iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 Issue: III Month of publication: March 2015

DOI:

Volume 3 Issue III, March 2015
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Secure and Adaptable Cloud Data Encryption System using cryptography: A Review

Anamika Sirohi
Department of Computer Science and Engineering, ARYA college of Engineering and IT, Jaipur, Rajasthan, India

Abstract: Security of data in cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. Cloud storage is an important part of cloud computing, which is used to achieve the target of storing data in the cloud. This paper proposes a highly active and efficient cloud security model. Our cloud security model plans to keep the most critical data security in cloud computing at different levels. The different levels are: user level, cloud service provider level, third party level and network intruder level. Data is protected against all level. To maintain data privacy re-encryption is performed with the help of third party and for data integrity Hash Based Message authentication code is generated on encrypted data. Also, the proposed model uses hash codes to tackle the issues regarding the integrity of the data at the public cloud. Proposed model is divided into two phases and consists of data owner, third party, cloud service provider and user. The phase's one is uploading or Data Storage and another one is Downloading or Data Retrieval.

Keywords: Cloud computing; Encryption; hash mac; public and private cloud, cryptographic process.

I. INTRODUCTION

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet. Cloud computing [1] is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing. Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers. In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide. It is an approach to maximize the capacity or step up capabilities vigorously without investing in new infrastructure, nurturing new personnel or licensing new software. It provides gigantic storage for data and faster computing to customers over the internet. It essentially shifts the database and application software to the large data centers i.e. cloud, where management of data and services may not be completely trustworthy. That is why companies are reluctant to deploy their business in the cloud even cloud computing offers a wide range of luxuries. It follows a utility based model in which the user pays as per resource utilization at the cloud. Makes it cheaper than the existing computing environments. The Cloud [2] can cater to end user with its unlimited and highly scalable pool of resources. These resources may be in the form of memory, processing time, processing power, application software, software development platforms, storage space etc. Cloud computing can effectively address the computing needs of users of versatile scales ranging from an individual to large organizations. It can cater to resource needs of all. One aspect of the cloud which prevents users from using cloud services is data security. There are user concerns about the security and privacy of data at the cloud. Cloud security is a multifaceted and highly complex issue. The data owners' especially large organizations fear possible data misuse by the cloud provider without their knowledge. This concern is a major deterrent in the path of shifting operations to the cloud. An effective security model addressing all these concerns is provided in this paper. This paper proposes a hybrid cloud computing model which effectively handles the issues related to cloud data security including confidentiality, integrity, authentication and authorization.

Cloud computing represents a distributing computing mechanism that by the utilize of the high speed network, data processing is moved from private PC or servers to the remote computer clusters (big data centers owned by the cloud service providers), any user has a potential super computer at hand and can access the data and get the computing capability at any time, from anywhere, you only need to pay for the resources which you have used, don't care about who provide the resources and in what way.

Actually, clouds [3] are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self-serviceabilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers must only pay for what they use and have not to pay for local resources which they need to such as storage or infrastructure. Nowadays, we have three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some r esources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud. In this type, cloud provider has a service that has private cloud part which only accessible by certified staff and protected by firewalls from outside accessing and a public cloud environment which external users can access to it. There are three major types of service in the cloud environment: SaaS, PaaS, and laaS. A cloud is a large group of interconnected computers that extends beyond a single company or enterprise. The applications and data served by the cloud are accessed via the Internet by a broad group of users across multiple enterprises and platforms. A cloud computing system consists of a collection of interconnected and virtualized computers dynamically provisioned as one or more unified computing resource(s) through negotiation of service-level agreements (SLAs) between providers and consumers. In cloud computing platforms, resources need to be dynamically re-configured and aggregated via virtualization and consumers' requirements can potentially vary over time and amendments need to be accommodated.

The cloud computing model revolves around three functional units or components as listed below:

A. *Cloud Service Provider*

It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients' data and high computation power.

B. *Client/Owner*

It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumer or organizations.

C. *User*

It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

Figure1: Cloud Architecture

II. HASH MESSAGE AUTHENTICATION CODE (HMAC)

Hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative FIPS-approved cryptographic hash function, in combination with a shared secret key.The cryptographic strength of HMAC depends on the properties of the underlying hash function. (MSE).

An HMAC function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input. The MAC is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender, and compares the result computed with the received MAC. If the two values match, the message has been correctly received, and the receiver is assured that the sender is a member of the community of users that share the key.

The HMAC [4] specification in this standard is a generalization of HMAC as specified in Internet RFC 2104, HMAC, Keyed-Hashing for Message Authentication, and ANSI X9.71, Keyed Hash Message Authentication Code.

HMAC shall be used in combination with a cryptographic hash function specified in a Federal Information Processing Standard (FIPS). HMAC uses a secret key for the calculation and verification of the MACs. The main goals behind the HMAC construction [RFC2104] are:

To use available hash functions without modifications; in particular, hash functions that perform well in software, and for which code is freely and widely available.

To preserve the original performance of the hash function without incurring a significant degradation.

To use and handle keys in a simple way.

To have a well-understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function, and

To allow for easy replace ability of the underlying hash function in the event that faster or more secure hash functions are later available.

A. HMAC Parameters and Symbols

H MAC uses the following parameters:
B-Block size (in bytes) of the input to the FIPS-approved hash function; e.g., for
SHA-1, B= 64.
H- FIPS-approved hash function, e.g., FIPS 180-1, Secure Hash Algorithm-1 (SHA-1).
Ipad- Inner pad; the byte x'36' repeated B times.
K- Secret key shared between the originator and the intended receiver(s).
K0-The key K with zeros appended to form a B byte key.
L- Block size (in bytes) of the output of the FIPS-approved hash function; for SHA-1,L= 20.
Opad- Outer pad; the byte x'5c' repeated B times.
T- The number of bytes of MAC.
Text- The data on which the HMAC is calculated; the length of the data is n bits, where the maximum value for n depends on the hash algorithm used.
X'N'-Hexadecimal notation, where each 'N' represents 4 binary bits.
||-Concatenation and
Exclusive-Or operation.

III. LITERATURE SURVEY

In this paper, I have made a review on my topic data security in cloud computing at different levels by reading different kinds of papers and analyzing different techniques which are being used in these papers published by authors which are discussed as follows:

Jing et.al [2] describes the security of data in cloud using hadoop framework. The proposed scheme focuses only on data encryption technique like DES or AES not on authorized user access. So, vulnerable to different attacks related to unauthorized access. Sood et.al [3] proposed approach to ensure data security in cloud computing. In this proposed approach key generation, encryption, indexing of data, user authentication and data integrity is performed by data owner itself. Unfortunately, there will be high overhead on data owner and hence time consuming too. Thilakanathan et.al [4] proposed scheme using proxy re-encryption for security of data. In this scheme data owner encrypt the data using his key piece then proxy encrypt the data using his key piece. Decryption is also carried in similar fashion. However, if proxy is fake then data becomes insecure. Sharma et.al.[5] discussed different service model of cloud computing and highlights the key security issues, challenges and solution at different layers of cloud. Jingwei et.al.[6] discussed efficient model for secure data sharing in cloud. The proposed model consists of user, authority, hybrid cloud and owner. The data is stored at private cloud and data shared is encrypted Encryption technology used is keyword-based encryption. The keys are generated by authority and given to user group for encryption and decryption. The model has some issues like if authority is fake then data is insecure and also it is costly to use the model. Sood et.al [7] proposed the scheme to highly secure the data at cloud. They provided improved data security by using concept of hybrid cloud. In this scheme the sensitive data i.e. about 3%-5% is stored at private cloud and rest of the data at public cloud. This model is applicable to organisations whose sensitive data is about 3%-5%. If the sensitive data increases then this model will prove to be expensive. The white papers[8] of many organisations describes three types of data security models in cloud. First model

Consists of key generation and encryption on data is performed by data owner itself. However this model results in high overhead for data owner. Second model describes encryption performed by data owner and key generation by cloud service provider. Unfortunately, cloud service provider is fake then data is insecure hands. Third model encryption and key generation is control by cloud service provider. If cloud service provider is fake then data is endangered. Hwang et.al [9] proposed business model in which encryption/decryption service and storage as a service of user data were separated i.e. they were not provided by single operator. After encryption/decryption performed system should delete all the data. Varalakshmi et.al[10] proposed system consists of three entities cloud broker, client and cloud storage. Broker handles encryption, hash key, decryption and local database management. According to cloud space available the client files are partitioned into segment and hash values of segments has been generated. When the client needs its file it sends request to broker then broker download the file, partition the file into segments and then calculate the hash values. For checking the data integrity hash values before uploading to the after downloading are matched. If this matches data is un-tampered. Mohamed et.al [11] performed randomness testing on various eight encryption technique namely RC4, RC6, MARS, AES, DES, 3DES, Two-Fish and Blowfish. Xu et.al [12] propose a dynamic user revocation and key refreshing scheme based on cipher policy attribute based encryption technique. In this technique user can be removed anytime without changing keys and also refresh keys without re-encrypting data. Huang et.al [13] proposed scheme that consists of four entities – SSManager, SSGuard, SSCoffer and user. SSGuard do encryption before uploading and uploaded files store at SSCoffer. File encryption key are encrypted by user public key and store at SSManger. For decryption of file QR code is used. User shows QR code to SSGuard to decrypt files. Sur et.al [14] proposed a model in which certificate based Proxy re-encryption scheme is followed before uploading data to cloud. Mowbray et.al [15] gives general overview of protecting data in cloud and describes various approaches to handle this protection. Some of these approaches are available for use now, others are relatively immature, but look promising. The most appropriate approach varies according to the type of data to be processed

Chandel et.al [16] presents a new scheme for secure cloud creation using RC6 (Rivest cipher 6) Encryption algorithm for securing the cloud environment. The results show the performance of proposed technique in public and private cloud. Fan et.al [17] describes Predicate encryption is a novel cryptographic primitive that provides fine-grained control over the accesses to encrypted data. It is often used in secure cloud storage and biometric matching. In this manuscript, we first propose a variant of symmetric predicate encryption, which provides controllable privacy preserving search functionalities, including revocable delegated search and un-decrypt able delegated search. Due to these functionalities, the owner of cloud storage can easily control the lifetimes and search privileges of cloud data. Hashizume et.al [18] describes the security risk associated with services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. It also discusses security issues as well as to identify and relate vulnerabilities and threats with possible solutions. Lenkala et.al [19] present a risk assessment framework to study the security risk of the cloud carrier between cloud users and two cloud providers. The risk assessment framework leverages the National Vulnerability Database (NVD) to examine the security vulnerabilities of operating systems of routers within the cloud carrier. This framework provides the quantifiable security metrics of each cloud carrier, which enables cloud users to select quality of security services among cloud providers. Such security metric information is very useful in the Service Level Agreement (SLA) negotiation between a cloud user and a cloud provider. It can be also used to build a tool for verifying the commitment of an SLA. Furthermore, implement this framework on Amazon Web Services and Windows Azure, respectively. Our experiments show that the security risks of cloud carriers on these two commercial clouds are significantly different. This finding provides guidance for a network provider to improve the security of cloud carriers. Dijk et.al [20] discusses lack of direct resource control in the cloud prompts concern about the potential for data privacy violations, particularly abuse or leakage of sensitive information by service providers. Cryptography is an oft-touted remedy. Among its most powerful primitives is fully homomorphic encryption (FHE), It argue that cryptography alone can’t enforce the privacy demanded by common cloud computing services, even with such powerful tools as FHE. It formally define a hierarchy of natural classes of private cloud applications, and show that no cryptographic protocol can implement those classes where data is shared among clients. It posit that users of cloud services will also need to rely on other forms of privacy enforcement, such as tamperproof hardware, distributed computing, and complex trust ecosystems. Kandukuri et.al [21] discusses cloud computing services and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no Control over it. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues.In cloud computing most prevailing issue is security due to which users fear to adopt cloud. Main concern is with uploaded data to cloud is secure or not. Keeping this concern model has been proposed which provide data security in cloud. It is highly efficient and secure model that can be used to upload data in cloud without fear. Another proposed model provides data protection at cloud and data security from internal as well as external threats. This model is organised in way that data remains private throughout transits and at rest.

