Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVII, Issue I, Jan-June 2023

UGC Approved Journal
ज्ञान-विज्ञान विमुक्तये
UGC
Sr.No. 26412

PERFORMANCE ENHANCEMENT OF CLOUD SECURITY USING HOMOMORPHIC AUTHENTICATION APPROACH

Shreekant Sharma and Dr.Abid Hussain

Research Scholar, School of Computer Applications and Technology, Career Point University
Kota, Rajasthan, India

ABSTRACT

The most dynamic and exciting area in the service delivery industry is cloud computing. Implementing security in the Cloud is currently very popular. As a result of the expansion of the Cloud environment, security limitations on users and service providers are growing. The goal of this study is to propose a more effective method of data integrity verification, "Cloud Audit." Our method is based on a homomorphic tag and combinatorial batch code version of the Paillier homomorphic encryption system. To achieve homomorphic encryption on data blocks, use a Paillier Homomorphic Cryptography (PHC) system enabling us to launch data processes on this block. In order to allocate and store integral data into various distributed cloud servers, combinatorial batch codes are used. We have developed a Hadoop and MapReduce-based programme to illustrate our methodology. We have evaluated this submission using a number of criteria. The results of the experiments have demonstrated the efficacy of the suggested technique. Our approach has significantly outperformed other contemporary approaches.

Keywords: Paillier Homomorphic Cryptography, Hadoop, Cloud Audit**.**

1. Introduction

The capacity to process and analyse sensitive data safely is crucial in the age of digitization and cloud computing. However, safeguarding data in unreliable environments presents major difficulties for conventional security measures. By allowing secure calculations on encrypted data, homomorphic encryption has emerged as a game-changing solution to this issue, protecting the secrecy and privacy of sensitive data. A key component of data security is authentication, which aims to confirm the identity of entities accessing or modifying the data. The data is often subject to security issues during data decryption in traditional authentication techniques. Researchers have looked at homomorphic encryption as a viable workaround to get around this restriction and execute authentication operations on encrypted data without the requirement for decryption.

In order to process data securely and privately in untrusted contexts, homomorphic encryption authentication, which combines the advantages of homomorphic encryption and authentication methods, is explored in this research article. This methodology offers a novel method for authenticating while safeguarding the confidentiality of sensitive data by utilising the special qualities of homomorphic encryption, such as the capacity to compute on encrypted data. Homomorphic Encryption (HE) is a recent area of research in cryptography that was developed to assist users in protecting the confidentiality and privacy of their data by enabling computations to be performed over encrypted data by untrusted parties. In contemporary real-world applications like cloud computing, data aggregation in wireless sensor networks, electronic voting, spam filters, etc., HE becomes a critical requirement.

When utilised by untrusted parties, HE will permit the development of new techniques that can operate over encrypted inputs to produce encrypted outputs without knowing anything about the primitive data. As a result, user privacy is assured. In the literature, a number of homomorphic concepts have been introduced. In [1], [2], and [3], a state of the art of the current HE algorithms is provided.

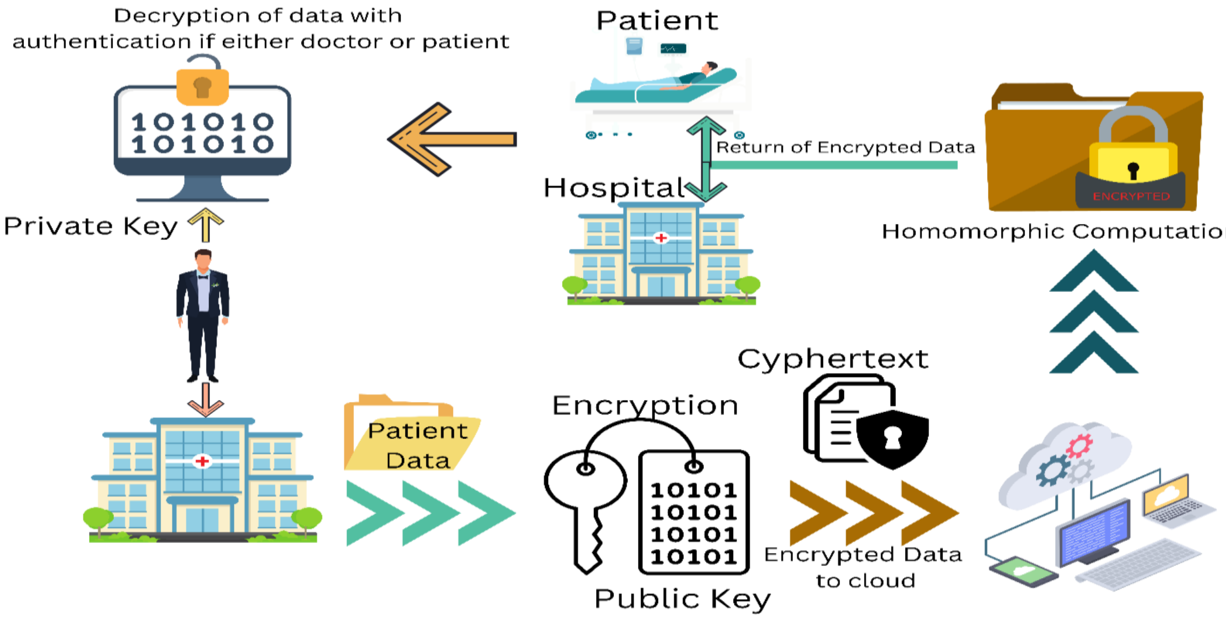

Figure 1. Homomorphic Encryption in Healthcare sector.

Since encryption techniques often forbid processing on encrypted data, processing always takes place on unencrypted data. Contrarily, homomorphic encryption enables computation on encrypted data and gives the user outputs that are also encrypted. In addition to enabling the processing of encrypted data, homomorphic encryption also protects privacy. Key generation, encryption, and decryption are the three algorithms that make up traditional public-key encryption; however, a homomorphic encryption feature is also necessary. Has an effective algorithm for homomorphic properties. Eval with PK encryption as the input. Fully homomorphic encryption (FHE) is defined as a system that meets the two following fundamental properties of addition and multiplication: and can be written as

$$[EnC_k(X_1) + EnC_k(X_2)]modN = EnC_k([X_1 + X_2]modN) \qquad \text{….. 1}$$

$$[EnC_k(X_1) \times EnC_k(X_2)]modN = [EnC_k([X_1 \times X_2]modN)]modN \qquad \text{….2}$$

In which X1, X2 are the two text files of the patients data in a given ring Z_n and where EnC is the algorithm applied for the encryption and K is the symmetric key.

Where as Key, C is a circuit created from the ciphertexts and set C_t.

Eval(pk, C_t ,C_e) then encrypts C_t(a1, a2,...., at) under pk, where C_t(a1, a2,...., at) is the output of C_t on inputs (a1, a2,...., at). C_e = (c_p1, c_p2,....c_pt) encrypted under public key pk. In healthcare this scenario can be very useful if maintained and deployed properly.

Homomorphic encryption in healthcare

In healthcare the system of homomorphic encryption can play a vital role and can be implemented using following procedure

Step 1: The client (a patient or a doctor) transfers data to a third-party service provider for the purpose of running a query or other operation.

The client encrypts the data before transmission.

Step 2: The customer then requests that the cloud service provider run a certain operation on the data and deliver the results.

Step 3: Next, the cloud service provider uses some function f(to perform activities using homomorphic encryption characteristic.

Step 4: The client receives encrypted findings.

Step 5: The client computes the decryption at its end using the decryption function, recovering f(message).

2. Literature survey

A digital revolution is taking place in the medical services sector. Modernising medical care has ushered in a new era of computerised health and wellbeing. Information about medical services is obtained from many sources (such as sensors connected to patients) and stored in specific medical services clouds (such as private and public clouds). Additionally, the quantity of combined medical data is sizable enough to be considered "Big Data". The need for securely sharing patient data across such different medical services clouds is becoming increasingly pressing as cloud medical services become a well-defined component of the medical services market. Additionally, with Accountable Treatment Organisations (ACOs) (such as medical service providers, specialists, clinics, and protection suppliers) collaborating to deliver top-notch treatment, there is a greater than ever before demand for continuous availability throughout cloud medical services. It is desirable to have a disentangled patient-driven paradigm in which patients can switch providers while continuing to provide their data in a usable manner for improved diagnosis and treatment, as well as, eventually, for improved global health. Currently, medical service providers who have sensitive patient data in personal medical clouds located all over the world are hesitant to exchange such data due to security and privacy concerns. The need for a secure link across various medical care clouds increases as healthcare providers shift to local and public cloud-based services. Furthermore, compliance with protection and security standards is a laborious task for the medical care Information Technology (IT) framework because it is mandated by the Health Insurance Portability and Accountability Act (HIPAA) [6] and Health Information Technology for Economic and Clinical Health (HITECH) [7]. Additionally, with the growth of the Internet of Things (IoT) market and its integration into the enormous information cloud stage, there is increased concern about security and protection in the context of cloud-based medical services. Numerous academics contributed their research on homomorphic encryption. Partial homomorphic encryption (PHE), somewhat homomorphic encryption (SWHE), and fully homomorphic encryption are the three types of homomorphic encryption. PHE allows just one operation over encrypted data, either addition or multiplication. SWHE assesses the circuit up to a certain depth or limit and supports a finite amount of operations. Over encrypted data, FHE supports both actions an infinite number of times.

Homomorphic Encryption

Homomorphic Cryptography Good cloud computing protocols can solve the issues the cloud faces, hence Secure Function Evaluation (SFE) is becoming more important. SFE is a crucial tool when creating protocols for information sharing between numerous parties while maintaining data confidentiality. A method that uses the SFE protocol and can be directly applied to encrypted data is homomorphic encryption. It can be defined as If it is possible to compute En (Func(P, Q)) from En (P) and En (Q), where 'Func' can be one of the operations +,, or * without requiring the private key, then the encryption is homomorphic.

Homomorphic encryption is of three types: partial homomorphic system, somewhat homomorphic system and fully homomorphic system. An encryption technique is identified as Somewhat Homomorphic if it performs a restricted amount of addition and multiplication on encrypted information A probabilistic asymmetric algorithm for public key cryptography was created by Pascal Paillier. It incorporates an additive that is intractable since it is based on the "Decimal Composite Residuosity Assumption (DCRA)". Its nature is additive.

It utilises various keys for encryption and decoding and is comparable to RSA. It is used in electronic voting, where each vote is encrypted but only the "sum" is decrypted, because of its malleable nature. For database operations, CryptDB uses the Paillier cryptosystem and enables SQL queries on encrypted data. The Paillier encryption scheme offers semantic protection from specific plaintext assaults. The Paillier's security is dependent on integer factorization. where 'n' should ideally be 2048 or 3072 bits. G must be a multiple of n when choosing the parameter, and it should be chosen as small as possible for better performance. Pascal. The subsequent equation can be used to calculate it:

$$\gcd[L(g^{\lambda} \cdot \mathrm{mod} n^{2}), n] =1 \qquad \text{.........3}$$

Problem attribution

Data security and privacy are now crucial components of many cloud-based apps, multiparty computation situations, etc. Homomorphic encryption is a recently developed method that addresses the issues of data privacy and secrecy. However, it is still quite difficult to use these homomorphic encryption techniques in practise. The primary issues that we have found in the current system are listed below: For some cryptographic techniques, the size of the cypher text is larger than the original plain text after the encryption process has been applied to the plain text data. The cause can be connected to a cushioning technique. Therefore, using this encrypted data in calculations will need more processing time. Cypher text may include noise components that become only those cypher messages whose noise estimation stays within a specific threshold value may be accurately decrypted using the subsequent homomorphic multiplication computations, which are relatively complex.

Comparison of partial homomorphic encryption schemes

Name of algorithm	**Multiplicative homomorphic**	**Additive homomorphic**	**Hard problem base**	**Encryption**	**Decryption**	**Key generation**
13	No	Yes	HR Problem	$E_r(m1)=\{y^{m1} u^r \bmod n : u \in (Z_n)*\}$, Where m1 is an element in Z_r and u a random number in $(Z_n)*$	$(y^{-i} c)^{\phi/r} \equiv 1$ message m1 is generated by extensive search for $i \in Z_r$	r is a prime number that can be divided by two huge prime numbers, p, and q. p-1, r, and p-1/r should all be substantially prime numbers, with n = pq and r and q-1/r also being reasonably prime. Select $y \varepsilon (Z_n) = \{x \varepsilon Z_n\}$ such that gcd(x, n) = 1 and y / r

						= 1modn, φ is (p-1) (q-1), and the public key is y, r, n, and the private key is p and q.
21	Yes	No	LP factorization	$c = m^{e}modn$	$m = c^{d}modn$	$\varphi =(q - 1)(p - 1)$, $ed \equiv 1mod\varphi$,q and p are prime nos. and (e,d) is key pair
09	No	Yes	Quadratic residuosity			n=pq and random y as quadratic non residue modulo n i.e.. (yn = 1)and(y, n) as public key and (p,q) is secret key
11	Yes	No	Discrete logarithms	$c_1, c_2) = (g^{k}$, $my^{K}{}_{A}$) in $Z^*{}_{P}$	$c_2(c^{a}{}_{1})^{-1}$ in $Z^*{}_{P}$	Public key is (g, q, yA), yA = g^{a} in $Z^*{}_{p}$ and Private key is a, p being large prime, g being a cyclic group's generating element $Z^*{}_{p}$ and $q = p - 1$, a is any random number
15	No	Yes	Composite residuosity problem	$Em = g^{m} \cdot r^{n}modn^{2}$ where $m < n$	$M = D(E_m) = L(E^{\lambda}{}_{m} (modn^{2}))/ L(g^{\lambda}(modn^{2})) modn$	p and q being large prime numbers such that gcd((p−1)(q−1), pq) = 1. calculate n = pq and λ (carmichael's function)= lcm(p − 1, q − 1), select random

						integer g ∈ $Z^{*}{}_{n}{}^{2}$with gcd(n, L($q^{\lambda modn2}$ = 1)) where function L (Lagrange function) = L(u)’ = (u−1)/n for every u within subgroup $Z^{*}{}_{n2}$ Public Key (Encryption): (n, g) Private Key (Decryption): λ

Materials and Methods

The FHE programme is divided into four categories in this section. These sophisticated cryptographic techniques serve as an introduction to completely homomorphic encryption algorithms. These standards are frequently used to evaluate research articles.

- Learning with mistakes (LWE/RLWE);

- Lattice-based cryptography;

- NTRU

Lattice-based encryption

A sophisticated cryptosystem is lattice-based cryptography.

It is the top-ranking post-quantum cryptosystem; specifically, lattice-based cryptography is believed to be impervious to extremely fast quantum computers. Lattice-based cryptosystems are built on challenging challenges, such as the shortest non-zero vector in the grid and the closest lattice vector to the provided vector in the case of the Closest Vector Problem. A lattice is any evenly spaced grid of points in n-dimensional space. is noise that gets louder as the number of homomorphic operations gets bigger. Correct decryption becomes difficult if the noise level increases significantly.

Gentry's method is partly homomorphic (SHE), which means it can only handle a certain number of homomorphic processes before needing to be refreshed via the bootstrapping mechanism. This method is ineffective since it involves re-encrypting data. In the beginning, ciphertext was produced through bitwise encryption, in which each bit of data was encrypted separately. To evaluate any Boolean circuit, or to do any calculation, first define the calculation in XOR and AND gates. Bit addition and multiplication (modulo 2) correspond to XOR and AND bitwise operations. The instantaneous division of a calculation into bits.

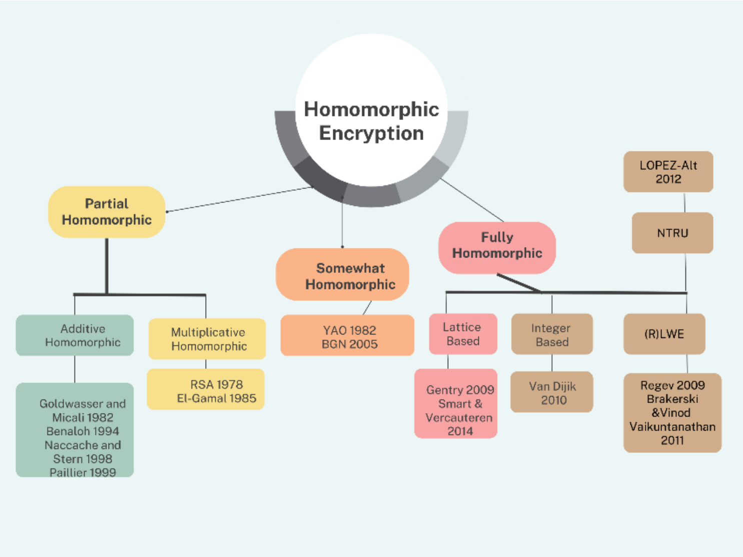

Figure 2: Classification of Homomorphic Encryption

However, if a calculation is immediately broken down into bit operations, it produces deep and sophisticated computing circuits that SWHE cannot handle and that require encryption, or bootstrapping.

Results

Healthcare Homomorphic Encryption

Electronic health records (EHR), a digital record of a patient's medical history maintained by hospitals or other healthcare providers, are known as patient health records in the healthcare sector. It contains demographic information, medical records, medical histories, and clinical data. Electronic health records (EHRs) are formal recordings of medical data produced by any healthcare professional. The quality of service and cost-effectiveness are projected to increase with the digitization of patient health information. Additionally, it makes it easier to access patient medical records whenever and wherever it is possible. The major objective of EHRs is to bridge the communication gap between healthcare professionals in order to deliver better care at lower costs. Additionally, it makes it easier to access patient medical records whenever and wherever it is possible. The major objective of EHRs is to bridge the communication gap between healthcare professionals in order to deliver better care at lower costs. Effective management of electronic health records is crucial for concerns related to data security because electronic health records (EHRs) contain a significant amount of sensitive data that is not only accessible to the doctor but also to a number of other sources like insurance companies and staff members.

Including radiology records like ECG, X-RAYS, and CT scans as well as laboratory results, patient demographic data, and medical history, a shared EHR has a demanding and complicated structure of sensitive data. A full secured model is necessary and must adhere to all rules and regulations set forth by governing and legal authorities. A secure model guarantees that only those parties with a legitimate need-to-know privilege granted by the patient will have access to sensitive information. When receiving an HIV/AIDS treatment, a patient may decide to purposefully conceal certain aspects of his health status until and unless a certain treatment choice is offered. As a result, it's essential to have a quick, easy, secure, and trustworthy method for patients to approve the number of medical partners that can access their entire or partial data. There are many methods for protecting data, such as anonymization and pseudonymization. Both of these methods can be used to safeguard a person's medical history.

Conclusion

Data privacy is more important than ever in the internet age. The cloud computing revolution has increased demand for outsourcing apps. Customers use the service by uploading their data to the cloud, where it is analysed and a result is returned. The consumer gains from it, and third-party service providers are exposed to sensitive data. Despite being encrypted, data presents a challenge because they need to be decoded before usage. Decrypting renders it susceptible to everything that was attempting to safeguard it. In the future, homomorphic encryption—which processes data while maintaining privacy and security—might be the best solution for this issue. HE has been present for more than three decades, but completely homomorphic encryption saw rapid advancement from Gentry's pioneering research to today's effective implementations. It is believed that digitising a patient's medical records will improve the effectiveness and efficiency of care while also reducing costs. Electronic health records (EHRs) do, however, contain a significant amount of sensitive data that is accessible to a variety of sources, including insurance providers and staff employees, in addition to doctors. For problems with data security, EHR administration is crucial.

References

[1] Fau S, Sirdey R, Fontaine C, Aguilar-Melchor C, Gogniat G. Towards practical program execution over fully homomorphic encryption schemes. In: P2P, parallel, grid, cloud and internet computing (3PGCIC), 2013 IEEE eighth international conference on; 2013. p. 284–90.

[2] Fontaine C, Galand F. A survey of homomorphic encryption for nonspecialists. Springer, EURASIP J Inf Secur 2007;2007(1):1–10.

[3] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21(2):120–6.

[4] Gentry C. A fully homomorphic encryption scheme. Phd thesis. Stanford University; 2009.

[5] Gentry C. Fullyhomomorphic encryption using ideal lattices. In: STOC '09 proceedings of the forty-first annual ACM symposium on theory of computing Pages 169-178 ACM New York, NY, USA; 2009.

[6] van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. Fully homomorphic encryption over the integers. EUROCRYPT'2010 (LNCS) vol. 6110. pp. 24–43.

[7] Sharma I. Fully homomorphic encryption scheme with symmetric keys. In: Rajasthan Technical University, Kota, University College of Engineering, Department of Computer Science and Engineering; 2013.

[8] Xiao L., Bastani O., Yen I.-L. An efficient homomorphic encryption protocol for multi-user systems. Citeseer, IACR Cryptology ePrint Archive 2012 193.2012.

[9] Kipnis A., Hibshoosh E. Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification. IACR Cryptology ePrint Archive 2012 637 2012.

[10] Akinori K, Keisuke T, Keita X (2007) Multi-bit cryptosystems based on lattice problems. In: International Workshop on Public Key Cryptography, pp 315–329. Springer, New York

[11] Steven DG (2002) Elliptic curve paillier schemes. J Cryptol 15(2):129–138

[12] Ronald LR, Adi S, LeonardMA A method for obtaining digital signatures and public-key cryptosystems. CACM 26(1):96–99

[13] Andrew CY (1982) Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982), pp 160–164. IEEE

[14] Dan B, Eu-Jin G, Kobbi N (2005) Evaluating 2-dnf formulas on ciphertexts. In: Theory of cryptography conference, pp 325–341. Springer, New York

[15] Yuval I, Anat P (2007) Evaluating branching programs on encrypted data. In Theory of Cryptography Conference, pp 575–594. Springer, New York

[16] Michael F, Neal K (1994) Combinatorial cryptosystems galore! Contemp Math 168:51

[17] Tomas Sander, Adam Young, and Moti Yung. Non-interactive cryptocomputing for nc1. In Proceedings of the 40th Annual Symposium on Foundations of Computer Science, FOCS '99, page 554, USA, 1999. IEEE Computer Society

[18] Kristian Gjøsteen. Subgroup membership problems and public key cryptosystems. 2004

[19] Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. An introduction to mathematical cryptography, volume 1. Springer, 2008

[20] Craig G, Shai H (2011) Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In: 2011 IEEE 52nd annual symposium on foundations of computer science, pp 107–109. IEEE

[21] Dan B (1998) The decision diffiehellman problem. In: International algorithmic number theory symposium, pp 48–63. Springer, New York

[22] Peikert C (2016) A decade of lattice cryptography. Found Trends Theor Comput Sci 10(4):283–424

[23] Nigel PS, Frederik V (2014) Fully homomorphic simd operations. Des Codes Cryptogr 71(1):57–81

[24] Marten Van D, Craig G, Shai H, Vinod V (2010) Fully homomorphic encryption over the integers. In: Annual international conference on the theory and applications of cryptographic techniques, pages 24–43. Springer, New York