iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6145

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 6 Issue VI, June 2018- Available at www.ijraset.com

Survey Paper on Attribute Based Encryption & Decryption

Pooja Prajapati[1], Makarand Samvatsar[2]
[1]*Research Scholar,* [2]*Assistant Professor Department of Computer Science Patel College of Science & Technology, Indore*

Abstract: ***Cloud security is the most critical task while considering its working environment, i.e. outsourced, distributed and utility based. In such cases making the users data confidential, increases the trust over the system. Also the security procedure does not make the availability affected in any ways. The users of these kind of systems is always retained the services and securities preliminaries with respect to the data itself. As the cloud user can access its data frequently and if here some encryption is used which requires decryption and the repetitive process continues to increase the overheads. It requires some mechanism in which encryption is performed and if the user requires performing some operations on secure file without decrypting it can be fulfilled. Thus homomorphic encryption lets the user facilitates about the performing operations on encrypted data which reduces the complexity of confidentiality operations. Also to prevent Cloud Servers from being capable to discover both the data file contents and user access privilege information used to generate key along with the fastest access of secured data by using Attribute-based encryption (ABE).***

In this Paper, we offer a new KP-ABE formation with constant cipher text size by adopting and applying the knowledge of the identity-basedbroadcast encryption method. In our algorithm independent of the number of cipher text features, and the number of bilinear pairing estimations is reduced to a constant. We prove that our scheme is semantically secure and locked in the selective-set

Keywords: Attribute Based Encryption, Cloud Storage, Data Storage, Homomorphic.

I. INTRODUCTION

Cloud computing is an overwhelming technology used to reduce the users operational and management worry about the memory by introducing and comprehensive mechanism of distributed, grid, autonomic computing. Cloud computing is creating a boom in present scenario. This area is gaining popularity and becomes a boom presently due to its wide applicability like client server and other browser dependent programming. It includes the delivery of various computing and storage aspects as a service to the end users. On comparing with respect to the measuring benefits among all security services is considered as one of the high priority open issues in adopting and accepting the cloud computing model. This service model faces a number of open issues that impact its credibility. The major issue is the data confidentiality; each and every person wants his data to be safe and secure from the third party. Data confidentiality against cloud servers is hence repeatedly preferred when users outsource data for storage in the cloud. Thus the security issues are generated because of these low trusted outside processing entities such as providers. Therefore, the trust factors at such services are very low. The consumer always likes to make its data & service in an isolated manner from external persons. In few practical situations of service application systems the data confidentiality will come under juristic boundaries by taking their security issues.

II. LITERATURE REVIEW

In this paragraph, we have gone through the closely related works, which includes no collaborative, supportable division, pairing designation and the proxy re encryption. The term used here No interactive Verifiable Computation: which simply concludes that the no interactive verifiable computation enables a computationally weak client to outsource or subcontract the computation of a function to single or more workers or we can call them as operatives here. The operative perform and operates the result of the function evaluation, as well as there is a no interactive proof that the computation of the function was carried out correctly. Hence, these schemes, deal with outsourcing of the general computation problems, which tends to preserve the privacy of input data, and this preservation can be used to outsource decryption in ABE systems. However, here the schemes proposed in use Gentry's fully homomorphism encryption system which can be used as a building block, and thus the overhead in these schemes is currently too large to be practical and it proved the disadvantage of this method. Recently, Parno et al. gave a proposal to establish an important connection between the two verifiable computation and ABE adopted algorithm. In this proposed method they stated to show how to construct a verifiable computation scheme with public delegation and public verifiability from any ABE scheme and how to

construct a multifunction verifiable computation scheme from the ABE scheme with outsourced decryption presented in given proposed system. After this Goldwasser et al. Propose a succinct functional encryption scheme for general functions, and tried to show that, by replacing the ABE scheme used in the system with their neat functional encryption scheme, one can be easily obtain a delegation scheme with is both publicly verifiable and secret key, in the logic that the prover does not learn anything about the input or output of the function being delegated. This stated system was proven to be more beneficial than that of the past and present once.

A. Attribute-Based Encryption with Verifiable Outsourced Decryption

[Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian WengIEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 8, AUGUST 2013]

Attribute-based encryption (ABE) is a public-key base done-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves e pensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green *et al.* proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied by that user's attributes or access policy into a simple cipher text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. In this paper, we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users.

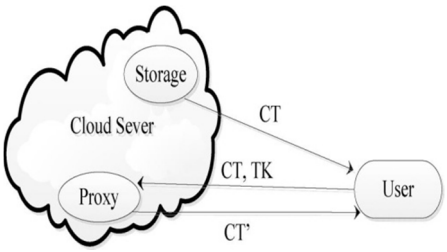


Figure 2.1: Description of ABE system

Here user interacts with the cloud through his tasks of the storage and with the help of the proxy server. Proxy servers identify the user then authenticate it.

B. How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption

[Bryan Parno Microsoft Research ,Mariana Raykova Columbia University, Vinod Vaikuntanathan_University of Toronto Supported by an NSERC Discovery Grant and by DARPA under Agreement number FA8750-11-2-0225]

The wide variety of small, computationally weak devices, and the growing number of computationally intensive tasks makes the delegation of computation to large data centers a desirable solution. However, computation outsourcing is useful only when the returned result can be trusted, which makes verifiable computation (VC) a must for such scenarios. In this work we extend the definition of verifiable computation in two important directions: public delegation and public verifiability, which have important applications in many practical delegation scenarios.

Yet, existing VC constructions based on standard cryptographic assumptions fail to achieve these properties. As the primary contribution of our work, we establish an important (and somewhat surprising) connection between verifiable computation and attribute-based encryption (ABE), a primitive that has been widely studied. Namely, we show how to construct a VC scheme with public delegation and public verifiability from any ABE scheme. The VC scheme

verifies any function in the class of functions covered by the permissible ABE policies. This scheme enjoys a very efficient verification algorithm that depends only on the output size. Strengthening this connection, we show a construction of a multi-

function verifiable computation scheme from an ABE with outsourced decryption, a primitive defined recently

C. Achieving Secure, Scalable, and Fine-grained Data

[Access Control in Cloud Computing Shushing Dept. of ECE, Illinois Institute of Technology, Liu Department of Computer and Information Engineering, Version 2056- isn 4569.] Service consumers can make sure that their sensitive data which should be kept private from third party that means which the users specify not to be mutual with their service providers is not revealed to their service providers even if there is no assistance from their service providers. Our approach does not cause much overhead on service performance. This paper is systematized as follows. We will articulate users' data confidentiality protection from service earners in cloud computing systems. This theory will be used to determine whether our approach can protect users' confidential data from service providers. In the problems of current cloud computing architecture in expressions of safeguard of users' data confidentiality will be discussed. We will present our approach, including a new architecture for cloud computing system and using data obfuscation to achieve the above both goals of our approach. Our data mystification and de-obfuscation developed for protecting user's data con denasality in cloud computing will be argued. Here we will present an example to show how the confidentiality of user's data can be threatened by our methodology in cloud computing systems. Experimental results are presented to show that our style has reasonable performance. We had discussed the advantages and limitations of our approach as well as future work.

D. Security Threats in Cloud Computing

[Farhan Bashir Shaikh Department of Computing & Technology Sajjad Haider IT Department NUML Islamabad, Pakistan, ISN provided on acceptance letter.. Version 2013-04-5678 [1] - v15.doc]

In this paper gave a new security and provenance proposal for data forensics and post examination in cloud computing. According to them their proposed system is typified, the proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed secure provenance scheme is working on the bilinear pairing method and they have claimed it as the necessary building blocks of data forensics and post examination in cloud computing environment. Using provable security techniques, they have formally verified that there proposed scheme is safe and sound in the standard model. There proposed secure provenance system for cloud computing includes five parts: [1] ―Setup, KGen, AnonyAuth, AuthAccess, and Prove Track‖. Due to the ample security features, the scheme proposed produces reliable facts for data forensics in cloud computing. They claim that their proposed system can be a cause to move forward for the wide recognition of cloud computing. The strength of their work is the proposed secure provenance system and limitation of their work is that their proposed scheme is difficult to implement as it is based on complex mathematical model which is very difficult to understand.

E. Cryptographic Secure Cloud Storage Model with Anonymous Authentication and Automatic File Recovery

[Sowmiya Murthy et all Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, India E-mail: sowmiyamurthy@gmail.com]

In our proposed security framework, we implement the Role Based Access Control (RBAC) model [11]. We preferred the RBAC access control method where users are

classified based on their roles and the access rights are defined accordingly. The implementation of anonymous authentication in RBAC is a challenging process and forms a new combination of secure cryptosystem in a cloud environment. There is a centralized administered control that defines the structure for interaction between “subjects” and “objects”. The subjects are entities to which execution can be attributed such as users, processes, threads, or even procedure activations. Objects are entities on which operations are defined including storage abstractions such as memory or files with read, write, and execute operations and code abstractions, such as modules or services with operations to initiate or suspend execution. Distinct privileges are typically associated with distinct operations on different objects [17]. In Table.1, we show a comparison of a number of past approaches for access control with the scheme proposed by us. It is quite evident that our decentralized scheme given in the last row is powered by the maximum number of features. It has multiple read and multiple write access, homomorphic encryption and performs anonymous authentication while hiding user attributes. The following types of access controls techniques are commonly used:

User Based Access Control (UBAC) [11] – An Access Control List contains the details of access rights defined for all users on different resources that are offered by the computing system. This method is not suitable for cloud services because of scalability issues [1]. It is difficult to update, maintain and store Access Control List (ACL). Moreover, for every operation the ACL needs to be referenced, which creates a performance bottleneck.

Mandatory Access Control (MAC) [11] [14] – Users alone do not have the right to decide on their access control privileges. Rather, it

is based on the combination of (i) The security levels associated with the data itself. These are defined by the metadata security labels according the sensitivity of data within a Multi-Level Secure (MLS) framework [15] (ii) The security clearance given to the individual processes that access data. MAC is designed for-Military based security applications and is not suitable for commercial cloud based The owners of the resources decide on the access rights for different users for these resources. The DAC technique is not always a suitable form of security mechanism for cloud services because with multiple users sharing information, it becomes very tedious to define the rights for each user. Attribute Based Access Control (ABAC) – The users get access to various resources based on user attributes that include the corresponding access policy. This too is not suitable for secure cloud-based applications as the access policies depend only upon user attributes and cannot be defined or changed dynamically for each user. Moreover, it is not possible to maintain anonymity of user to download the file.

III. PROBLEM STATEMENT

The work focuses on improving the existing security solutions using some of the modified policies and generation methodologies. But for cloud computing, where the data and its total controls are distributed over some third party servers that reduce trust over the system. To increase these factors and reliability over the system, some modified and well-performed encryption standard is required in which security operations do not bother other services. Also, when a user places their data on a cloud after encrypting, and for retrieving it data decryption is required each time even for a small change. User needs to provide some functionality by which certain level of Security can be enhanced. This can be achieved by using. In homorphic encryption some mathematical operations are applied to encrypted cipher blocks and can be retrieved. But existing systems with this property is not practically developed till now. Some extents of this property are achieved. Thus this work focuses on achieving Attribute Based Encryption (ABE).

A. Attribute Based Encryption

Green et al. wished-for an ABE system in the company of outsourced decryption that fundamentally dissolve the decryption operating cost for users. In such a system, a user provides an un-trusted server, say a cloud service provider, with a change key that allows the cloud to convert any ABE cipher text satisfied by that user's properties or access procedure into a simple cipher text, and it only incurs a tiny computational overhead for the user to recuperate the plaintext from the changed cipher text.

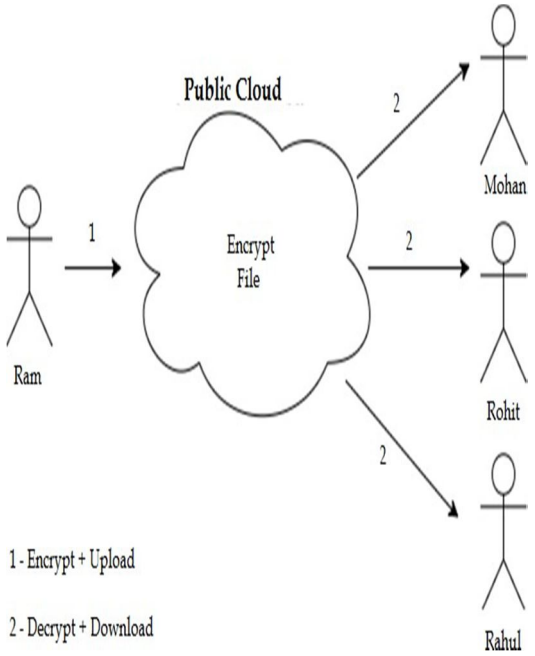


Figure 3.1 Existing System of Attribute-based encryption

Figures 3.1 show existing system, which used in Attribute-based encryption. User Ram can encrypt file and upload in cloud server then Users Mohan, Rohit or Rahul can download file with decryption. Attribute-based encryption (ABE) is a comparatively latest method that reconsiders the concept of public-key cryptography. In usual public-key cryptography, a message is encrypted for a certain receiver using the receiver's public-key. Identity-based cryptography and in actual identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by permitting the public-key to be an arbitrary string, e.g., the

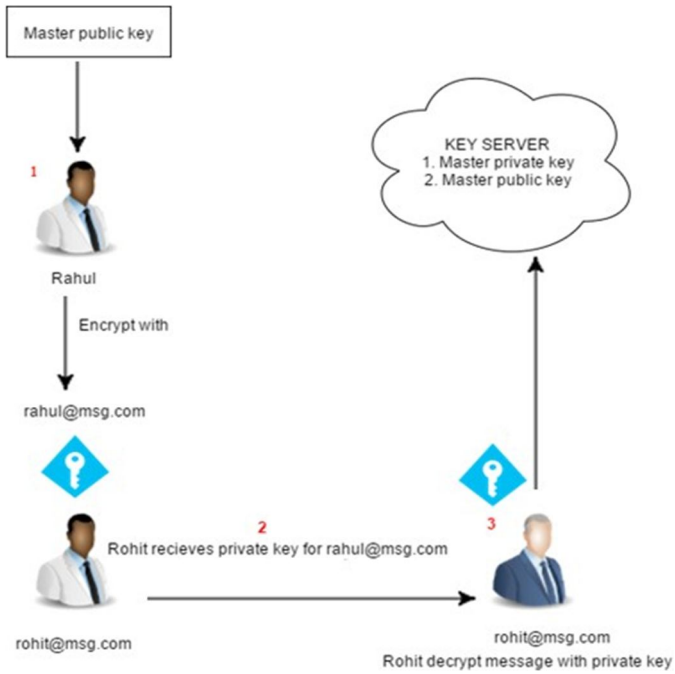


Figure 3.2: Attribute-based encryption using Master key email address of the receiver.

Attribute-based encryption using master key describe in figure 3.2. ABE turns a single step further and defines the identity not tiny but as a set of attributes, e.g., roles, and messages can be encrypted with detail near subsets of characteristics (key-policy ABE - KP-ABE) or policies defined over a set of features (cipher text-policy ABE - CP-ABE). The key concern is, that somebody should only be able to decrypt a cipher text if thesomebody clutches a key for "matching attributes" (more below) where some always issues user keys trusted party. Attribute Based Encryption can be divide in two-sub category.

1) Key-Policy Attribute–Based Encryption (KP-ABE)
2) Cipher Text-Policy Attribute –Based Encryption (CP-ABE)

B. Key-Policy Attribute Based Encryption (KP-ABE)

KP-ABE is the twin to CP-ABE in the logic that an access policy is encoded into the users secret key, e.g., (A^C) V D, and a cipher text is divided with respect to a set of aspects, e.g., {A,B}. In this example the user cannot be capable to decrypt the cipher text but would for instance be able to decrypt a cipher text with respect to {A, C}.

An essential estate, which has to be achieved by both, CP-ABE and KP-ABE is called collusion resistance. This mostly means that it should not be conceivable for different users to "pool" their secret keys such that they would together decrypt a cipher text that will neither of them would decrypt on their own (which is attained by independently randomizing users' secret keys).

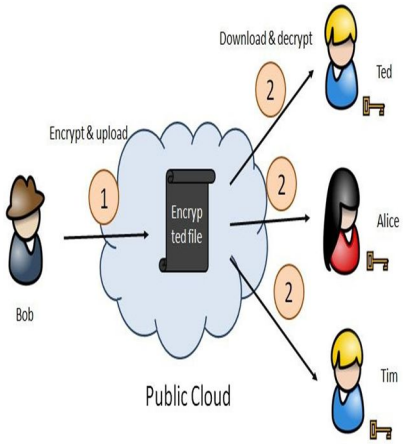
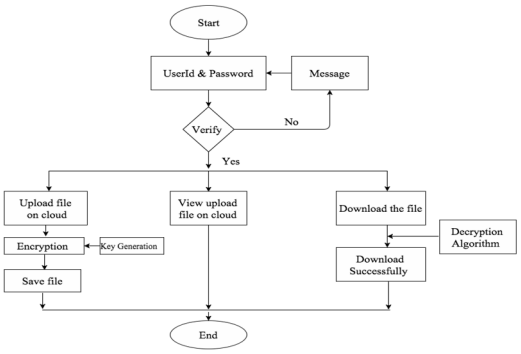


Figure 3.3: key-Policy Attribute-based encryption



IV. PROPOSED SYSTEM

Our propose framework will use three-layer system structure, in which every layer execute its own duty to ensure the data security of data in the cloud. The primary layer: accountable for user authentication. The subsequent layer: accountable for user's data encryption, and protect the users data during a convinced technique by with one symmetric encryption algorithms. The third layer: The user data for speedy decryption

A. Proposed Algorithm

Proposed Algorithms of KP-ABE with improvement are deliberated as below:

1) Kp-Abe Setup (A): Outputs public key PK and Master key MK for A as set of attribute

2) Subordinate for each attribute in A with attributes universe as U = {1, 2,..., n}

3) It defines a bilinear group G1 of prime order p with a generator g, a bilinear map e g: G1 × G1 -> G2 which has the properties of bilinearity, computability, and non- degeneracy

B. Algorithm Description

This algorithm returns an undisclosed key D enclosed with an access structure T. The resulting three steps agree the admission structure A:

1) For root node r, set value secret = y. spot all node un-assigned and mark root node assigned.

2) Recursively, for each assigned non-child node

3) If the operator is ^ (and) and its child nodes are marked un-assigned, let n be the number of child node leaf, fixed the value of each child node, except the last one, to be si ε Zp, and the value of the last node to be sn = s -Σ si. Mark this node assigned

4) If the operator is V (or), set the values of its child leaf nodes to be s. Mark this node assigned. For separately leaf characteristic aj,i ε T , compute Dj;i = Tj∧si

5) KP-ABE Decryption (E, D) this algorithm takes as input the cipher text E encrypted under the attribute set U, the user's secret key SK for access tree T, and the public key PK. Finally it output the message M if and only if U Satisfies T.

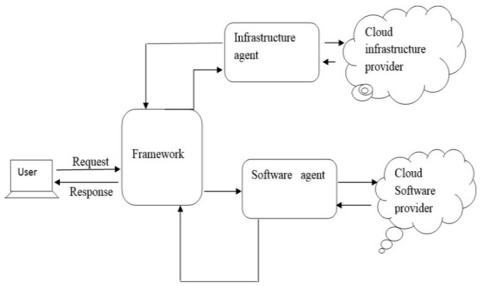


Figure 3.6 Proposed System

Propose System Contains three stakeholders like Data owner, who generates and owns the data, possessing all rights about file operation, it can pass on the same to other Cloud data users.

Cloud service provider (CSP), which is the central core component of the whole system. It also acts as a cloud data server.

User, who uses the data based on credentials received from the data owner. Following steps performed by user when interact with System

6) Data owner upload encrypted file on cloud Service provider (CSP). If later data owner want to verify that file on CSP they send request to CSP. So CSP calculates hash code for the encrypted file (KP-ABE), which is uploaded by the DO and sends it to DO.

7) DO compare the hash code received by CSP with the actual hash code to check the correctness of data, which is stored on the CSP.

8) CSP decrypt file using ABE algorithm and send to DO And DO requests for view/download the file.

9) DO Grant file Access Rights (Sharing of file) to other cloud user.

V. CONCLUSION

Futuristic results of the technique may show the improvement in providing the security with feasible operations on cipher using partially homomorphic cryptosystems and is most suitable for outsourced cloud environment. This improved encryption is faster and less computational overhead is involved. It provides the high end reliability towards the new orientation of the system.

The third party mechanism deals with continuous monitoring of user record. This monitoring along with improved throughput and efficiency is achieved. Out of these methods an enhanced secure scenarios is generated through our proposed CP-ABE. At the initial level of our research, we get the following benefits.

A. Improved security solution with less operational overheads and retains reliability on novel encryptions

B. Unauthorized access is blocked using improved key generation through user characteristics.

C. Continuous monitoring gives the user behavior measurements and analyzes the affection of such novel cryptosystem on other services.

REFERENCES

[1] Shucheng Yu , “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, in Proceedings of IEEE Infocomm, ISSN: 978-1-4244-5837-0/10, 201

[2] Srijith “Towards Secure Cloud Bursting,Brokerage and Aggregation” 2010 Eighth IEEE European conference on web service

[3] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE,KuiRen, Member, IEEE, and Wenjing Lou, Member, IEEE “Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE-2012

[4] Cong Wang1, Qian Wang1, Kui Ren1, and Wenjing Lou2,” Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, IEEE INFOCOM 2010, San Diego, CA, March 201

[5] Ms. Vaishnavi Moorthy1, Dr. S. Sivasubramaniam2,” Implementing Remote Data Integrity Checking Protocol for Secured Storage Services with Data Dynamics and Public Verifiability In Cloud Computing, IOSR Journal of EngineeringMar. 2012, Vol. 2(3) pp: 496-50

[6] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capability-based Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 201