IV. PROPOSED METHOD

The model is divided into two phases and consists of data owner, third party, cloud service provider and user. The phases are:

Phase I (Uploading or Data Storage)

Phase II (Downloading or Data Retrieval)

A. Phase I- Uploading

1) Key Generation and Distribution the: In this security model data owner generate Keys and divide the keys into key pieces. Owner keeps his piece with it for encryption. Distribute other piece of key to third party for re-encryption and also store key pieces for corresponding to user id for later use.

2) Re-Encryption and Indexing: For maintaining data privacy, data is encrypted and then uploaded to cloud. In this model owner perform encryption on data with its key piece and give encrypted data to third party. Thirdparty re-encrypt the data with its key piece and then upload to cloud. As it is very complicated to search on encrypted data so indexing of data has been made by owner. Indexing is way to retrieve data faster. As we do not want our data disclosure to cloud provider or network attacker or third party so index is encrypted by owner first with its key piece. Further pass to third party to re-encrypt it before uploading to cloud.

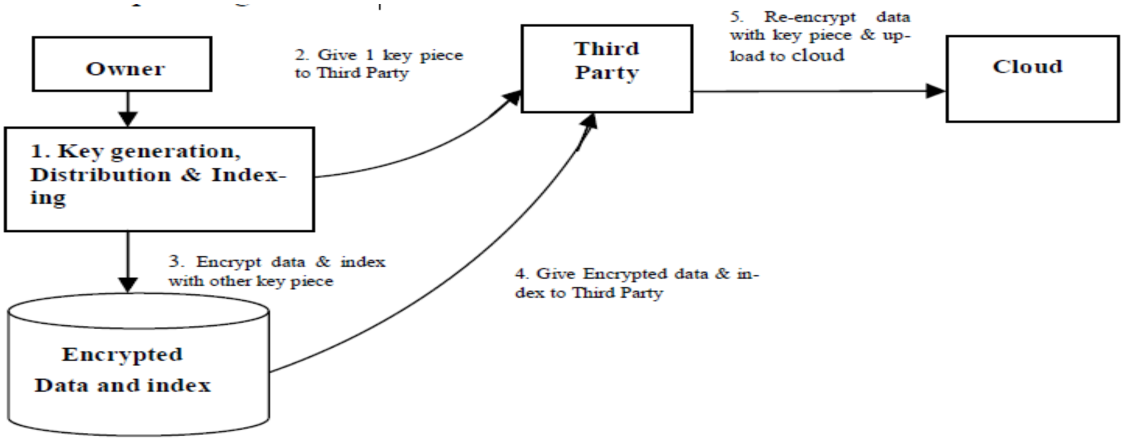

Owner
2. Give 1 key piece to Third Party
Third Party
5. Re-encrypt data with key piece & upload to cloud
Cloud
1. Key generation, Distribution & Indexing
3. Encrypt data & index with other key piece
4. Give Encrypted data & index to Third Party
Encrypted Data and index

Figure 2. Re-Encryption and Indexing

3) HMAC for Data Integrity

Although data is in encrypted format but there is fear of data being tampered during transit or on storage of data? To resolve this fear of data tampering hash-based message authentication code (HMAC) is calculated after data encryption. Basically, HMAC is process to use cryptographic hash function for message in the form of data authentication. It is encrypted by owner then re-encrypted by third party and uploaded along with data to cloud.

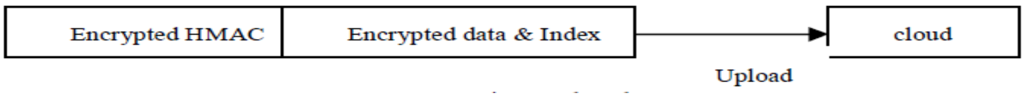


Figure 3. HMAC for Data Integrity

B. *HMAC Generation*

After decryption by third party, the data is still in encrypted format and passed to owner. Then data owner generate HMAC of data. If HMAC before uploading the data to cloud equals HMAC after downloading data then data integrity holds else data has been tampered by some intruder.

$$\text{HMAC(uploading)} = \text{HMAC(Downloading)} \longrightarrow \text{Data is un-tampered}$$

Figure 4. Data Integrity

V. CONCLUSION

The proposed technique provides a way to protect the data, check the integrity and authentication by different levels such as user level, cloud service provider level, third party level and network intruder level. In cloud computing most dominant issue is security due to which users fear to approve cloud. The main apprehension is with uploaded data to cloud is secure or not. Keeping this concern model has been proposed which provide data security in cloud. The proposed HMAC model gives outstanding results as compared to different types of cloud network models. It is highly efficient and secure model that can be used to upload data in cloud without fear. This model is suitable for various areas of secure cloud development such as public cloud, private cloud.

REFERENCES

[1] Mrinal RajkumarBuyya, Christian Vecchiola and S. ThamaraiSelvi, Mastering Cloud Computing Foundations and Applications Programming.Morgan Kaufmann, USA.

[2] Jing Huang Jing, LI Renfa, and TangZhuo, "*The Research of the Data Security for Cloud Disk Based on the Hadoop Framework*", IEEE,2013.

[3] Sandeep K. Sood, "*A Combined Approach to Ensure Data Security in Cloud Computing*", Submitted to Journal of Network and Computer Applications, Elsevier Ltd, 2012.

[4] Danan Thilakanatha, Shiping Chen,Surya Nepal, Rafael A. Calvo and Leila Alem, *"A platform for secure monitoring and sharing of generic health data in the Cloud"*, Elsevier Ltd, 2013.

[5] Pardeep Sharma, Sandeep K. Sood, Sumeet Kaur, "*Cloud Implementation Issues and What to Compute on Cloud*", International Journal of Advances in Computer Networks and its Security, vol.1, no. 1, pp. 130-135, 2011.

[6] Jingwei Li, Jin Li, Zheli Liu and Chunfu Jia "*Enabling efficient and secure data sharing in cloud computing*" Concurrency Computat.:Pract Exper.,John Wiley & Sons, Ltd.,2013.

[7] Sandeep K. Sood, "*A Highly Secure Hybrid Security model for Data Security at Cloud* ", Submitted to Security and Communication Networks, John Wiley and Sons (Interscience), Special Issue on Trust and Security in Cloud Computing, 2012.

[8] Amazon Web Services.: "*Encrypting Data at Rest in AWS*", https://aws.amazon.com/whitepapers.

[9] Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu, "*A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service*", National Science Council of Taiwan Government.

[10] P.Varalakshmi and Hamsavardhini Deventhiran, "*Integrity Checking for Cloud Environment Using Encryption Algorithm*", IEEE, 2012.

[11] Eman M.Mohamed and Sherif EI-Etriby, "*Randomness Testing of Modem Encryption Techniques in Cloud Environment*", 8th International Conference on Informatics and Systems, 2012.

[12] Zhiqian Xu and Keith M. Martin, "*Dynamic User Revocation and Key Refreshing for Attribute-Based Encryption in Cloud Storage*", International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[13]Kuan-Ying Huang, Guo-Heng Luo and Shyan-Ming Yuan, "*SSTreasury+: A Secure and Elastic Cloud Data Encryption System*", International Conference on Genetic and Evolutionary Computing, IEEE(2012).

[14] Chul Sur, Youngho Park, Sang Uk Shin, Changho Seo and Kyung Hyune Rhee, "Certificate-Based Proxy Re-Encryption for Public Cloud Storage", International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2013.

[15] NarendraChandel, Sanjay Mishra, Neetesh Gupta and AmitSinhal, "Creation of Secure Cloud Environment using RC6", IEEE,2013.

[16] Miranda Mowbray and Siani Pearson, "Protecting Personal Information in Cloud Computing", Springer Verlag, 2012

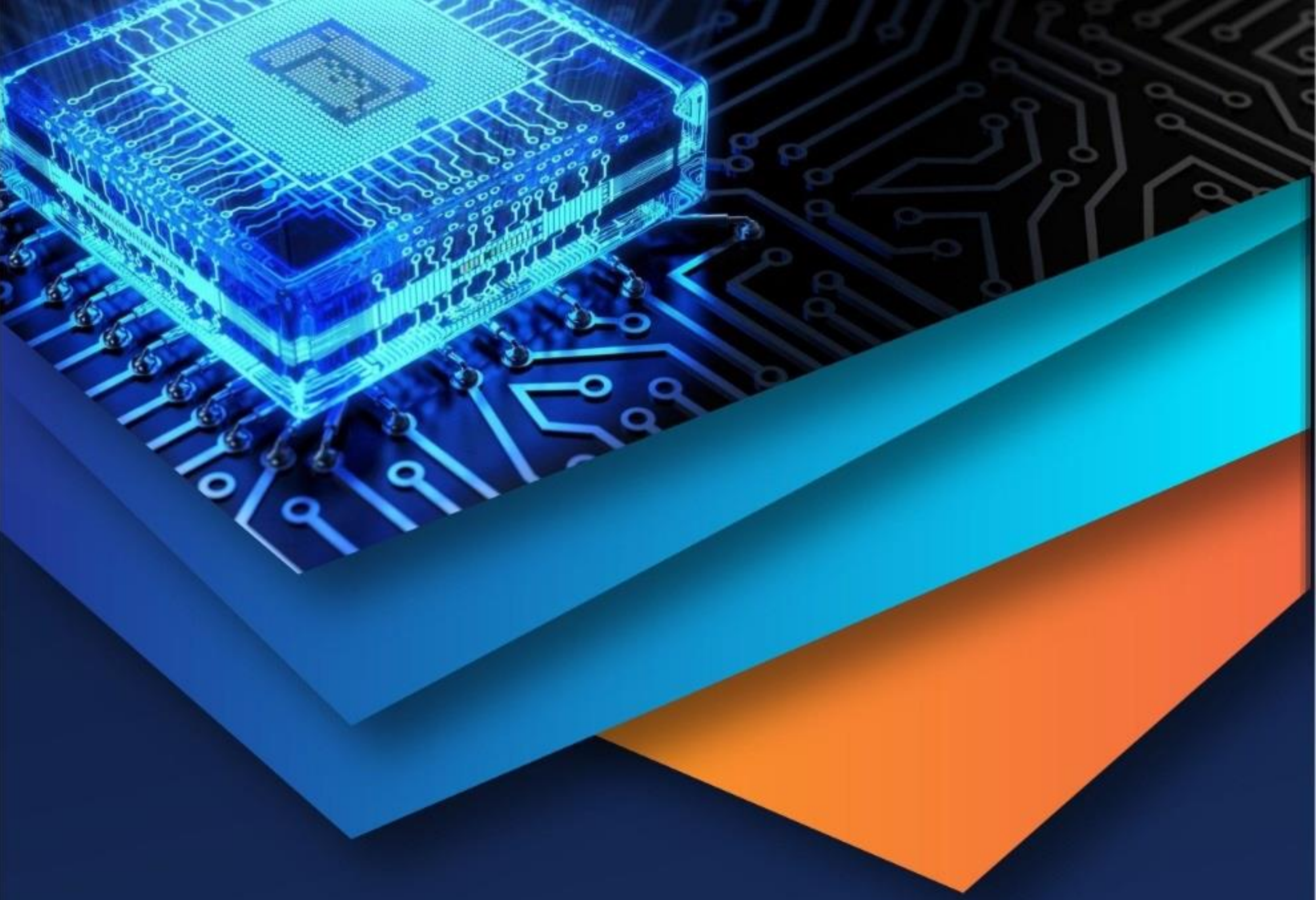
[17] Chun-I Fan and Shi-Yuan Huang, "Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage", International Conference on Cyber Enabled Distributed Computing and Knowledge Discovery, IEEE, 2011.

[18] Keiko Hashizume, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Springer,2013.

[19] Swetha Reddy Lenkala, KaiqiXiong and Sachin Shetty, "Security Risk Assessment of Cloud Carrier", IEEE,2013.

[20] Marten van Dijk and Ari Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", ACM,2010.

[21] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and AtanuRakshit, "Cloud Security Issues", IEEE 2009



crossref

10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY