IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. II (Nov. - Dec. 2016), PP 13-18
www.iosrjournals.org

Effective Crypto Systemfor Achieving Security and Performance over Market Basket Data Analysis

[1]N.Swetha, [2]Prof. S Ramachandram
[1]Research Scholar,Dept of CSE, Osmania University, Hyderabad
[2]Vice Chancellor,Dept of CSE,OsmaniaUniversity,Hyderabad

Abstract:*Nowadays Cloud computing plays a vital role in diverseareaslike Personal Health,Social applications,enterprise,Finacial and Public domains etc.,Security is an important province in as far as cloud computing is concerned , Nevertheless one of the biggest issues is while implementing cloud remains data security i.e Leading data integrity and Privacy plays a Keyrole. In this connection,secure cryptographic algorithms could be used to ensure the data privacy such as play fair cipher.In this paper, we focus on to explore efficient cryptographic algorithm for protecting cloud data over homomorphic encryption scheme and also explore the Keymanagement and system performance for market basket analysis i.e on customer purchased product data.*

Keywords: *Crypto System,Homomorphic Encryption, Cloud Security, market basket analysis,Porticor Homomorphic Key Management(PHKM)*

I. Introduction

Nowadays Cloud leads a majority role in the market due to its primitive services ,however, the issue of full trust stays uncertain. In applying encryption to secure kind data and an essential secret is the encryption key itself for organizations moving workloads to the cloud, e.g., public clouds, holding possession and control of encryption keys while understanding the advantages of the cloud are frequently viewing for concerns. In the past few years, the security requirements for data are very strong and various algorithms have been developed based on homomorphic techniques [9]. Only a few algorithms play aninclusive role in maintaining security to the data, the main goals at executionarbitrary calculation on the encrypted data called, Homomorphic techniques which give privacy inclines toward executing aproblematic operation on encrypted data. Homomorphic encryption is grown to solve such perilous issues. The Homomorphic properties of ciphers have been implemented in various real-time applications i.e 1.Private Data, Public functions: like in Medical Applications 2.Private data, Private functions: like in Financial Applications 3. Applications like Advertising and pricing where only results should be public such as market basket analysis which is one of the marketing analyses in order to identify purchase patterns (e.g., to identify what items tend to be purchased together, sequentially or by seasons). Using Homomorphic encryption data protection is achieved through which allows additive and multiplicative operations over encrypted bits.

Product purchase patterns scenario:

For illustration, Assume that there are two association companies C and D and they only share their customer's ID. The two companies C and D have their own customers purchase history data of items X and Y, respectively. Then they would like to know the number of customers who bought both items X and Y in order to identify how much the items are purchased sequentially, without revealing each customer purchase history data to one another". When purchase history data are analyzed, it needs to share both customer ID and purchase history data among association companies. In this case, customer information of each company would be exposed to the other companies, and hence some problems related to the customer's privacy might be doubtful. Moreover, since purchase history data of each company are directly related to its own sales, the data should be undisclosed to the other companies. In this connection in order to provide the data security, we need to apply privacy preserving approaches i.e Homomorphic encryption where depending on operations on encrypted data.

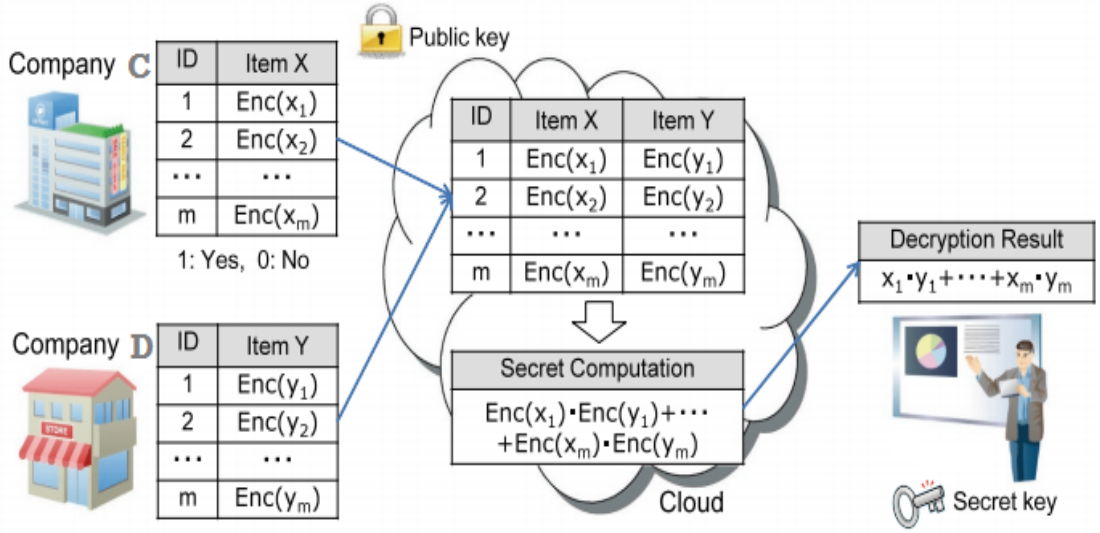

Fig 1. Computation model of purchase history data between two companies

II. Privacy-Preserving Approach

2.1 Homomorphic Encryption

Definition: Homomorphic encryption is the encryption technique where functioning on encrypted data rather than original data, as a result, the complex mathematical operations can be performed on the ciphertext without changing the nature of the encryption.

2.2 Partially Homomorphic encryption

Definition: Partially Homomorphic encryption schemes means Homomorphic computation supports only one operation (either addition or multiplication) on plaintexts. The following is an account of the partial encryption schemes that support computations.

Somewhat Homomorphic Encryption (SHE)

A recent trend in the HE encryption literature has been something called Somewhat Homomorphic Encryption (SHE). These are ciphers which support both addition and multiplication but not unlimited numbers of operations. E.g., SHE cipher as it supports unlimited additions and one multiplication. The current FHE ciphers are all built using SHE ciphers plus a bootstrapping operation (or generating the keys such that enough of each operation can be supported to compute the desired function, making bootstrapping unnecessary).

Definition: An encryption is homomorphic, if: from Enc(a) and Enc(b) it is possible to compute Enc(f (a, b)), where f can be: +, ×, ⊕and without using the private key. Among the Homomorphic encryption we distinguish, according to the operations that allows to assess on raw data, the additive Homomorphic encryption (only additions of the raw data) is the Pailler [2] and Goldwasser-Micalli [3] cryptosystems, and the multiplicative Homomorphic encryption (only products on raw data) is the RSA [4] and El Gamal [5] cryptosystems

Types of Homomorphic encryptions performed on customer purchased data :

1. Additive Homomorphic Encryption:

A Homomorphic encryption is additive, if:

$$\text{Enc}(x \oplus y) = \text{Enc}(x) \otimes \text{Enc}(y)$$

$$\text{Enc}\left(\sum_{i=1} m_i\right) = \prod_{i=1} \text{Enc}(m_i)$$

Suppose we have two ciphers C1 et C2 such that:

C1 = gm1. r1n mod n2

C2 = gm2. r2 n mod n2

C1.C 2 = gm1. r1n. gm2. r2 nmod n2 = gm1+ m2 (r1r2) n mod n2

So, Pailler cryptosystem realizes the property of additive Homomorphic encryption. An application of an additive Homomorphic encryption is Market basket analysis: Each purchased product count is encrypted but only the "sum" is decrypted to authorized end.

III. Problem Statement

Cloud storage security is giving more focus on how to make data more secure and giving less attention towards degradation of Cloud performance due to fail in selecting proper encryption and Encoding algorithms. So, if Client selects a proper cryptographic scheme then it can achieve confidentiality without losing performance of Cloud.

IV. Cryptosystem For Cloud Security

Understanding Crypto System for Cloud Security over Homomorphic Operations:

Inorder to provide the data privacy while outsourcing the client data onto cloud servers, data must be encrypted using cryptographic algorithms. In this connection as off our cryptographic algorithms classified into two major type of Encryptions i.e , symmetric Encryption and Asymmetric encryption .There is a variety of symmetric or asymmetric algorithms available as shown in fig 2., such as DES, AES, IDEA, RSA, and EIGamal (Salomaa, 1996; Tanenbaum, 2003; Burnett and Paine, 2001).

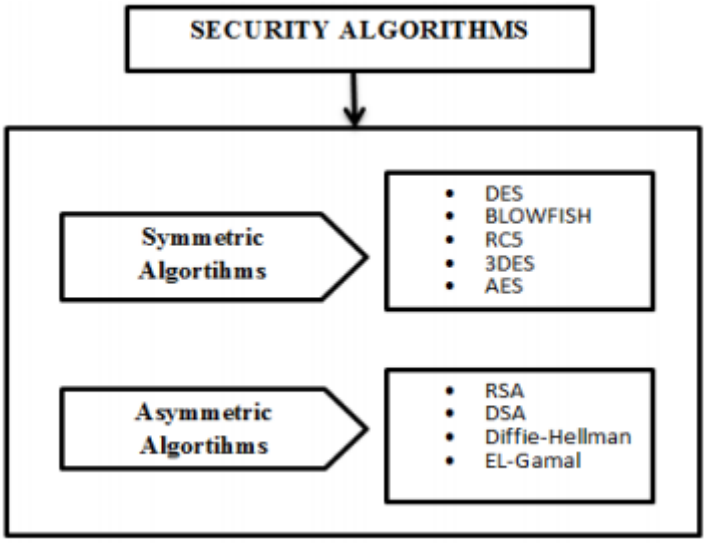

Fig 2. Classifications of Security algorithms in Crypto System.

The storage system may invoke both the encryptions mechanism as Asymmetric keys to exchange symmetric keys and asymmetric keys to Encrypt/Decrypt the data.

Symmetric Keys: Same(Single) keyis used for both Encryption and Decryption the data.and requires low computing power, Symmetric encryption is typically more efficient than asymmetric encryption, and is often used for bulk data encryption.

Asymmetric Keys: Its uses Private and Public key pairs It also is known also known as public-key encryption, It can't be derived from each other where data encrypted with aPublic key and decrypted with Private key and it requires greater computing power.

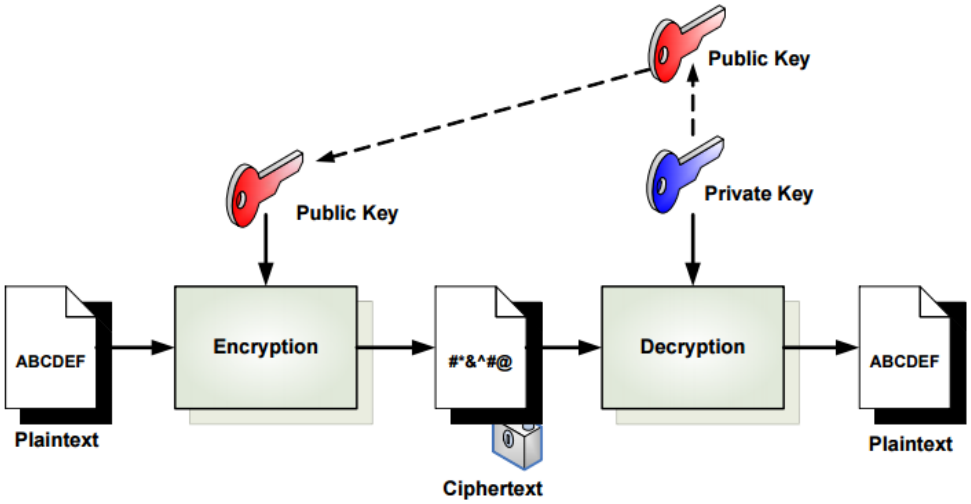

Fig 3. Asymmetric Key Operations

Encryption Strength:
In cryptography, key size or key length is the number of bits in a key used by a cryptographic algorithm . Inorder demonstrates the encryption strength on 112 bits and 128 bits of data with various key size i.e 128 bit AES and 3072-bit RSA ,3DES ,128 bit AES and 2048-bit RSA.

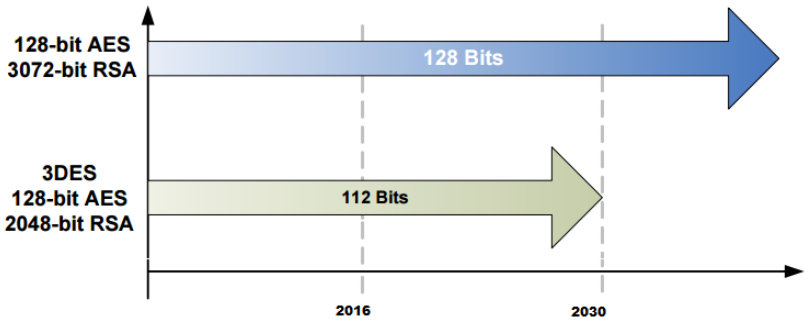

Fig 4. Encryption Strength

A brute force attack against an n bit key that simply tries to guess the key costs 2^(n-1) calls to the encryption function on average, which lead to this convention of expressing the strength of an algorithm in bits.Thus you could understand "n bit strength" as "Breaking this costs approximately as much as breaking a symmetric encryption algorithm with an n bit key."
But they differ in other cases. A few examples:

- An RSA key with a length 2048 bits only has a strength of about 112 bits.
- A hash with length 128 bits can only have 64 bits of collision resistance.
- 3DES takes a 168 bit key, but only offers 112 bits of security, due to a meet-in-the-middle attack.

Table 1. Homomorphic Operations over Cryptosystem

Cryptosystem	**Homomorphic Operations**
RSA	Multiplication mod n
Elgamal	Multiplication, Exponentiation*
Paillier	Addition
Goldwasser-Micali	XOR
Benaloh	Addition, Subtraction
Naccache-Stern	Addition, Subtraction, Multiplication*

For Achieving high performance and security users can select any of modern symmetric encryption like AES.

V. Keymanagement Process

Keymanagement is a primitive process as in cloud computing concerned, managing encryption keys effectively are vibrant. Unless the creation, secure storage, handling and deletion of encryption keys is carefully monitored, unauthorized parties can gain access to them and render them worthless. And if a key is lost, the data it protects becomes impossible to retrieve. However, as more encryption software is implemented in different parts of the storage infrastructure, the number of keys to be managed increases.Today's cryptographic key management is largely based onsymmetric and asymmetric encryption algorithms. Symmetric algorithms utilize a solitary private key for both encryption and unscrambling of information. Asymmetric algorithms contrast in that they encode information with an public key and afterward decode it with a private key. The upside of asymmetric encryption is established in the publically known encryption key, permitting anyone to encode data in a manner that exclusive the substance holding the private key can decode it. In return for this preferred standpoint, asymmetric key algorithms are altogether more asset serious and depend upon confused hypotheses in science, themselves making an interest for advancement in the field of mathematics.

Symmetric-key cryptography algorithms are very fast but not that versatile. Key management with only symmetric-key algorithms is very difficult and non-repudiation is unattainable. Asymmetric-key cryptography, also known as public-key cryptography, resolves these problems. Public-key cryptography also provides digital signatures for non-repudiation and key agreement techniques that greatly simplify key management.

Porticor Homomorphic Key Management (PHKM) protocol
The Porticor Homomorphic Key Management (PHKM) protocol involves the following three entities
1. The Porticor Virtual Key Management (PVKM) service (runs on the Porticor server).
2. The Porticor Usage (Created by the user and at allorganization on the cloud).
3. The User (a human who is denoted by a different client platform).

The Client holds a master key, which is utilized mutually with the apparatus and PVKM key-shares to reproduce particular keys for information encryption. The part of the PVKM is to help the Machine in key administration without knowing master keys or particular keys and empower distinctive cases of the Apparatus to reliably recreate particular keys by consolidating relating key shares. The particular keys are then used to scramble different capacity questions, for example, singular documents.

For cloud services that require provider-managed encryption key management, The most serious key management infrastructure includes a hardware security module, or HSM, which allows for dedicated storage with high-performance key access for both encryption and decryption operations.**Porticor** is a vendor offering key management services, with split keys and homomorphic encryption, which allows mathematical operations to be performed on data that is already encrypted.

VI. System Performance Using Effective Cryptosystem

System performance may involve one or more of the following[6]:

- Short response time for a given piece of work
- High throughput (rate of processing work)
- Low utilization of computing resource(s)
- High availability of the computing system or application
- Fast (or highly compact) data compression and decompression
- High bandwidth
- Short data transmission time

Illustrating System Performance Over Symmetric and Asymmetric Algorithms. Where on four different product size additive and multiplicative operations over homomorphic encryption applied schemes .

Table 2. Comparison of Symmetric and Asymmetricalgorithms

Algorithms	DES	Blowfish	RC5	3DES	AES	RSA
Key Size	56 (+8 parity bits)	32-448(default 128)	Max 2040	112,168	128,192 or 256	1024 to 4096
Block Size	64	64	32,64 or 256	64	128,192 or 256	Variant.
Number of Rounds	16	16	1-255(12 suggested)	48	10(128),12(192),14 (256)	1
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Key type	Private Key	Private Key	Private Key	Private Key	Private Key	Public Key
Speed	Very slow	Fast	Slow	Slow	Very fast	Slow

Evaluation Parameters

The performance of encryption algorithm is evaluated considering the following parameters.

A. Encryption Time B. Decryption Time

The encryption time is viewed as the time that an encryption calculation takes to produces a figure content from a plain content. Encryption time is utilized to ascertain the throughput of an encryption plan, is computed as the aggregate plaintext in bytes encoded isolated by the encryption time. Examinations investigations of the consequences of the chose distinctive encryption plan are performed[1].

Hypothesis result for Encryption algorithm AES, DES and RSA are shown in following graph, which shows the comparison of three algorithm AES, DES and RSA applied on various customer purchased product data for experiment[7].

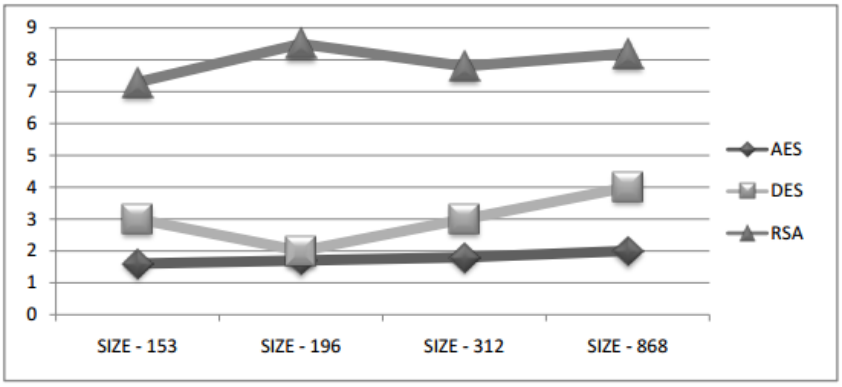

Figure 5 : Comparison of Encryption Time among AES, DES, and RSA

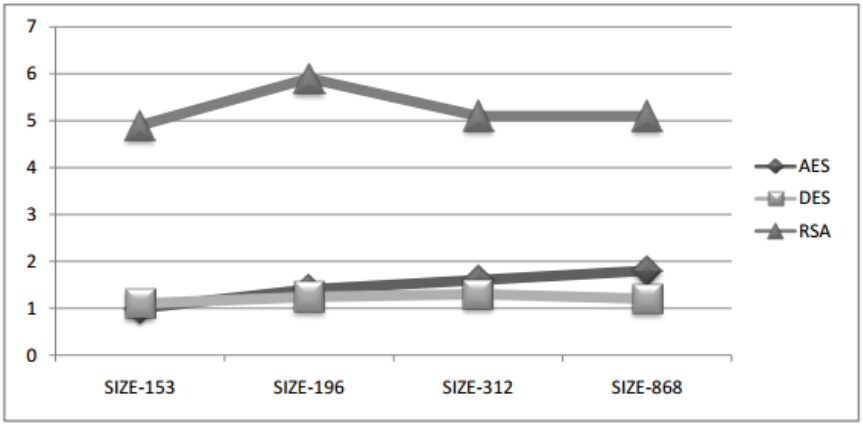

Figure 6. Comparison of Decryption Time among AES, DES, and RSA

By analyzing Fig-5 , Fig-6 which shows time taken for encryption and decryption on various product size by three algorithms. RSA algorithm takes much longer time compare to thetime taken by AES and DES algorithm. AES and DES algorithm show thevery minor difference in time taken for encryption and decryption process from the hypothesis result, we evaluated that AES algorithm is much better than DES and RSA algorithm over securing cloud server. For Achieving high performance and security users can select any of modern symmetric encryption like AES.

VII. Conclusion

In this paper, we explored over Effective Crypto System for achieving security and performance over market basket data analysis i.e on customers purchased product data. And also comprehend the several crypto algorithms applied on homomorphic encryption scheme with respect to keymanagement we dealt with Porticor Homomorphic Key Management (PHKM) protocol and Illustrating System Performance Over Symmetric and Asymmetric algorithmswe evaluated that AES algorithm is much better than DES and RSA algorithm over securing cloud server.Future work is to be focused on the challenges of cloud encryption key management are still a major barrier to storing sensitive data within cloud provider environments. key management will be a major focus area for cloud security in the coming months and years.

References

[1]. Singh Narjeet, Raj Gaurav. "Security On Bccp Through Aes Encryption Technique". International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-4, 813 – 819. pp. 817.
[2]. Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In 18th Annual Eurocrypt Conference (EUROCRYPT'99), Prague, Czech Republic , volume 1592, 1999
[3]. Julien Bringe and al. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication, Springer-Verlag, 2007.
[4]. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2) :120-126, 1978. Computer Science, pages 223-238. Springer, 1999.
[5]. Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 469-472, 1985.
[6]. Article :https://en.wikipedia.org/wiki/Computer_performance
[7]. Dr. Prerna Mahajan & Abhishek Sachdeva ,"A Study of Encryption Algorithms AES, DES and RSA forSecurity"Volume 13 Issue 15 Version 1.0 Year 2013, Global Journals Inc. (USA)
[8]. Yasuda, M., Yajima, J., Shimoyama, T., Kogure, J.: Secret totalization of purchase histories of companies in cloud (in Japanese). In: 29th Symposium on Cryptography and Information Security–SCIS 2012 number 3D-2. IEICE, (2012)
[9]. Craig Gentry, A Fully Homomorphic Encryption Scheme, http://crypto.stanford.edu/craig/craig-thesis.pdf, 2009.
[10]. Samunnisa et al., International Journal of Computer Engineering In Research Trends ,Volume 3, Issue 2, February-2016, pp. 42-27