iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IV **Month of publication:** April 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Enhanced Privilege Level Wise Access Control for Secure Cloud Storage

Dathi Soniya.M[1], Roshni Thanka.M[2]

Department of Computer Science and Engineering, Karunya University, India

Abstract— ***Data storage in cloud is possibly a safe and secure way for data accessing and data retrieval, but not at all criteria. Certain security guarantees for the outsourced data were needed to make sure of the access control. To achieve such security goals, many algorithms are used to keep both the data and the key in a secure way. Certain cryptographic key operations using the Advanced Encryption Standard (AES) algorithm were previously implemented that were self-maintained by a quorum of key managers that are independent of third-party clouds. In particular, the work provides insights of how to incorporate value-added security features into today's cloud storage services. Regarding the enhancement based on improving file access privilege level, Attribute-Based Encryption (ABE) is used in order to improve the security related to the clients/providers accessing the data. Accessing privilege level, like user getting policy base accessing data is concentrated. Accessing level wise is a polynomial interpolation technique, presenting the ABE scheme that can generate security keys of different class for users (like privilege) by integrating cipher text policy attribute-based encryption and hierarchical cryptographic key management. Improvement in the level of security is achieved by handling the key generation technique, using the enhancement made in this paper using ABE.***

Keywords - *Access Control, Data Security, Data Storage.*

I. INTRODUCTION

Cloud computing is an up-and-coming technology which further branches into various areas. Cloud is a scattered system that consists of a compilation of unified and virtualized computers which are presented as cohesive computing resources. The vital aim of cloud computing is to share the data and its services along with the resources among its users [20]. Each file that is created and is loaded into the cloud must be given a privilege level to access based on the policy on which the clients/providers are activated. It provides the clients to make use of loads of applications. It trusts in getting your strength back with the utilization rate of the systems and decreasing the power utilization. Pay per usage is the mode of payment to be paid. This reduced the management cost of the server. Also when there is any limitation regarding the usage of the data would be efficient in order to reduce the data traffic. Payment is done only for resources that are consumed. Even this service is a kind of making the client to be safe with their related policy and the amount of consumed data. The services provided by cloud computing is chiefly separated into three categories namely, Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (Paas) [20]. The cloud environment is an outsized open dispersed system. It is significant to safeguard the data and also the privacy of users who maintain it. Access Control methods make certain that approved user's access the data and the system. Access control is in the main a policy or practice that allows, denies or blocks access to a system. Also monitoring and recording all attempts are made to access a system [20]. Access Control might also recognize users attempting to access a system that is unauthorized. For the protection in computer security, access control is very much important.

Cloud storage is an illustration of networked enlargement storage where information/data is stored in virtualized pools. This is done for storage purposes that are generally hosted by third parties. The companies that locate perform huge data centres. The public who require their data are to be loaded buy certain storage facility from them. The data storage centre operator in the atmosphere virtualizes the data resources based on the needs of the customer and shows them as storage space. The storage spaces are used to store resources or files by the users. Essentially, the stockpile may cover transversely numerous servers and several hosts. The applications which control the cloud storage and the hosting companies play a major role in the protecting the files.

IJRASET: ISSN: 2321-9653

Security concerns become relevant as we now outsource the storage of possibly sensitive data to third parties. Particular interest is maintained by the system in two security issues. It need to provide guarantees of access control, in which we must ensure that only authorized parties, can access the outsourced data on the cloud. In particular, third-party cloud storage providers from mining any sensitive information of their clients' data for their own marketing purposes are prohibited. It is important to provide guarantees of assured deletion, meaning that outsourced data is permanently inaccessible to anybody (including the data owner) upon requests of deletion of data.

Keeping data permanently is undesirable, as data may be unexpectedly disclosed in the future due to malicious attacks on the cloud or careless management of cloud operators. The challenge of achieving assured deletion is that we have to trust cloud storage providers to actually delete data, but they may be reluctant in doing so. Also, cloud storage providers typically keep multiple backup copies of data for fault-tolerance reasons. It is uncertain, from cloud clients' perspectives, whether cloud providers reliably remove all backup copies upon requests of deletion. There is no assurance of files deleted in cloud because the copies may be replicated elsewhere even after deletion. Performance of Access control for accessing the right data at right time and by the right user. A secure overlay cloud storage system that provides fine-grained access control and assured deletion for outsourced data on the cloud, while working seamlessly atop today's cloud storage services.

II. RELATED WORKS

Many researchers are involved in improving the security level of the cloud data storage. RACS (Redundant Array of Cloud Storage) is a middleware which extends the bulk of stored data over multiple clients who provide data. RACS is placed as a replacement that performs between the client and the several repositories [1]. RACS is likely to be performed parallel communication in a disseminated atmosphere with compound proxies. Using the policies, the same set of repository can also be run on numerous proxies. RACS is used to keep away from vendor lock-in and also to condense the rate of switching clients. The client failures are tolerated and are also simple and easy to work with. All the data must pass through a RACS proxy both for encoding and decoding, hence a single proxy could either become a bottleneck [1]. Secure Overlay Services (SOS) is an architecture proposed with intent to put off DOS attacks. There are two principles behind this technique. The exclusion of communication pinch points that represent attractive DoS targets, using the filtering and the ability to make progress from capricious failures within the forwarded infrastructure. In this technique, the prevalence of attacks may be condensed by not allowing the hackers to perform any kind of denial of service attacks with the cloud [3]. Secure overlay services diminish the probability of booming attacks. Implementing an SOS infrastructure is fairly straightforward and can be done using exclusively readymade protocols and software. It is not quite an easy job to solve DDoS problem entirely. The supreme solution might be quiet complicated to get through. It may need some kind of an incorporated solution [3]. FADE is a secure overlay cloud storage system that ensures file assured deletion [11]. FADE is a sensible and readily deployable cloud storage system that focuses on defending deleted data with policy-based file assured deletion [11]. FADE is built upon paradigm cryptographic techniques, such that it encrypts outsourced data files to guarantee their privacy and integrity, and also in particularly assures about the deleted files upon revocations of file access policies [11]. They are practical to use and thus, the data owners can be made sure of the deleted file [11].

III. MOTIVATION

The security level of the key generated is to be aimed for providing a safer zone of the file to be either uploaded or downloaded from the cloud. The previously used algorithms make security for the data but, the key might be predictable in certain cases. To avoid this prediction of the key by the hackers, that plays a major role in the area of access control, better algorithms are tried out. Poly encryption can improve the level of security. In all the algorithms that we use, there is a pattern of generating the key. And this pattern must be an uncommon one and also a difficult task for the hacker to break the key pattern.

IV. METHODOLOGY

Cloud storage is a model of networked online storage where data is stored in virtualized pools of storage which are generally hosted by third parties. The files are associated with file access policies that control how files can be accessed. Policy-based file assured deletion, in which files are assuredly deleted and made unrecoverable by anyone when their associated file access policies are revoked. The essential operations on cryptographic keys must be generated so as to achieve access control and assured deletion. So it could be accessing any file easily. Whether large and small any files it

IJRASET: ISSN: 2321-9653

should be accessed, No more limitation for each subscriber. In this proposed system, the security level is improved using ABE algorithm for access control with privilege level wise, so that the possibility of predicting the secret key is completely reduced.

A. Configuration

A client/provider is an interface that connects the data and the cloud. It applies encryption (decryption) to the outsourced data files uploaded to (downloaded from) the cloud [12]. There are different ways businesses run applications today. Applications can be hosted and installed locally (on the client system), on each computer, and are referred to as standalone applications. They can also be set up through the client-server model where one computer acts as a server and other users connect to it through client computers. In this case, the application is mostly run from a private cloud. The third option is running applications through the public cloud and using SaaS.

B. Key Management

Seeking to achieve both access control and assured deletion for outsourced data using various algorithms were implemented earlier. But as for now, the possibility of predicting the key used for encryption and decryption is reduced by implementing the ABE (Attribute Based Encryption). First review time-based file assured deletion proposed in earlier work. The key manager is a server that is responsible for cryptographic key management. In the control key is time-based, meaning that it will be completely removed by the key manager when an expiration time is reached, where the expiration time is specified when the file is first declared.

C. Security Issues

The cloud may keep backup copies of any outsourced file even after it is requested for deletion. Suppose that a hacker has an access to the cloud storage and obtains the copies of all the encrypted data and already deleted files. An active file on the cloud is encrypted with a data key, which is generated using the Attribute Based Encryption that can only be decrypted by the data owner or the person who borrows the key from the data owner. The response from the key manager is protected with the ABE-based access key. As long as the attacker does not have the access key, it cannot decrypt the data key, and hence cannot decrypt the original data. A file becomes deleted when its associated policy is revoked. A deleted file is still encrypted with a data key. However, since the key manager has purged the control key for the revoked policy permanently, it loses the ability to decrypt the data key. Therefore, the attacker cannot recover the original data. Moreover, even if the attacker is powerful enough to get the ABE access key or compromise the key manager to get all control keys, the original data of the deleted file is still unrecoverable as the corresponding control key is already disposed.

D. Security Level

A client/provider is deployed locally with its corresponding data source as a local driver or daemon. Note that it is also possible to deploy the client as a cloud storage proxy so that it can interconnect multiple data sources. In proxy deployment, we can use standard TLS/SSL to protect the communication between each data source and the proxy. Security properties is given our threat model, we focus on two specific security goals that system seeks to achieve for fine-grained security control. A client is authorized to access only the files whose associated policies are active and are satisfied by the client. Policy-based assured deletion: A file is deleted (or permanently inaccessible) if its associated policies are revoked and become obsolete. That is, even if a file copy that is associated with revoked policies exists, it remains encrypted and we cannot retrieve the corresponding cryptographic keys to recover the file. Thus, the file copy becomes unrecoverable by anyone (including the owner of the file).

V. ALGORITHM

ABE (Attribute Based Encryption) is a collected works of encryption trappings based on attributes and policies assigned to the users by an authority. ABE is a new technology that supports fine grained access control along with the cryptography [18]. In particular, it allows one to match certain attributes and policies to a message being encrypted based on which the key is generated. So only a receiver who is activated to the corresponding policies/attributes can decrypt it. The attributes are boolean variables along with arbitrary labels, and the policies are computations represented as boolean circuits over the attribute variables [18].

ABE basically requires nominal access to a key authority. When the clients/providers are capable of holding the cryptographic information, then the access for the authority is no longer needed. The server who is executing the authorization may be offline, but the probability of authorization is minimised. Only when the user's rights are

IJRASET: ISSN: 2321-9653

changed, the access is required. General analysis shows that the proposed scheme is simple, efficient and secure. The proposed scheme can provide "one fits- many" encryption service. Attribute-based encryption can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipient's attributes.

ABE is a cryptographic technology where encryption and keys are generated in terms of attributes. Two main methods of ABE are discussed based on the application of the related policies and attributes. Random pieces of text that are significant within the policies are assigned when a file is encrypted. ABE is a variety of public key cryptography where unique keys are used for encryption and decryption [18]. At the time of encryption only the ABE system parameters are required, such as the public information generated initially by an authorised person and a choice of about which attributes to be applied. At the time of decryption the ABE system parameters along with a private key generated by the authorised person is required. This key must not be publicized to other users who are in need of the data.

VI. PERFORMANCE ANALYSIS

The cloud storage is untrusted and insecure. The cloud may still keep backup copies of any outsourced file after it is requested for deletion. Suppose that an attacker gains access to the cloud storage and obtains the (encrypted) copies of all active and deleted files. Security is improved in this case for both the access control and the assured deletion of data in cloud. The performance of the proposed method is improved mainly in the area of security using ABE algorithm compared to the previously used algorithms.

A. Active Files

An active file on the cloud is encrypted with a data key, which can only be decrypted by the key manager. In order to reveal the original data, the attacker has to request the key manager to decrypt the data key. The response from the key manager is protected with the ABE-based access key. As long as the attacker does not have the access key, it cannot decrypt the data key, and hence cannot decrypt the original data.

B. Deleted Files

A file becomes deleted when its associated policy is revoked. A deleted file is still encrypted with a data key. However, since the key manager has purged the control key for the revoked policy permanently, it loses the ability to decrypt the data key. Therefore, the attacker cannot recover the original data. Moreover, even if the attacker is powerful enough to get the ABE access key or compromise the key manager to get all control keys, the original data of the deleted file is still unrecoverable as the corresponding control key is already disposed.

C. Level of Security

The key generated using various algorithms are done randomly. And hence, the possibility of guessing the key is there in certain cases by the unauthorized person. But this can be avoided by the ABE algorithm. In the proposed system all the cryptographic operations are performed by the ABE algorithm. The key generated for the proposed method is based on certain attributes. The security implemented using ABE based on the key size is high when compared to the other algorithm as shown in Figure 1 as an example. To make it complicated for the hackers to try with any guesses with the key, polynomial interpolation technique is implemented in the proposed algorithm.

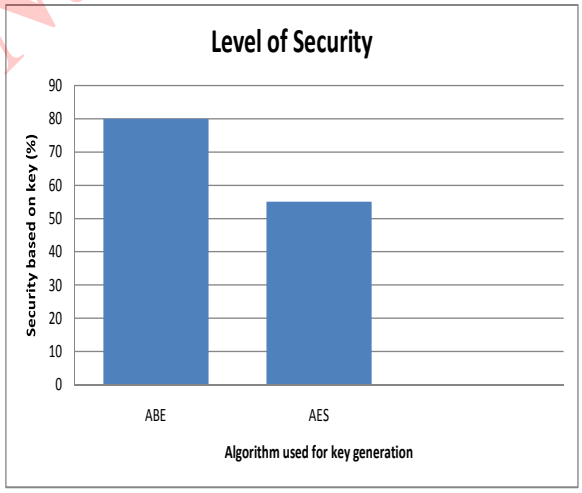


Fig. 1 Performance Level of Security

VII. CONCLUSION

The earlier implemented concepts provided access control and security of deletion of files using various algorithms in today's cloud storage services. FADE system associate files with file access policies that control how files can be accessed

IJRASET: ISSN: 2321-9653

[11]. Then present policy-based file assured deletion, in which files are assuredly deleted and made unrecoverable by anyone when their associated file access policies are revoked [11]. Several systems describe the essential operations on cryptographic keys using the multiple algorithms, so as to achieve access control and assured deletion. Regarding the enhancement based on improving file access privilege level, the ABE algorithm is introduced to raise the level of security in the existing system. Using ABE algorithm, the security level of the key is improved as the attributes are based on the name of the clients. Accessing level wise, this concept is polynomial interpolation technique. The attribute based encryption is quiet flexible and performs one-to-many encryption to provide security. The encrypted data is kept confident even if the data storage is untrusted. The privacy of the access policy is preserved specified by the authorized person who encrypted the file.

REFERENCES

[1] Abu-Libdeh, L. Princehouse, and H. Weatherspoon, (2010) "RACS: A Case for Cloud Storage Diversity," Proc. ACM First ACM Symp. Cloud Computing (SoCC).

[2] Boldyreva, V. Goyal, and V. Kumar, (2008) "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS).

[3] Angelos D.Keromytis, Vishal Misra, Dan Rubenstein, (2002), "SOS:Secure Overlay Services", https://www.cs.columbia.edu/sos.pdf.

[4] Geambasu, T. Kohno, A. Levy, and H.M. Levy, (Aug. 2009) "Vanish: Increasing Data Privacy with Self-Destructing Data," Proc. 18th Conf. USENIX Security Symp.

[5] Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, (2008) "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. (SecureComm).

[6] Wolchok, O.S. Hofmann, N. Heninger, E.W. Felten, J.A. Halderman, C.J. Rossbach, B. Waters, and E. Witchel, (2010) "Defeating Vanish with Low-Cost Sybil Attacks against Large DHTs," Proc. 17th Network and Distributed System Security Symp. (NDSS).

[7] Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, (Apr. 2010) "A View of Cloud Computing." Comm. ACM, vol. 53, no. 4, pp. 50-58.

[8] Vrable, S. Savage, and G.M. Voelker, (2009) "Cumulus: Filesystem Backup to the Cloud," ACM Trans. Storage, vol. 5, no. 4, article 14, Dec.

[9] Stallings. Cryptography and Network Security. Prentice Hall, (2006).

[10] Perlman, "File System Design with Assured Delete, (2007)" Proc. Network and Distributed System Security Symp. ISOC (NDSS).

[11] Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman, (2010) "FADE: Secure Overlay Cloud Storage with File Assured Deletion," Proc. Sixth Int'l ICST Conf.Security and Privacy in Comm. Networks (SecureComm).

[12] Yang Tang, Patrick P.C .Lee, John C.S. Lui and Radia Perlman, (2012) "Secure Overlay Cloud Storage with Access Control and Assured Deletion" IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, November/December.

[13] Perlman, C. Kaufman, and R. Perlner, (2010) "Privacy-Preserving DRM," Proc. Ninth Symp. Identity and Trust on the Internet (IDTRUST).

[14] Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, (2003) "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.Second USENIX Conf. File and Storage Technologies.

[15] Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Lui, (2011) "A Secure Cloud Backup System with Assured Deletion and Version Control," Proc. Third Int'l Workshop Security in Cloud Computing.

[16] Kamara and K. Lauter, (2010) "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security.

[17] Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, Aug. 2008.

[18] Alan Cullen, Christopher Dearlove, "Secure Information Sharing using Attribute Based Encryption", BAE Systems (Operations) Limited, Advanced Technology Centre, Chelmsford CM2 8HN United Kingdom.

[19] Goyal, O. Pandey, A. Sahai, and B. Waters, (2006) "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS).

[20] Dathi Soniya.M, Roshni Thanka.M, (2013) "A Survey on Secure Overlay Techniques for Cloud Storage", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue.12, December.