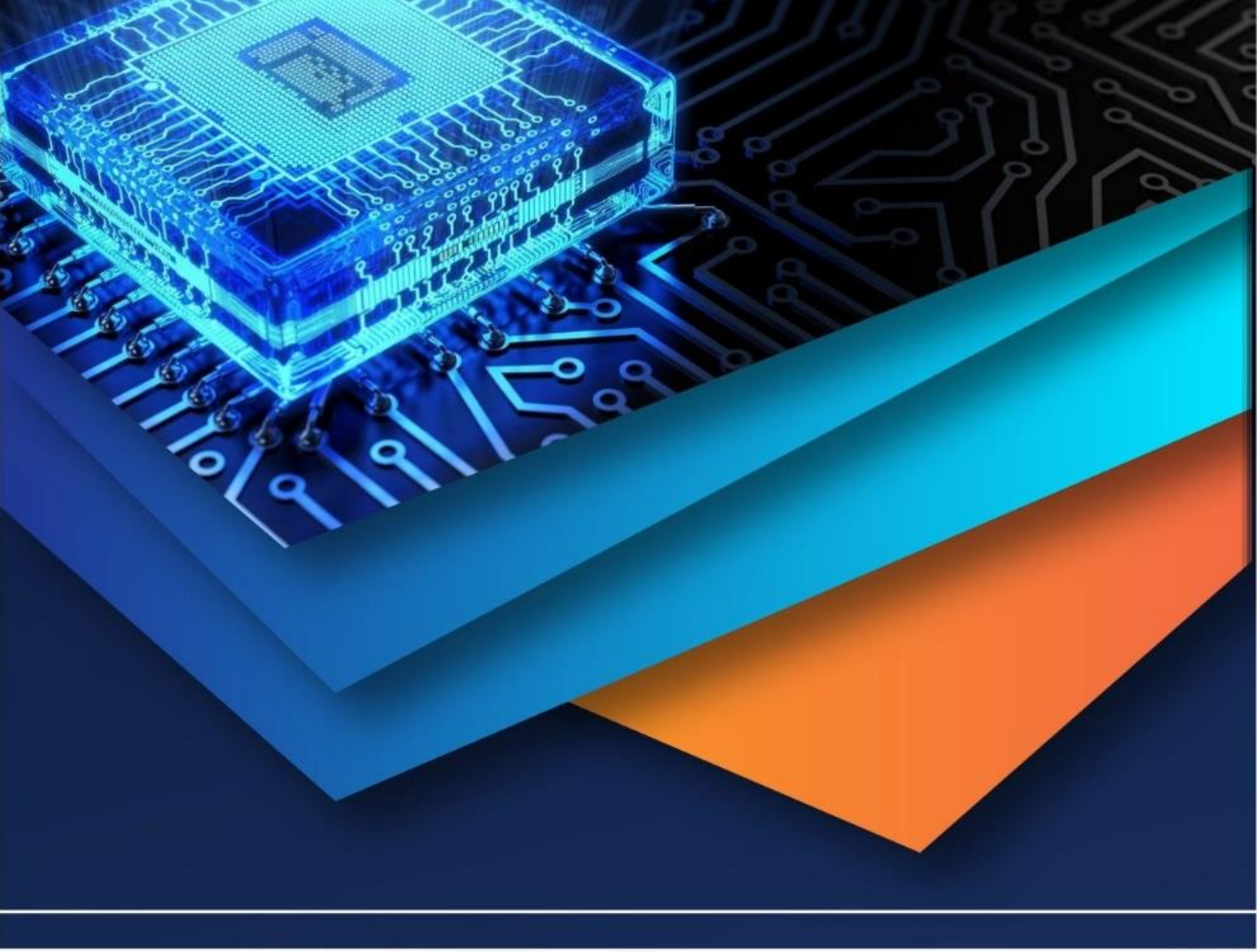
[7] Rosario Gennaro and Daniel Wichs, Fully Homomorphic Message Authenticators IBM Research, T.J. Watson, May 23, 20

[8] K. Kajendran, J. Jeyaseelan, J. Joshi, “An Approach for secures Data storage using Cloud Computing” In International Journal of Computer Trends and Technology- May to June Issue 201

[9] W. Luo, G. Bai, “Ensuring the Data Integrity In Cloud computing” In Proceedings of IEEE CCIS, 2011

[10] S. Sanka, C. Hota, and M. Rajarajan, “Secure data access in cloud computing,” in 2010 IEEE 4th International [13]

[11] H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY