iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Symmetric Fully Homomorphic Encryption with Access Control Over the Cipher

C.N.Umadevi[1], N.P. Gopalan[2]
[1]*Research and Development Centre, Bharathiar University, Coimbatore, Tamilnadu, India*
[2]*Professor, Department of Computer Applications, National Institute of Technology, Tiruchirapalli, Tamilnadu, India*

Abstract: Cloud computing is a benevolent paradigm which drives the current world but the security threats makes its ratification slower. Fully Homomrphic Encryption(FHE) is a solution to this problem and it also permits the Cloud users to perform mathematical computations on ciphers without deciphering. By adopting FHE, Cloud computing can provide "Computation-As-A-Service" without loss of security, privacy and confidentiality. But the current internet based services suffers to provide a secure access control over the heirloom resources. This paper is an extension of our conference paper in [23]. The secret data is encrypted using Symmetric Fully Homomorphic Encryption based on Smith Normal Form. And it addresses a new technique which provides access control over the encrypted data using XACML for constituting the access policies(SFHE-ACC).
Keywords: Fully Homomrphic Encryption, Access Control, Extensible Access Control Markup Language, Fibonacci-P number.

I. INTRODUCTION

Cloud computing is a growing technology evolved from cluster, grid and utility computing. Cloud computing provides "Everything-as-a-service" as "pay-per-use", to the end user. The users of cloud can share resources from anywhere through connected devices at any time. A cloud computing model can be visualized as distributed parallel computing over data center resources rather than centralized computing at data centers. The three classes of cloud called Public, Private and Hybrid clouds can be employed over Intranets as well as in open Internet. Cloud computing is gaining its popularity through its scalable, durable, flexible, highly available, inexpensive and on-demand computing resources regardless of its complexity and volume. Though cloud has many advantages, it has many problems too. Level of security is the success factor of a new technology [26]. Data privacy and security is the primary threat faced by cloud model in this data centric world. The conventional encryption techniques can ensure security and confidentiality over the cloud data and such an environment do not supports Computation-As-A-Service since, the encrypted data must be decrypted for performing operations on it.

Encryption technique with homomorphic property is called Homomorphic Encryption (HE) which supports performing operations on the encrypted data. Homomorphic encryption can be used in an open and un trusted network where the data is to be kept confidential but involved in some computations. Let *d* be a confidential data, the resultant of an encryption function *Enc(d)* is the cipher C, *Dec(C)* is the decryption function and *f* is an arithmetic function on *C* then by homomorphic encryption,

$$\text{Dec}\,(f(C)) = f(d)$$

For example, let *f* be an integer addition and *C1* and *C2* are the ciphers of the plain text *d1*,*d2* respectively then,

$$Dec\,(C1+C2) = d1+d2$$

The homomorphic encryption technique can provide privacy, security and confidentiality over cloud data without loss of computation-as-a-service. Consequently the critical cloud applications can be accessed by the end user, without affecting the security and privacy. But to prevent the access of everything by all end users, the cloud must stipulate some control over the access. Attribute Based Encryption (ABE) a cryptographic primitive, realizes access controls cryptographically[22]. ABE encapsulates the user's private key with the access policy. Variations of ABE are Key Policy-ABE (KP-ABE) and Cipher Text Policy-ABE (CP-ABE). Both KP-ABE and CP-ABE differs by the place of encapsulating access policies, whether in the cipher or in the key. But CP-ABE has a fore deal of protecting confidential cipher text even on a compromised data server [7]. This paper is an extension of [23].

A. Literature Survey

From 1970 onwards the data are secured by privacy homomorphism [21] and are only partial homomorphic systems. They support either addition or multiplication but not both. In 2009 Craig Gentry [5] proposed a new scheme called Fully Homomorphic Encryption [FHE] system, supporting all possible operations on ciphers and this scheme is based on Ideal Lattices. Later on several variations and advancements of Craig's method was developed ([4], [6], [7],[8], [9], [11], [12], [15]) with Lattices in background.

