International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 6 4158 – 4161

Secure Cloud using RGB value and Homomorphic Encryption for Shared Data in Cloud

Yogita S. Pawar[1]
Asst Prof., Department of Computer Science and Engineering, GHRIEM, Jalgaon, India[1]
E-mail: pawaryogita04@gmail.com

Shambhu Kumar Singh [2]
Research Scholar, Department of Computer Science and Engineering, GHRIEM, Jalgaon, India[2]
E-mail: sambhusingh90@gmail.com

Abstract— Cloud computing is a promise computing technology where all the services are provided via Internet. Recent Years have seen increasing attractiveness of storing and managing personal data on the cloud. Preserving confidentiality of personal data while offering efficient functionalities thus becomes an important and pressing research issue. We all know the demand for privacy of information of enterprise has increased tremendously. For this, technologies such as data encryption methods are used. However a critical problem arises when there is a need of computation on encrypted data where privacy is established. At this situation homomorphic encryption can be applied. In this paper we propose the application that perform the operation on encrypted data and provides the same result on raw data as well as encrypted data when calculation to be performed. We also use RGB value for accountability purpose and proxy re-encryption technique for preventing chosen cipher text attacks.

Keywords*: Cloud Computing, Cloud Data Security, Homomorphic Encryption Techniques, RSA Encryption Techniques*

*****

I. INTRODUCTION

When plugging electric appliance into an outlet, we care neither how electric power is generated nor how it gets to that outlet. This is possible because electricity is virtualized; that is, it is readily available from a wall socket that hides power generation stations and a huge distribution grid. When extended to information technologies, this concept means delivering useful function while hiding how their internal work. Computing itself, to be considered fully virtualized, must allow computers to be built from distributed components such as processing, storage, data and software resources [1].

Technologies such as cluster, grid, and now cloud computing, have all aimed at allowing access to large amounts of computing power in fully virtualized manner, by aggregating resources and offering a single system view. In addition, an important aim of these technologies has been delivering computing as a utility. Utility computing describes a business model for on-demand delivery of computing power; consumers pay providers based on usage ("pay as-you-go"), similar to the way in which we currently obtain service from traditional public utility services such as water, electricity, gas and telephony. Cloud computing has been coined as an umbrella term to describe a category of sophisticated on-demand computing service initially offered by commercial providers, such as Amazon, Google and Microsoft. It denotes a model on which a computing infrastructure is viewed as a "Cloud" from which businesses and individual access applications from anywhere from anywhere in the world on demand [2]. The main principle behind this model is offering computing, storage, and software "as a service". There are many problem related with cloud computing traffic, security and resource management. We can provide security in cloud by many ways like on data, network and storage. Homomorphic encryption method provides more security on data because provider is not involving in key management. We have use proxy re-encryption technique and colors technique that prevents ciphertext from chosen cipher text attack [3]. This system is more secure than existing system [11]. By Cloud Computing we mean: The Information Technology (IT) model for computing, which is composed of all the IT components (hardware, software, networking, and services) that are necessary to enable development and delivery of cloud services via the Internet or a private network. This definition has no notion of security for data in the cloud computing even if it's a very new. Cloud providers like: IBM, Google and Amazon use the virtualization in their Cloud platform, and in the same machine can coexist the storage space and treatment virtualized which belong to the concurrent enterprises[3].

In cloud computing, everything is delivered *as a Service* (*XaaS*), from testing and security, to collaboration and Meta modeling. The cloud was rapidly becoming a conflagration of buzzwords "as a service". Today there are three main service models, which are agreed on and defined in the NIST document [10].

1. *Software as a Service*– Applications reside on the top of the cloud stack. Service provided by this layer can be accessed by end users through web portals. Therefore, consumers are increasingly shifting from locally install computer programs to on-line software services that offer the same functionality. Traditional desktop applications such as word processing and spreadsheet can now be accessed as a service in the web. This model of delivering applications, known as Software as a Service (SaaS) Typical examples are Google Docs and Salesforce.com CRM [10].

2. *Platform as a Service*– In addition to infrastructure-oriented clouds that provide raw computing and storage services, another approach is to offer a higher level of abstraction to make a cloud easily programmable, known as Platform as a Service (PaaS).This gives a client (developer) the flexibility to build (develop, test and deploy) applications on the provider's platform (API, storage and infrastructure). *PaaS* stakeholders include the *PaaS* hosted who provides the infrastructure (servers etc), the *PaaS* provider who provides the development tools and platform and the *PaaS* user. Examples of *PaaS* are Microsoft Azure and Google AppEngine [10].

3. *Infrastructure as a Service*–Offering virtualized resources (Computation, storage, and communication) on demand is known as Infrastructure as a Service (IaaS). A cloud infrastructure enables on-demand provisioning of servers running several choices of operating system and customized software stack. Infrastructure services are considered to be bottom layer of cloud computing. Amazon Web Services mainly offers IaaS, which in the case of its EC2 service means offering VMs with software stack that can be customized similar to how an ordinary physical server would be customized [10].

Depending on infrastructure ownership, there are four deployment models of cloud computing each with its merits and demerits. This is where the security issues start.

1. The Public Cloud

This is the traditional view of cloud computing in every day lingua. It is usually owned by a large organization (e.g. Amazon's EC2,

Google's AppEngine and Microsoft's Azure). The owner-organization makes its infrastructure available to the general public via a multi-tenant model on a self-service basis delivered over the Internet. This is the most cost-effective model leading to substantial savings for the user, albeit with attendant privacy and security issues since the physical location of the provider's infrastructure usually traverses numerous national boundaries [10].

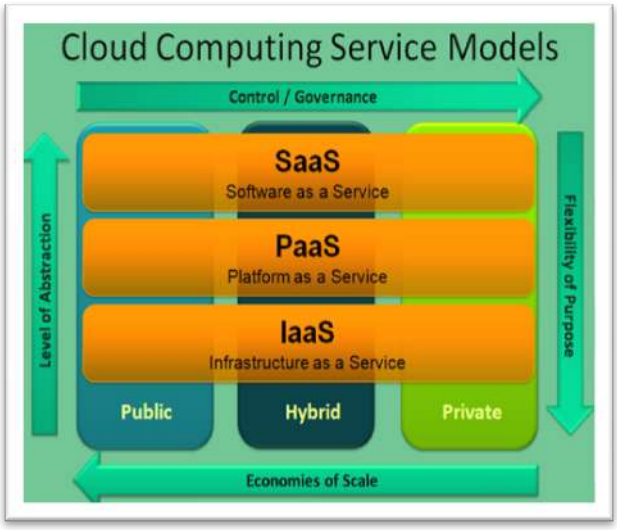


Figure 1 Basic Architecture of cloud computing

2. The Private Cloud

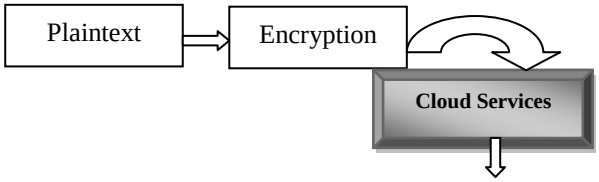
It refers to cloud infrastructure in a single tenant environment. It defers from the traditional data center in its predominant use of virtualization. It may be managed by the tenant organization or by a third party within or outside the tenant premises. A private cloud costs more than the public cloud, but it leads to more cost savings when compared with a data center as evidenced by Concur Technologies. The private cloud gives an organization greater control over its data and resources. As a result, the private cloud is more appealing to enterprises especially in mission and safety critical organizations [1].

3. The Hybrid Cloud

It comprises of a combination of any two (or all) of the three models discussed above. Standardization of APIs has lead to easier distribution of applications across different cloud models. This enables newer models such as "Surge Computing" in which workload spikes from the private cloud is offset to the public cloud [1].

II. HOMOMORHIC ENCRYPTION TECHNIQUES

Homomorphic Encryption techniques are one type of techniques on which we can performs operation on encrypted data without knowing original plaintext data. This technique also allows server to perform the operation on encrypted data without knowing the original plaintext data. It can also allows complex mathematical operations to be performed on encrypted data without using the original plaintext data. For plaintexts A1 and A2 and corresponding ciphertext B1 and B2, a Homomorphic encryption scheme allows the computation of A1 Θ A2 from B1 and B2 without using P1 Θ P2.The cryptosystem is multiplicative or additive Homomorphic depending upon the function Θ which can be multiplication or addition [12].



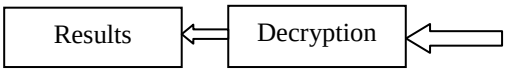


Figure 2 Data protection System over the Cloud

III. CRYPTOGRAPHY CONCEPT

The art or science surrounding the principles and methods of transforming a comprehensible message into one that is inarticulate, and then retransforming that message back to its original form is basic idea behind of cryptography. Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Encryption and decryption require the use of some secret information, usually referred to as a key [5]. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different [7].

1. Ways of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use as in. The three types of algorithms are depicted as follows

1.1) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard (AES) [7].

1.2) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, and Adleman) algorithm is an example [7].

1.3) Hash Functions: This function creates fixed size encrypted message called hash irrespective of size of input message. MD (Message Digest) algorithm is an example. Hash functions are one way [7].

2. RGB Color Value

Any color is the combination of three primary colors Red, Green and Blue in fixed quantities. A color is stored in a computer in form of three numbers representing the quantities of Red, Green and Blue respectively. This representation is called RGB representation which is used in computers to store images in BMP, JPEG and PDF formats. Here each pixel is represented as values for Red, Green and Blue. Thus any color can be uniquely represented in the three dimensional RGB cube as values of Red, Green and Blue. The RGB color model is an additive model in which Red, Green and Blue are combined in various ways to produce other colors. By using appropriate combination of Red, Green and Blue intensities, many colors can be represented. Typically, 24 bits are used to store a color pixel. This is usually apportioned with 8 bits each for red, green and blue, giving a range of 256 possible values, or intensities, for each hue. With this system, 16 777 216 (256^ 3 or 2^24) discrete combinations of hue and intensity can be specified [5].

IV. EXISTING SYSTEM

A. Additive Homomorphic Encryption

A Homomorphic technique is additive, if: Enc(a + b) = Enc(a) + Enc(b)

TABLE I PAILLIER CRYPTOSYSTEM [8]

Key Generation: KeyGen (p,q)	Encryption: Enc(m, pkey)	Decryption: Dec(ci, skey)
Input: p, q € P	Input: m € Z_n	Input: Ci € Z_n
Compute: n=p*q, and =lcm(p-q)(q-1) Choose g € Z_n such that Gcd(L(g^ mod n^2),n)=1 with L(u)=(u-1)/n	Choose r € Z_n Compute: ci=$g^m * r^n$ mod n^2	Compute: m= mod n [L((c^ mod n^2)/L((g^ mod n^2)]
Output: (pkey, skey) Public Key: pkey=(n, g) Secret Key: skey=(p,q)		Output: m € Z_n

Suppose we have two ciphers Ci1 and Ci2 such that:
Ci1=gm1. r1 n mod n2
Ci2=gm2.r2 n mod n2
Ci1. Ci2= gm1.r1 n.gm2.r2 nmod n2= gm1+m2 (r1r2) n mod n2
So, Paillier cryptography system realizes the property of additive Homomorphic encryption.

B. Multiplicative Homomorphic Encryption

A Homomorphic technique is multiplicative, if:
Enc(a * b) = Enc(a) * Enc(b)

TABLE III RSA CRYPTOSYSTEM (1978) [8]

Key Generation: KeyGen (p,q)	Encryption: Enc(m, pkey)	Decryption: Dec(ci, skey)
Input: p, q € P	Input: m € Z_n	Input: Ci € Z_n
Compute: n=p*q, and ǿ(n)=(p-q)(q-1)	Compute: ci=m^e mod n	Compute: m= c^d mod n
Choose e such that Gcd(e, ǿ(n))=1 Determine d such that e* d=1 mod ǿ(n)	Output: Ci € Z_n	Output: m € Z_n
Output: (pkey, skey) Public Key: pkey=(e,n) Secret Key: skey=(d)		

Suppose we have two ciphers Ci1 and iC2 such that:
Ci1= m1e mod n
Ci2= m2e mod n
Ci1. Ci2= m1e m2e mod n= (m1m2)e mod n

So, RSA cryptography system find the properties of the multiplicative Homomorphic technique, but does not satisfied good notions of security, Because if we think two ciphers Ci1, Ci2 equivalent to the messages m1, m2, respectively, so :
Ci1= m1 e mod n
Ci2= m2 e mod n
The source sends the pair (Ci1, iC2) to the Cloud server; the server will perform the calculations requested by the client and sends the encrypted result (Ci1XCi2) to the customer. If the attacker intercept two ciphers Ci1 and Ci2, which are encrypted with the same key, it will be decrypt all messages exchange between the two interactions because the Homomorphic technique is multiplicative, i.e. the product of the ciphers equal to the cipher of the product.

Suppose we have two ciphers Ci1 et Ci2 such that:
Ci1 = m1e mod n
Ci2 = m2e mod n
Ci1.Ci2 = m1em2e mod n = (m1m2) e mod n

RSA cryptography system is working with property of multiplicative Homomorphic technique, but it has a lake of security, because if we have two ciphers Ci1, Ci2 corresponding respectively to the messages m1, m2 so:
Ci1 = m1e mod n
Ci2 = m2e mod n
The client sends the pair (Ci1, Ci2) to the Cloud server and server performs the calculations requested by the client and sends the encrypted result (Ci1 × Ci2) to the client. If the attacker intercepts two ciphers Ci1and Ci2, which are encrypted with the same private key, so they are, decrypt all messages exchange between the server and the client. Because the Homomorphic technique is multiplicative, i.e. the product of the ciphers equals the cipher of the product [4]. The basic RSA algorithm and Paillier Cryptography system is defenseless to chosen ciphertext attack (CCA).CCA is defined as an attack in which adversary chooses a number of ciphertext and is given the corresponding plaintext, decrypted with the target's private key. Thus the enemy can able to select a plaintext messages, encrypt it with the target's public key and then be able to get plaintext messages back by having it decrypted by private key. So attacker will know the entire data in-between client and cloud server [13].

V. PROPOSED SYSTEM

For preventing of cipher data from CCA (chosen ciphertext attack) and accountability I propose Proxy Re- Encryption algorithm with paillier and RSA Cryptosystem. Initially users are identified by assigning of unique RGB value. Each RGB value is represented with a set of three values for example violet red color is represented in RGB format as (138, 158, 40) simultaneously user signup will done, after then user can able to login in system, at the time of login OTP will generated which is accessible from registered email_id. In next step actual data are encrypted using RGB and Homomorphic encryption technique, after then these data are sent on the cloud. After then user can able to decrypt the data by using login into system again OTP will generated, user can login into system by providing OTP which is accessible from registered email_id then user can decrypt the data by providing RGB value and key of Homomorphic encryption. Detail description of proposed system model is shown in fig. 3.

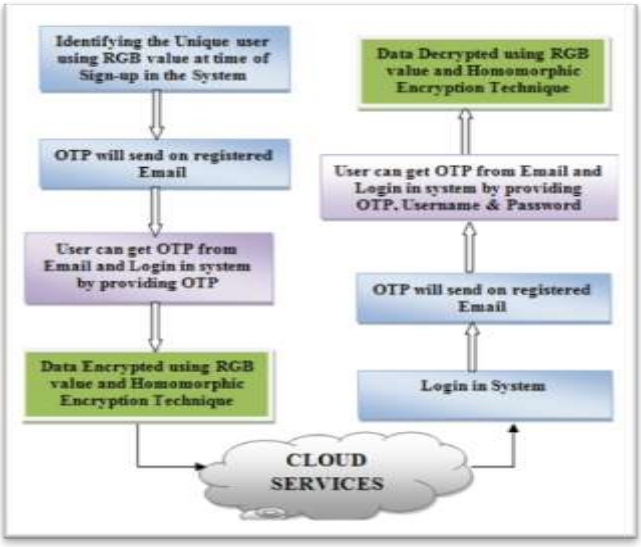


Figure 3 Proposed System Model

Homomorphic encryption techniques:

Key Generation -keygen (p,q)
1. Take two prime number p and q.

2. Compute n=p.q, Φ(n)=(p-1)(q-1) and choose e such that gcd(e, Φ(n)))=1.
3. Determine d such that e.d=1 mod Φ(n).
4. The Proxy public key (Rpk) is (e,n) is generated.
5. The proxy Secret key (Rsk) is (d) is generated.
Encryption: Enc (c,Rpk)
1. Let m be a message to be encrypted where m Є Zn.
2. Compute ciphertext as: rc=me mod n.
Decryption: Dec (rc,Rsk)
1. Ciphertext c Є Zn.
2. Compute message m=cd mod n.

Proxy Re-Encryption Algorithm:

Key generation:
1. Choose two large prime numbers p and q randomly and independently of each other such that,
gcd (pq ,(p-1)(q-1))=1.
2. Compute n=pq and λ=lcm (p-1, q-1).
3. Select random integer g where g Є Z*n2
4. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: μ=(L(a λ mod n2))-1 mod n, where function is defined as L(u)=u-1/n.
5. The public (encryption) key is. (n,g)
6. The private (decryption) key is (λ, μ) Encryption: Enc (m, pk)
1. Let m be a message to be encrypted where m Є Zn.
2. Select random where r Є Zn*.
3. Compute ciphertext as: c=gm . rn mod n2.
Proxy Re-Encryption(c)
1. Compute Private and Public key.(Rsk,Rpk).
2. Re Encrypt Ciphertext generated and send Public key (Rpk) to cloud server.
Decryption: Dec(c,sk)
1. Ciphertext c Є Zn2*.
2. Compute message: m=L(c λ mod n2)/ L (g λ mod n2).
Mod n

VI. CONCLUSION

The above combination of secret key and public key cryptography can be applied mainly at initial level we provide the mechanism for to identifying the receiver. At the final level we provide Homomorphic encryption technique which is a new concept of security on the cloud that enables proving results of calculations on encrypted data without knowing the row data. In this paper we have proposed RSA and Paillier algorithm for Homomorphic encryption with RGB color model that prevents cipher data from Choosen Cipher text Attack (CCA). So this system is more secure than existing system.

REFERENCES

[1] Anjana Chaudhary, Ravinder Thakur and Manish Mann "Security in Cloud Computing by Using Homomorphic Encryption Scheme with Diffie-Hellman Algorithm" Proceedings of 7th SARC-IRF International Conference, 03rd August-2014, New Delhi, India, ISBN: 978-93-84209-41-4.

[2] Hu Shuijing "Data Security: the Challenges of Cloud Computing" 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation.

[3] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Transactions On Parallel And Distributed Systems Vol: 25 NO: 2 YEAR 2014.

[4] Bhabendu Kumar Mohanta and Debasis Gountia "Fully homomorphic encryption equating to cloud security: An approach" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 2 (Jan. - Feb. 2013), PP 46-50.

[5] Shashank Bajpai and Padmija Srivastava "A Fully Homomorphic Encryption Implementation on Cloud Computing" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 811-816

[6] Iram Ahmad and ArchanaKhandekar "International Journal of Information & Computation Technology" ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530"

[7] S. Pavithra Deepa, S. Kannimuthu, and V. Keerthika "Security Using Colors and Armstrong Numbers" National Conference on Innovations in Emerging Technology Year 2011.

[8] Maha Tebaa, Saïd El Hajji, Abdellatif El Ghazi "Homomorphic Encryption Applied to the Cloud Computing Security" Proceedings of the World Congress on Engineering 2012 Vol I WCE 2012, July 4 - 6, 2012, London, U.K.

[9] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE 5th International Conference On Cloud Computing Year 2014

[10] Rajkumar Buyya, James Broberg and Andrzej Goscinski "Cloud Computing Principles and Paradigms" ISBN 978-81-265-4125-6

[11] Vidya S and Vani K "Secured PHR Transactions using Homomorphic Encryption in Cloud Computing" International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 2 Issue 12 Dec, 2013 Page No. 3540-3543.

[12] Myur Sunil Patil and Shambhu Kumar Singh "Cloud Security using Colors and Homomorphic Encryption" International Journal on Emerging Trends in Technology ISSN: 2350-0808, September 2014, Volume 1 Issue 1, 182.

[13] S. J. Patil, N. P. Jagtap and Shambhu Kumar Singh "Use of RGB Colors and Cryptography for Cloud Security" International Journal of Science Spirituality Business and Technology ISSN: 2277-7261.

ACKNOWLEDGMENT

Mrs. Yogita Pawar is an Assistant Professor in G. H. Raisoni Institute of Engineering and Management, Jalgaon. She has 5 years experience in the same Institute.

Mr. Shambhu Kumar Singh is a research scholar in GHRIEM, Jalgaon. He has 2.5 year experience and he is working as an Assistant Professor in SSBT's COET, Bambhori, Jalgaon.