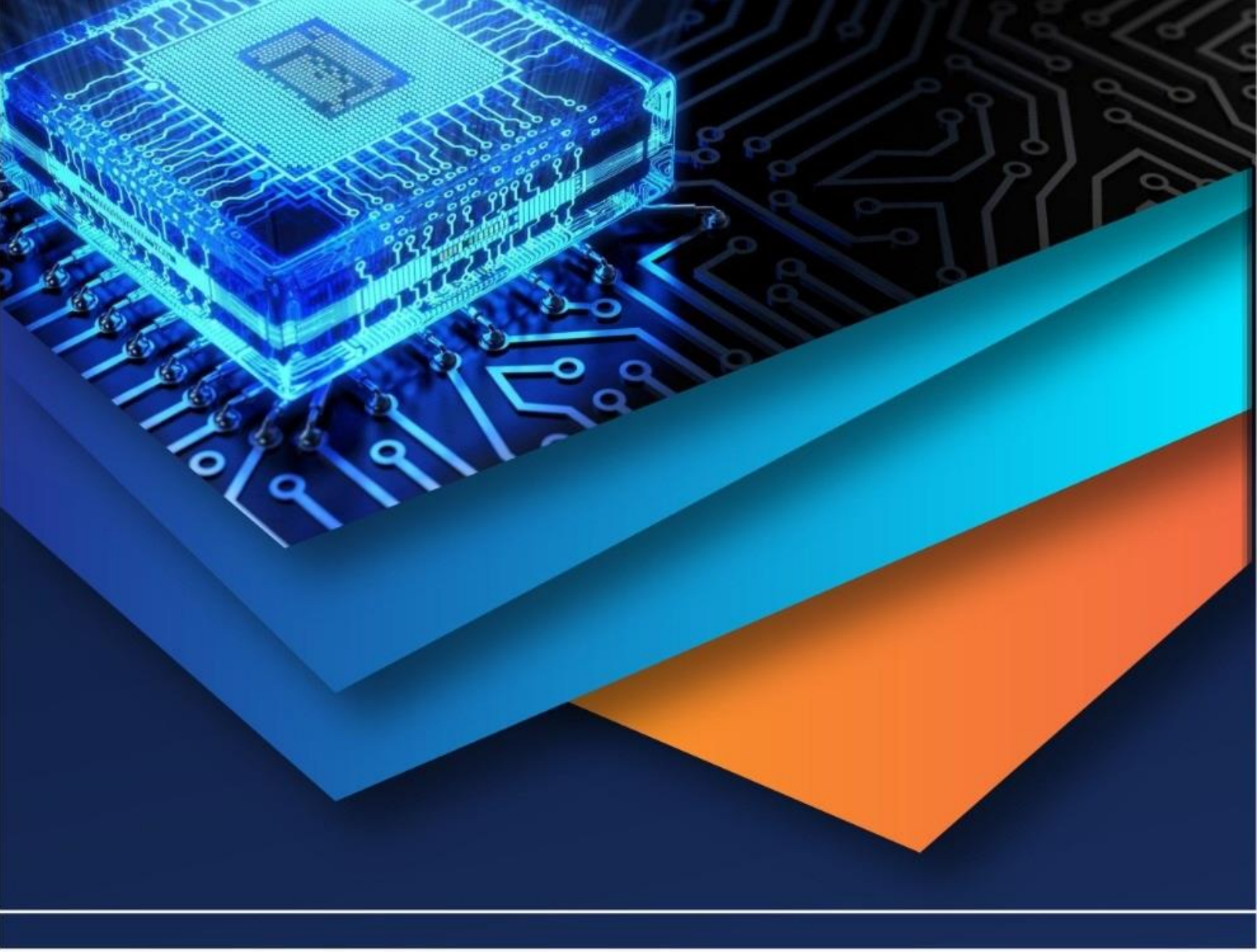
[21] Wang, Q. Wang, K. Ren, and W. Lou, (2010) "Privacy-preserving public auditing for storage security in cloud computing". In Proc. of IEEE INFOCOM, Mar.

[22] Yun, C. Shi, and Y. Kim, (2009) "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage". In ACM Cloud Computing Security Workshop (CCSW), Nov.

[23] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing. http://www.cloudsecurityalliance.org/, April 2009.

[24] Wang, Z. Li, R. Owens, and B. Bhargava, (Nov. 2009) "Secure and Efficient Access to Outsourced Data," Proc. ACM Workshop Cloud Computing Security (CCSW).

IJRASET : ISSN: 2321-9653



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)