimu, Emil Simion, s IEEE.