All these techniques are initially developed as Partial Homomorphic Systems and later on transformed into FHE system using techniques called Bootstrapping. Thus making the system having computational complexity and impractical because of larger key size, cipher size and noise generation. An approach in [16] introduced a new FHE scheme based on integers to overcome the above said problems. Since then several variations of integer and Linear algebra based Homomorphic schemes are evolving. Some of the techniques used in Fully Homomorphic Encryption scheme and their problems are given below:

S.no	Techniques used	Problems
1	Vector based	Learning With Errors (LWE)
2	Polynomial based	Polynomial LWE (PLWE)
3	Ring based	Ring base LWE (RLWE)
4	Squashing technique	Sparse Subset Sum Problem (SSSP)
5	Lattice based	Bounded Distance Decoding Problem (BDD)
6	Integer based	Approximate Greatest Common Divisor Problem (ASCD)
7	Polynomial based	Polynomial Coset problem (PCP)

Identity Based Encryption (IBE) was introduced in 1985[24]. The identity in IBE was replaced with an attribute set in Attribute Based Encryption (ABE) [25]. ABE supports fine-grained access control system by encapsulating user's private key with the access policy and it was classified as KP-ABE and CP-ABE [26]. Both differs by the place of embedded access policies, whether in the cipher or in the key. First CP-ABE was proposed in 2007[27]. Goyal et al., [28] proposed a CP-ABE based on number theory. Gentry, Sahai and Waters achieved the first Identity Based Fully Homomorphic Encryption (IBFHE) and Attribute Based Fully Homomorphic Encryption (ABFHE) [28]. An extension of this work is done by Clear and Mc Goldrick([29], [30]) called multi-identity IBFHE. But these schemes are not "pure" that is the operations are in limited depth.

B. Our Contribution

The proposed scheme is an extension of [23] in which a new FHE scheme using Q_p^n matrices as symmetric keys was introduced. It is based on linear algebra concept and the homomorphic property of the system was achieved through Smith Normal Form (SNF). In the prior work [31] the security and privacy of the cloud data is preserved with a very small key size of order of O (1), a fixed cipher text size and through this proposed work, access control over the cipher text is enforced. The proposed system involves the following entities of cloud: Cloud Owner (CO), Cloud User (CU) and Cloud End-User (CEU). The owner of the cloud resources is CO, the tenants are the CU and CEU are authorized users who are allowed to perform operations on the cipher text on behalf of the CU without decrypting. Thus the problem of key management and key sharing can be avoided.

The symmetric FHE scheme in [31] protects the encrypted data and CEU are allowed to perform operations over the cipher without decryption. When this scheme is used in a private cloud, the CEU will access over the entire data server of encrypted data. Thus the necessity to provide a controlled access over the data server arises. Moreover in the CP-ABE schemes the end users can decrypt the cipher.

The proposed scheme modifies this concept by allowing the CEU only to access the cipher and restricted to decrypt. The access policy is expressed in Extensible Access Control Markup Language (XACML), it is attached to the cipher and any access which is satisfied to the policy can only gain access the cipher to operate on it. The access policy of CEU is decided by their location, IP address, time and number of times they have accessed the cipher. Thus the proposed scheme, Symmetric Fully Homomorphic Encryption with Access Control over the Cipher Text (SFHE-ACC) provides an encrypted, controlled access over cipher texts stored in a private cloud for its CEU.

C. Organization

The rest of the paper is organized as follows: Section II presents the preliminary concepts. Section III introduces the encryption and decryption process. Section IV discusses the access control over encrypted cipher, Section V deals with the security analysis, Section VI involves some discussions and Section VII concludes the paper.

II. PRELIMINARIES

A. Access Control

Permission to access a resource is called Authentication and selective restriction to a resource is called Access Control (AC) [24]. The set of rules that define the conditions under which an access may take place is called Access Control Policy [25]. In other words Access Control is a process of mediating every user requests to the resources of a system and determining whether the request should be denied or granted, it involves two steps: authentication and authorization. A system must ensure availability, reliability and safety. In Discretionary Access Control (DAC) the access permissions are determined by the owner, Mandatory Access Control (MAC) the access request of user is controlled centrally and it is designed using information flow control. A combination of MAC and DAC is called Roll Based Access Control (RBAC). A special case of MAC is called Multilevel Access Control which has different implementations based on the context. Many access policy structures are found in the literature ([22], [26], [27], [28], [29], [30]), but the recent structures are XML based and they are attracting the interest of the researchers. The Organization for the Advancement of Structured Information Standard's (OASIS) Extensible Access Control Markup Language (XACML) is a XML based access control policy frameworks. XACML is a general purpose access control policy specifying language. In XACML access control and authorization policies for XML objects can be expressed with the help of a core scheme and a namespace. From XACML policy file the following functions can be performed:

1) A simple resource access request.
2) Whether the subject is allowed to login to access a resource.
3) To allow the subject to login on a specific time, date, specific IP address and even location based on city or country.

XACML produces the following responses for an access request: Permit, Deny, Indeterminate and Not Applicable. XACML can be used to represent a broad range of access policies.

The proposed scheme translates all the integers in a Ring $Z_N$to operations on matrix $M_4(Z_N)$, where N is nonprime and it is product of 2m numbers. The scheme is made CPA secure by a security parameter denoted by λ and to withstand η number of plain text attacks, m and λ are selected such that $\eta=m\ ln poly(\lambda)$ where $poly(\lambda)$ is a fixed polynomial in λ. This scheme involves $2m$ odd, mutual prime numbers $p1_i$ and $p2_i, 1\leq i\leq m$, let $f_i=p1_i\ p2_i$ and $N=\prod_{i=1}^{m} f_i$where N is a RSA type modulus of unknown factorization. Primality testing of a number takes only polynomial time, thus choosing $2m$ odd mutual prime numbers, which involves a time complexity of $O(m)$ that is $O(poly(\lambda))$. By making the large integer factorization infeasible, factoring N in polynomial time is also infeasible.

III. ENCRYPTION AND DECRYPTION TECHNIQUES

The encryption and decryption system translates all the integers in a Ring $Z_N$to operations on matrix $M_4(Z_N)$, where N is nonprime. This scheme involves $2m$ odd, mutual prime numbers $p1_i$ and $p2_i$, $1\leq i\leq m$, let $fi=p1_i\ p2_i$and $N=\prod_{i=1}^{m} f_i$ where N is a RSA type modulus of unknown factorization and it is the product of 2m numbers [23]. The security parameter is denoted by λ and to withstand η number of plain text attacks, m and λ are selected suchthat, $\eta=m\ ln\ poly\ (\lambda)$ where $poly\ (\lambda)$ is a fixed polynomial in λ and the secret data x is translated to a matrix$M_4(Z_N)$. The system involves the following three algorithms where n1, n2 are any two arbitrary integer key pairs, x is the data to be encrypted, P is the Fibonacci P-number and C is the cipher text:

Keygen (P, (n1, n2)) $\rightarrow Q_P^{n1}$ and Q_P^{n2}
Enc (x, (Q_P^{n1} andQ_P^{n2})) $\rightarrow$ C
Dec(C, ((Q_P^{n1})$^{-1}$ and(Q_P^{n2})$^{-1}$)) $\rightarrow$ x
Where all the above are modulo N operations.

A. Addition: Dec (Enc (d1) + (Enc (d2)) mod N=d1+d2
B. Subtraction: Dec (Enc (d1) - (Enc (d2)) mod N=d1-d2
C. Multiplication: Dec (Enc (d1) × (Enc (d2)) mod N=d1×d2

IV. ACCESS CONTROL OVER THE CIPHER

The Cloud User encrypts the private data using the secret key as explained in Section 3, and the access policy for the each known CEU is constructed in XACML with policy attribute values described in Table.2.

TABLE 2
ATTRIBUTES OF CEU AS EXPRESSED IN ACCESS POLICY

S. No.	Policy Attributes	Description
1	Access ID	Unique ID for each CEU to be keyed in during data access
2	Subject	Name or role of the CEU
3	Object	Resource allowed for access
4	Action	Access rights like READ,COPY,PRINT
5	Max. Access Time	The maximum number of accesses
6	IP address	To confirm that the CEU access the data from preferred machine
7	Time	The time allotted for CEU to access
8	Location	The city or country from which CEU is allowed for access
9	Duration	The start and expiry date of data access

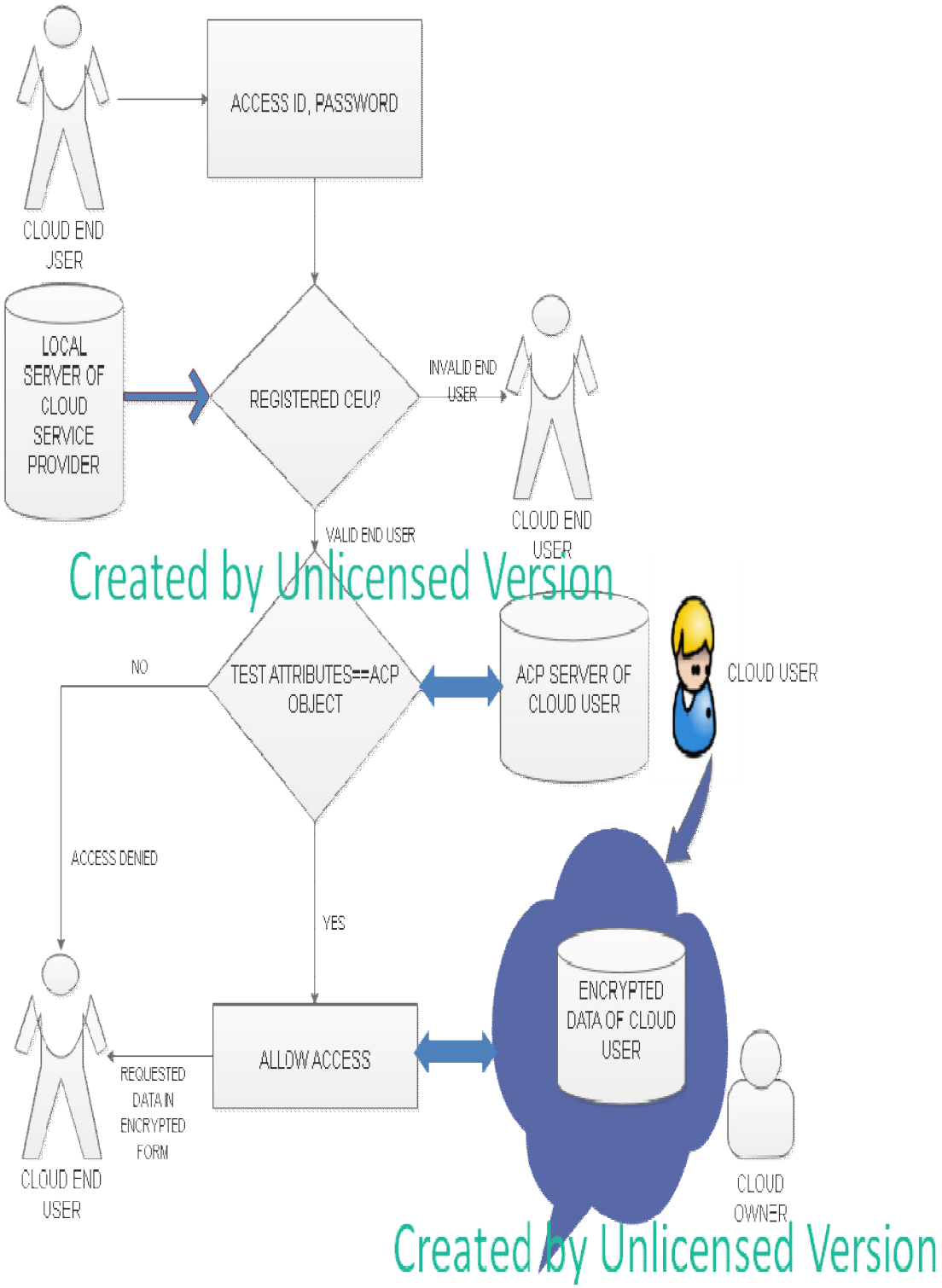
The XACML file is encapsulated into ACP Object and stored in ACP server of the CU and the secret data is encrypted by the CU which is stored in the Cloud. Services to CEU are provided by the Cloud Service Provider (CSP) who is restricted to access the ACP server. The CSP validates the CEU by storing only the Access ID and password in a local server and on validating the CEU it collects the *test-attributes* of CEU like Access ID, IP address, Location and time, date of login through cookies and communicates them to the CU. The CU verifies the XACML access policy stored in ACP server of CU, when there is a match the response is "allow" and the requested data in encrypted form is sent to the CEU otherwise the response will be "deny".
The software components of Cloud User which performs the validation of access rights of a CEU are described below:

A. Access Policy Verification
The Cloud End User request is processed by the CUwith the software components, Access Control Policy Enforcement (ACPE), Access Control Policy Decision Point (ACPDP) and ACP-File handler.

B. Access Control Policy Enforcement
ACPE receives the request from CSP and forwards the test-attributes to the ACPDP to make decisions based on ACP Object. And sends response to the CSP based on ACPDP.

C. Access Control Policy Decision Point
ACPDP searches for an ACP Object whose Access ID matches with the Access ID of the test-attributes, when there is a match it validates the access policy attributes with the test-attributes. On successful validation it initiates the ACP File-Handler.

D. ACP File-Handler
The number of access on an object by a subject is maintained by the ACP File-Handler using a counter. When the decision made by the ACPDP is "allow", it gives a command to the ACP File-Handler to handle this issue by sending Max. Access Time attribute. ACP File-Handler, increments its counter and compares with the Max. Access Time. When the counter value is greater than the Max. Access Time, it issues an error message to ACPDP, thus the CEU is not allowed to access the specified object.



V. SECURITY ANALYSES

The security of the system is discussed based on the characteristics of cloud and also of secure outsourcing of the secret data.

A. Confidentiality

Data ever remains encrypted for the CEU and it can be decrypted only by the CU. Since, the secret key is private to the CU, the reverse engineering process is impossible. The confidentiality of the data is preserved and unauthorized data access is restricted.

B. Scalability

By selecting the required amount of storage resources, the massive, secret and encrypted data can be stored successfully. It is easy to revise or update the access rules because they are expressed in XACML. And the existing structures like, ACL, Access Matrix and so on needs to be entirely revised.

C. Security

The security of the system is guaranteed by Fully Homomorphic Symmetric Key Encryption with Smith Normal Form [23]. In a hybrid cloud environment, the data owner has to perform major computations on the stored private data, thus the workload increases. Enough manpower could solve this problem but, the secrecy leverages. Thus the proposed system can be employed in such situations without loss of privacy and secrecy.

D. Data Outsourcing

Government organizations, private companies spread across continents and even military networks can use this scheme withassured security, confidentiality, authorization with access control. Data outsourcing is supported by this system, so hosted services can be delivered through internet to the data consumers.

VI. DISCUSSIONS AND FUTURE WORK

Most of the social networks based on Cloud Computing architecture are built so as to provide security and confidentiality towards its user's information. Though the private data can be made secure through encryption techniques, some form of access control must be enforced in the Cloud. For data sharing and collaboration, the encryption technique and key management suffices to be strong and secure. When the system is homomorphically encrypted the key management and distribution can be excluded but a secure access control mechanism must be provided over the end user to operate on the encrypted data. The present paper addresses a new Symmetric Homomorphic encryption scheme and an access control mechanism over the encrypted data. Thus the data is restricted from unauthorized access.

This approach is beneficial because it enhances information privacy, improved data security and eliminates the burden of data owner for computations over the encrypted data with access control without decrypting.

VII. CONCLUSION

In this paper we have presented a simple Fully Homomorphic Encryption technique based on symmetric key. It also provides a new method to control the access of multiple cloud users. Cloud computing can optimize the utilization of computer resources in a cost effective manner. But due to broad access and distributed architecture, cloud computing has data security, confidentiality and access control as its main challenges. The new FHE scheme discussed in this paper solves the above said problems without computational overhead. This scheme finds its application in customized advertisements, real-time health analysis, mining from large datasets, outsourcing forensic image recognition and for a financial corporation which requires financial privacy.

REFERENCES

[1] C.Gupta and I. Sharma, A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds, Proceedings of Networks of the Future (NOF), 2013 Fourth International Conference. Pp.1- 4, 23-25 Oct. 2013.

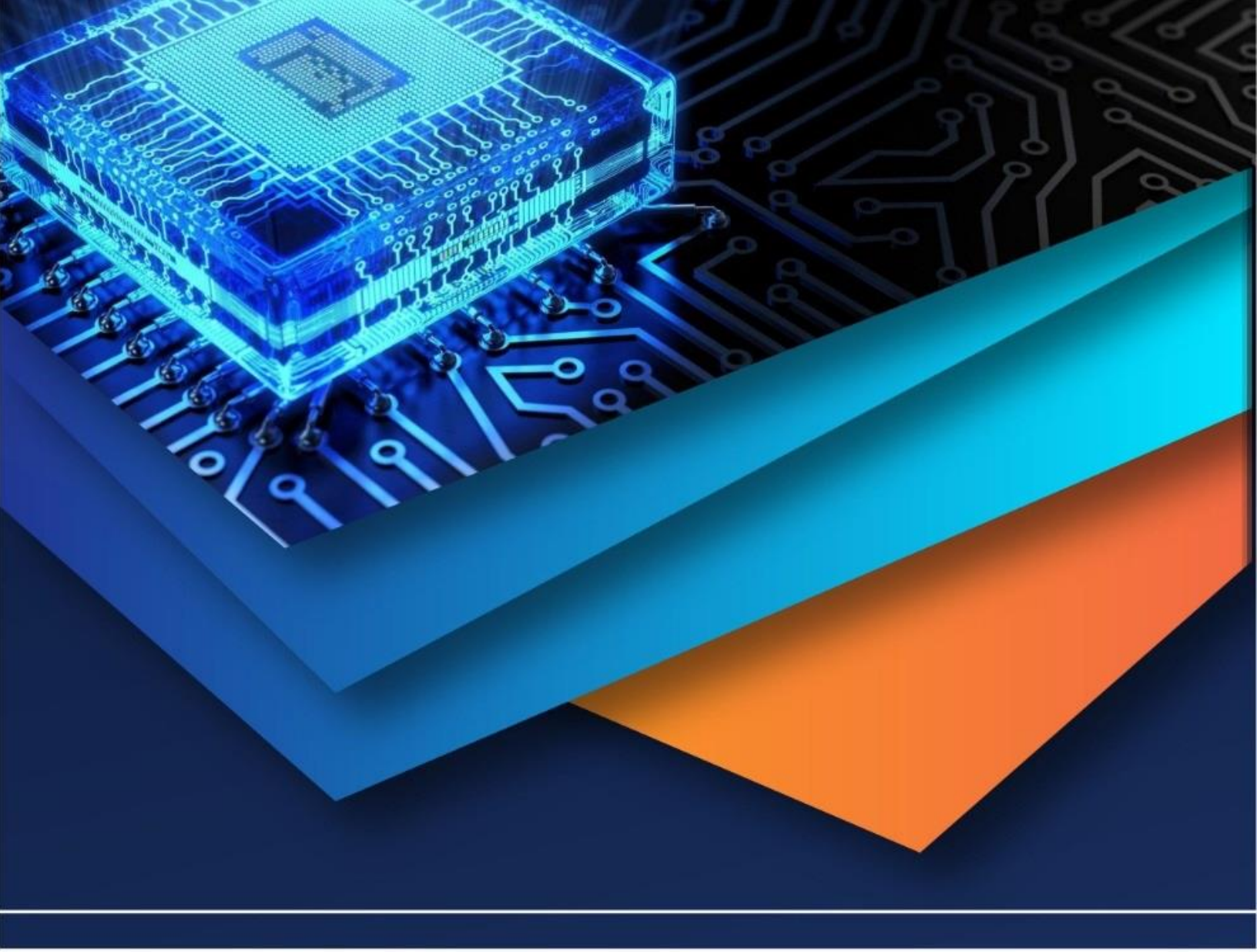
[2] Iti Sharma, A Symmetric FHE Scheme Based on Linear Algebra, International Journal of Computer Science & Engineering Technology (IJCSET), vol. 05, pp. 558-562, 2014.

[3] Coron JS, Lepoint T, Tibouchi M., New multilinear maps over the integers, Annual Cryptology Conference 2015 Aug 16 (pp. 267-286), Springer Berlin Heidelberg.

[4] Cheon JH, Stehlé D, Fully homomophic encryption over the integers revisited, Annual International Conference on the Theory and Applications of Cryptographic Techniques 2015 Apr 26 (pp. 513-536), Springer Berlin Heidelberg.

[5] Gentry, A Fully Homomorphic Encryption scheme, Dissertation. Sep 2009. Available at https:// crypto. stanford.edu/Craig/Craig-thesis.

[6] Gentry and S. Halevi, Implementing Gentry's fully homomorphic encryption scheme, EURO-CRYPT 2011, LNCS, Springer, K. Paterson (Ed.),2011.
[7] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, Fully homomorphic encryption over the integers, Proceedings of Eurocrypt-10, Lecture Notes in Computer Science, vol 6110,. Springer, pp. 24-43, 2010.
[8] J.-S Coron, A.Mandal, D.Naccache, and M. Tibouchi. "Fully homomorphic encryption over the integers with shorter public-keys", Advances in Cryptology - Proc. CRYPTO 2011, vol. 6841 of Lecture Notes in Computer Science. Springer, 2011.
[9] Z. Brakerski and V.Vaikuntanathan, Efficient fully homomorphic encryption from (standard) LWE, Foundations of Computer Science, 2011. Available at Cryptology ePrint Archive, Report 2011/344.
[10] Z.Brakerski, C.Gentry, and V.Vaikuntanathan, Fully homomorphic encryption without bootstrapping, Cryptology ePrint Archive, Report 2011/277.
[11] R. Rivest, L. Adleman, and M. Dertouzos, On data banks and privacy homomorphism's, Foundations of Secure Computation, pp. 169-180, 1978.
[12] N. P. Smart and F. Vercauteren, Fully homomorphic SIMD operations, Cryptology ePrint Archive, Report 2011/133.
[13] A.P.Stakhov, A Generalization of the Fibonacci Q-Matrix, Reports of the National Academy of sciences of Ukraine", vol.9, pp.46-49, 1999
[14] A.P. Stakhov,"A History, the Main Mathematical Results and Applications for the Mathematics of Harmony, Applied Mathematics, vol.5, pp. 363-386, 2014.
[15] Zhigang Chen, Jian Wang, ZengNian Zhang and Xinxia Song, A Fully Homomorphic Encryption Scheme with Better Key Size, Cryptology ePrint Archive, Report 2014/697.
[16] N.P.Smart1 and F.Vercauteren, Fully Homomorphic Encryption with Relatively Small Key and Cipher text Sizes, Cryptology ePrint Archive, Report 2009/571.
[17] J.Coron, T.Lepoint and M.Tibouchi, Batch fully homomorphic encryption over the integers, 2012. Available at http://eprint.iacr.org/2013/36.
[18] J.Kim, M.S. Lee, A.Yun and J .H. Cheon. CRT-based fully homomorphic encryption over the integers, 2012. Available at http://eprint.iacr.org/2013/57.
[19] L.Xiao, O Bastani and I-L.Yen., An efficient homorphic encryption protocol for multiuser systems, 2012. Available at http://eprint.iacr.org/2012/193.
[20] Donald E. Knuth, The Art of Computer Programming, Volume 1, Fundamental Algorithms.
[21] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2), pp. 120-126, February 1978.
[22] Sahai and B.Waters. Fuzzy Identity Based Encryp-tion. In Advances in Cryptology – Eurocrypt, volume3494 of LNCS, pages 457–473. Springer, 2005.
[23] C.N. Umadevi and N. P. Gopalan. 2016. Fully Homomorphic Symmetric Key Encryption with Smith Normal Form for Privacy Preserving Cloud Processing. In "Proceedings of the International Conference on Informatics and Analytics" (ICIA-16). ACM, New York, NY, USA, Article 101, 5 pages. DOI: http://dx.doi.org/10.1145/2980258.2980462
[24] https://en.wikipedia.org/wiki/Access_control.
[25] http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf.
[26] ShyamNandan Kumar, and Amit Vajpayee, "A Survey on Secure Cloud: Security and Privacy in Cloud Computing." American Journal of Systems and Software, vol. 4, no. 1 (2016): 14-26. doi: 10.12691/ajss-4-1-2.
[27] Sabri K, Obeid M. A temporal defeasible logic for handling access control policies. Applied Intelligence, 2016, 44(10): 30–42.
[28] Cheng Y, Park J, Sandhu R. Attribute-Aware Relationship-Based Access Control for Online Social Networks. Lecture Notes in Computer Science, 2014. 8566:292–306, Springer Berlin Heidelberg.
[29] Bibin K Onankunju "Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013 ISSN 2250-3153.
[30] Guoyuan Lin, YuyuBie, Min Lei "Trust Based Access Control Policy in Multi-domain of Cloud Computing", JOURNAL OF COMPUTERS, VOL. 8, NO. 5, MAY 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY