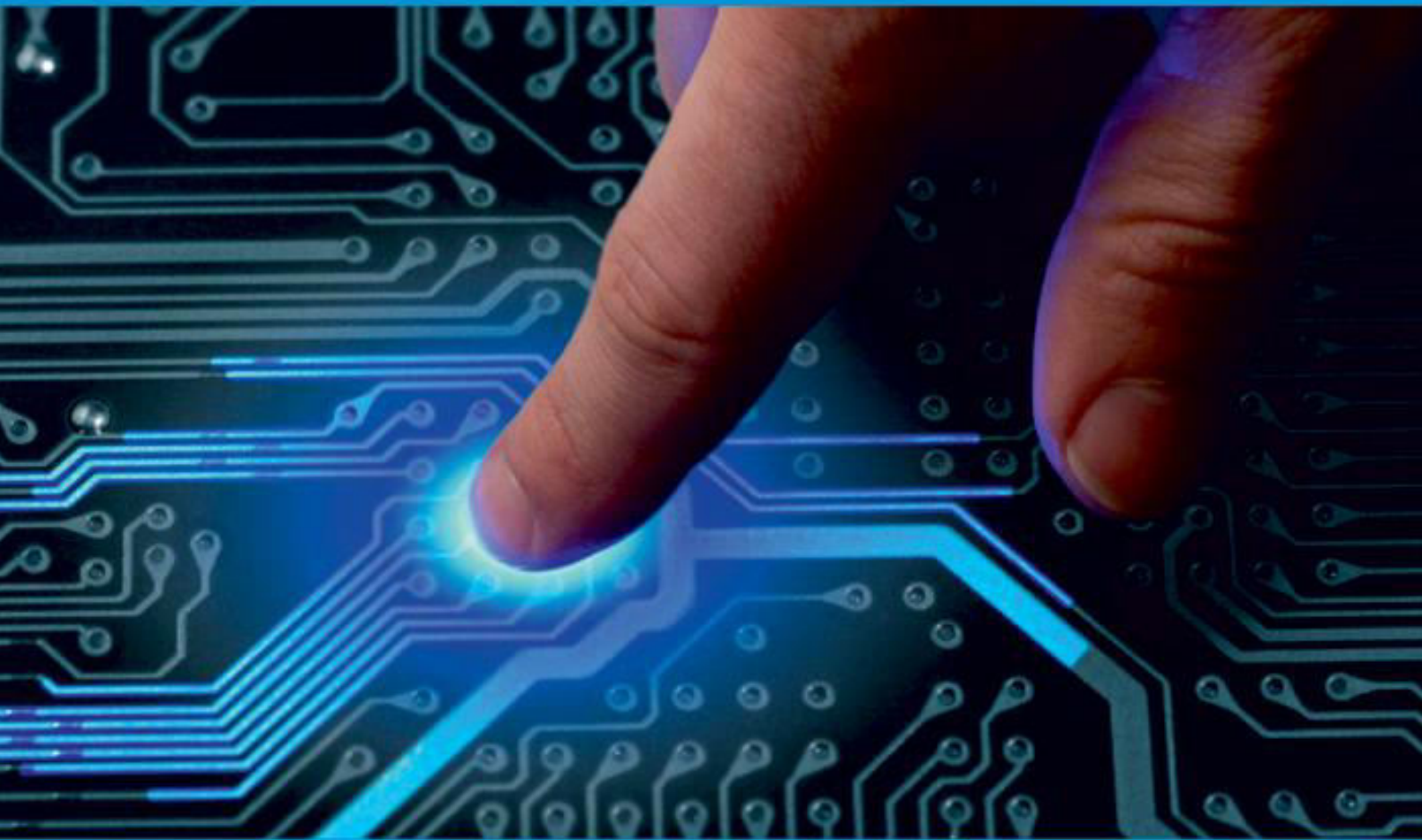




**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

**Volume 10, Issue 5, May 2022**

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.165**



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

# Multiple Key Security Scheme for Data Protection on Cloud Server

Mrs. B. ANANTHI<sup>1</sup>, M.BALAMANCHARI<sup>2</sup>, D.GAYATHRI<sup>3</sup>, S.KARUNYAA<sup>4</sup>, T.MAHESWARI<sup>5</sup>

<sup>1</sup> Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Engineering For Women(Autonomous), Tiruchengode, India

<sup>2,3,4,5</sup> UG Student, Department of Computer Science and Engineering, Vivekanandha College of Engineering For Women(Autonomous), Tiruchengode, India

**ABSTRACT:** Internet science is developing quickly, and human beings can process, store, or share with their information through the usage of its ability. Cloud shares infrastructure between quite a few businesses and it is managed internally or by means of a third-party. The consumer shops the information in an encrypted format. ABE is an encryption scheme used by way of the person to keep the facts in the cloud. ABE is a public-key primarily based one to many encryption methods which lets in customers to encrypt and decrypt records based totally on person attributes. Access manage of encrypted statistics saved in the cloud is, through the usage of get right of entry to polices and ascribed attributes related with non-public keys and cipher texts. In present ABE schemes decryption has high-priced paring operations and the complexity of the get entry to coverage is proportional to the wide variety of attributes. An ABE gadget with outsourced decryption eliminates the decryption overhead. Here consumer offers facts to the cloud provider provider, with a transformation key that permits the cloud to translate any ABE cipher textual content blissful with the user's attributes or get entry to coverage into a easy cipher text. In this project, use the protection mannequin of ABE with verifiable outsourced decryption through imparting the verification key at the time of output decryption. Then the use of consumer revocation scheme to overcome the key leakage problems. Multiple key protection scheme for facts safety on cloud server works in actual time cloud environments.

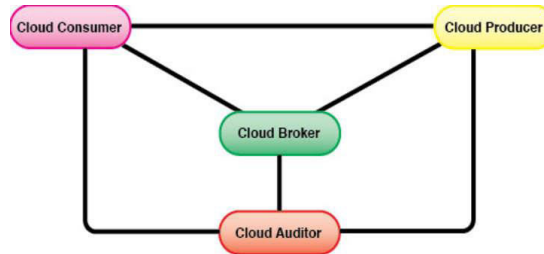
**KEYWORDS:** php, cloud computing.

## I.INTRODUCTION

### 1.1 Cloud Computing

Cloud computing is a computing paradigm, the place a massive pool of structures are related in personal or public networks, to grant dynamically scalable infrastructure for application, statistics and file storage. With the introduction of this technology, the value of computation, utility hosting, content material storage and transport is decreased significantly. Cloud computing is a realistic method to trip direct price advantages and it has the attainable to radically change a information core from a capital-intensive set up to a variable priced environment. cloud computing defined as: "A pool of abstracted, relatively scalable, and managed compute infrastructure succesful of internet hosting stop consumer purposes and billed with the aid of consumption." Cloud Computing is a technological know-how that makes use of the web and central far flung servers to keep information and applications. A easy instance of cloud computing is Yahoo email, Gmail, or Hotmail etc.

## 1.2 Cloud Computing architecture



### Cloud Provider:

A person, organization, or entity accountable for making a carrier reachable to involved parties. A Cloud Provider acquires and manages the computing infrastructure required for imparting the services, runs the cloud software program that affords the services, and makes association to supply the cloud offerings to the Cloud Consumers via community access

### Primary Cloud Provider:

A Primary Provider gives offerings hosted on infrastructure that it owns. It may also make these offerings accessible to Consumers thru a 1/3 celebration (such as a Broker or Intermediary Provider), however the defining attribute of a Primary Provider is that it does no longer supply its provider choices from different Providers.

### Cloud Consumer:

"A character or business enterprise that continues a enterprise relationship with, and makes use of provider from, Cloud Providers. A cloud patron browses the provider catalog from a cloud provider, requests the suitable service, units up provider contracts with the cloud provider, and makes use of the service. The cloud client can also be billed for the carrier provisioned, and desires to organize repayments accordingly."

What is no longer included here is the quit person that consumes the maybe enriched carrier supplied via the Cloud Consumer. In SaaS, the Cloud Consumer is frequently same with the give up user. However, in commercial enterprise environments this is no longer constantly the case. Using the instance of GMail, solely the paying entity is the Cloud Customer (e.g. IT department) whilst many different personnel can also use the mailing carrier as stop users.

### Cloud Auditor:

A celebration that can habits impartial evaluation of cloud services, records machine operations, overall performance and safety of the cloud implementation. A cloud auditor is a birthday celebration that can operate an impartial examination of cloud carrier controls with the intent to categorical an opinion thereon. Audits are carried out to affirm conformance to requirements via assessment of goal evidence. A cloud auditor can consider the offerings supplied by using a cloud issuer in phrases of safety controls, privateness impact, performance, etc.

### Cloud Broker:

"As cloud computing evolves, the integration of cloud offerings can be too complicated for cloud buyers to manage. A cloud client can also request cloud offerings from a cloud broker, as a substitute of contacting a cloud company directly. Hence the broking is an entity that manages the use, overall performance and transport of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers." Brokers furnish three distinctive sorts of services to the Cloud Consumer.

### Mediating Broker

A cloud broking enhances a given carrier by way of enhancing some precise functionality and imparting value-added offerings to cloud consumers. The enchancement can be managing get right of entry to to cloud services, identification management, overall performance reporting, more suitable security, etc.



### Aggregating Broker

A cloud broking combines and integrates more than one offerings into one or extra new services. The dealer offers information integration and ensures the invulnerable facts motion between the cloud patron and a couple of cloud providers.

### Arbitraging Broker

Service arbitrage is comparable to carrier aggregation barring that the offerings being aggregated are no longer fixed. Service arbitrage skill a dealer has the flexibility to select offerings from more than one agencies. The cloud broker, for example, can use a credit-scoring provider to measure and choose an organization with the satisfactory score.

### 1.3 SERVICE MODELS OF CLOUD

Cloud Providers provide offerings that can be grouped into three categories.

- Software as a Service (SaaS)
- Platform as a Service (Paas)
- Infrastructure as a Service (Iaas)

#### Software as a Service

In this model, a whole software is supplied to the customer, as a provider on demand. A single occasion of the carrier runs on the cloud & more than one give up customers are serviced. On the customers" side, there is no want for upfront funding in servers or software program licenses, whilst for the provider, the charges are lowered, given that solely a single utility desires to be hosted & maintained. Today SaaS is presented by means of businesses such as Google, Salesforce, Microsoft, Zoho, etc.

#### Platform as a Service

Here, a layer of software, or improvement surroundings is encapsulated & provided as a service, upon which different greater ranges of carrier can be built. The purchaser has the freedom to construct his very own applications, which run on the provider"s infrastructure. To meet manageability and scalability necessities of the applications, PaaS companies provide a predefined aggregate of OS and utility servers, such as LAMP platform (Linux, Apache, MySQL and PHP), constrained J2EE, Ruby etc. Google"s App Engine, Force.com, and many others are some of the famous PaaS examples.

#### Infrastructure as a Service

IaaS presents primary storage and computing competencies as standardized offerings over the network. Servers, storage systems, networking equipment, statistics centre area etc. are pooled and made on hand to deal with workloads. The purchaser would normally install his personal software program on the infrastructure. Some frequent examples are Amazon, GoGrid, three Tera, etc.

## II. OBJECTIVE

While the storage of company records on far off servers is now not a new development, modern-day enlargement of cloud computing justifies a greater cautious seem to be at its proper penalties involving privateness and confidentiality issues. As customers no longer bodily possess the storage of their data, regular cryptographic primitives for the reason of information safety safety can't be immediately adopted. In particular, really downloading all the statistics for its integrity verification is no longer a realistic answer due to the expensiveness in I/O and transmission value throughout the network. Besides, it is regularly inadequate to notice the information corruption solely when getting access to the data, as it does no longer provide customers correctness assurance for these un-accessed facts and would possibly be too late to get better the facts loss or damage. Considering the massive measurement of the outsourced information and the user's restrained aid capability, the duties of auditing the facts correctness in a cloud surroundings can be bold and pricey for the cloud users. Moreover, the overhead of the use of cloud storage must be minimized as a great deal as possible, such that person does no longer want to operate too many operations to use the statistics (in extra to retrieving the data). For example, it is appropriate that customers do no longer want to fear about the want to confirm the integrity of the facts earlier than or after the facts retrieval. Besides, there may additionally be greater than one person accesses the identical cloud storage, say in an

corporation setting. For less complicated management, it is suitable that the cloud server solely entertains verification request from a single distinct party. To absolutely make sure the information integrity and keep the cloud users' computation assets as properly as on line burden, it is of imperative significance to allow public auditing carrier for cloud statistics storage, so that customers might also lodge to an unbiased cloud storage server to audit the outsourced information when needed. The CSS, who has knowledge and skills that customers do not, can periodically test the integrity of all the information saved in the cloud on behalf of the users, which affords a a whole lot extra less difficult and low priced way for the customers to make certain their storage correctness in the cloud.

ABE additionally introduces the intermediate server recognised as the proxy server that performs a necessary position in decreasing the work load of the predominant server. The consumer as soon as he encrypts the file, the file will be saved in the server.

In a CP-ABE scheme, each and every cipher textual content is related with an get entry to coverage on attributes and each user's non-public key is related with a set of attributes.

### III. LITERATURE SURVEY

#### 3.1 Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, 2006

A an awful lot richer kind of attribute-based encryption cryptosystem and demonstrates its applications. In our machine every cipher text is labeled by means of the encryptor with a set of descriptive attributes. Each non-public key is related with an get right of entry to shape that specifies which kind of ciphertexts the key can decrypt. We name such a scheme a Key-Policy Attribute-Based Encryption (KPABE), seeing that the get admission to shape is exact in the personal key, whilst the ciphertexts are really labeled with a set of descriptive attributes and observe that this placing is reminiscent of secret sharing schemes.

#### 3.2 Cipher text-Policy Attribute-Based Encryption 2007

Provide the first building of a cipher text-policy attribute-based encryption (CP-ABE) to tackle this problem, and provide the first development of such a scheme. In our system, a user's non-public key will be related with an arbitrary wide variety of attributes expressed as strings. On the different hand, when a birthday party encrypts a message in system, they specify an related get admission to shape over attributes. A person will solely be in a position to decrypt a cipher textual content if that user's attributes bypass thru the cipher text's get right of entry to structure. At a mathematical level, get admission to constructions in our gadget are described by using a monotonic "access tree", the place nodes of the get entry to shape are composed of threshold gates and the leaves describe attributes.

#### 3.3 Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization 2011

A new methodology for realizing Ciphertext-Policy ABE structures from a typical set of get right of entry to constructions in the preferred mannequin below concrete and non-interactive assumptions. Both the ciphertext overhead and encryption time scale with  $O(n)$  the place  $n$  is the measurement of the formula. In addition, decryption time scales with the wide variety of nodes. The first device approves an encryption algorithm to specify an get entry to method in phrases of any get entry to formula. In reality our strategies are barely greater general. We specific get admission to manage with the aid of a Linear Secret Sharing Scheme (LSSS) matrix  $M$  over the attributes in the system. Previously used buildings such as formulation (equivalently tree structures) can be expressed succinctly in phrases of a LSSS. We do now not lose any effectivity through the use of the extra universal LSSS illustration as hostile to the until now used tree get entry to shape descriptions.

### IV. EXISTING SYSTEM

As a lot of touchy statistics is shared and maintain on with the aid of third-party web sites on the net, there'll be a wish to cipher records preserve on at these sites. One downside of encrypting data is that it will be by way of resolution shared fully at a coarse-grained stage (i.e., giving any other celebration your non-public key). And proposed a scheme for fine-grained sharing of encrypted facts that it has the tendency to developed Key-Policy Attribute-Based coding. In that, attributes and non-public keys are associated to get admission to constructions that manipulate the cipher texts that the person is geared up to rewrite. It did not disguise the set of attributes beneath that the facts is encrypted. Then proposed a cipher textual

content coverage attribute-based coding (CP-ABE), each and every secret key is related with a set of attributes, and every cipher textual content is related with get entry to shape on attributes. Secret writing is enabled if and solely if the user's attribute set satisfies the cipher textual content get right of entry to structure. This affords fine-grained get entry to administration on shared records in a number of smart settings, likewise as invulnerable databases and tightly closed multicast. It presents a variant with properly smaller cipher texts and quicker encryption/decryption operations. The most prepare is to shape a hierarchy of attributes, so fewer cluster aspects rectangular measure required to signify all attributes inside the system. This budget friendly variant is tested to be controller tightly closed and additionally proposed the first attribute-based encryption (ABE) schemes permitting for really expressive get admission to buildings and with steady cipher textual content size.

#### 4.1 DISADVANTAGES

- ABE schemes are that decryption is high-priced for resource-limited units due to pairing operations.
- The ABE cloud no longer secures.
- ABE gadget with outsourced decryption eliminates the decryption overhead

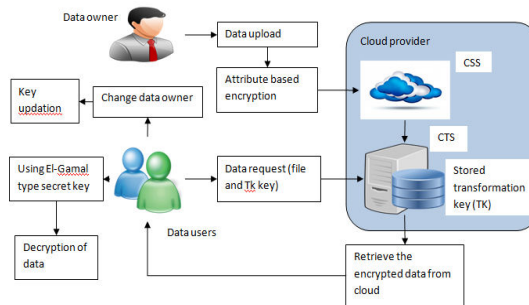
### V.PROPOSED SYSTEM

The verifiability of the cloud's transformation and a approach to confirm the correctness of the transformation is provided. Initially it modifies the authentic mannequin of ABE with outsourced decryption then the current to allow for verifiability of the transformations. Once describing the formal definition of verifiability, we have a tendency to endorse a new ABE mannequin and supported this new mannequin assemble a concrete ABE theme with verifiable outsourced decryption. Abe scheme with verifiable outsourced decryption and recoverability consists of seven algorithms specifically Setup, KeyGen, Encrypt, Decrypt, GenTkOut , Transformout, and Decrypt Out. A relied on Party makes use of the SetUp algorithmic rule to come up with the usual public parameters and a grasp secret key, and makes use of KeyGenOut to come up with a private key. Encrypt algorithmic rule makes use of the universal public parameters and get entry to shape to cipher the message. In Outsourced Decryption the person makes use of the GenTkOut algorithmic rule to come up with the transformation key and the retrieving key. The person sends the transformation key to the cloud. Taking as enter the transformation key given by means of a consumer and a cipher text, the cloud will use the algorithmic rule Transformout to transform the cipher textual content into a easy ciphertext. If the user's attribute satisfies the get right of entry to shape associated to the cipher text; then the person makes use of the DecryptOut algorithmic rule to get better the plaintext from the converted cipher text. It takes enter as cipher text, public parameters and consequently the changed cipher text. The hashed blocks of authentic message are in contrast with the hashed blocks of retrieved message; if any exchange inside the block then we can affirm that the closing blocks are original. User splits the unique message in to constant measurement blocks, and for every block sha1 algorithm is applied. The resultant random hashed blocks can be saved in the consumer side. After retrieving the facts from the cloud the verification operation is performed. If the verification consequences the statistics is modified then to perceive the modified block and get better the closing content material Random hash feature is utilized to the retrieved data.

#### Advantages:

- The cloud impervious machine for the double secret.
- The scheme notably decreased the computation time required for resource-limited gadgets to get better plaintexts.

**VI.SYSTEM ARCHITECTURE**



**6.2 MODULES**

**Modules:**

- 6.2.1 Cloud Entities
- 6.2.2 Access manipulate mechanism
- 6.2.3 Security Model
- 6.2.4 Secure records Sharing
- 6.2.5 Key revocation
- 6.2.6 Evaluation criteria

**Modules description:**

**6.2.1 Cloud Entities:**

Cloud computing is computing in which giant organizations of far off servers are networked to enable the centralized statistics storage, and on line get right of entry to to pc offerings or resources. Clouds can be categorised as public, personal or hybrid. Cloud computing, or in less complicated shorthand simply "the cloud", additionally focuses on maximizing the effectiveness of the shared resources. Cloud assets are generally now not solely shared by means of more than one customers however are additionally dynamically reallocated per demand. This can work for allocating sources to users. The device mannequin consists of three sorts of entities: the cloud server (server), the statistics proprietors (owners) and the statistics buyers (users).

Cloud server is accountable for save the records in cloud storage. It consists of two sub servers such as Cipher textual content transformation server (CTS), Cloud storage server (CSS)

**6.2.2 Access Control Mechanism:**

Access manipulate is usually a coverage or process that allows, denies or restricts get right of entry to to a system. It may, as well, screen and document all tries made to get admission to a system. Access Control may additionally additionally discover customers trying to get right of entry to a device unauthorized. It is a mechanism which is very a lot essential for safety in laptop security. Various get admission to manage fashions are in use, which includes the most frequent Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these fashions are acknowledged as identification based totally get entry to manage models. In all these get admission to manipulate models, person (subjects) and assets (objects) are recognized with the aid of special names. Identification may also be Data proprietor ne at once or thru roles assigned to the subjects. These get admission to manage techniques are positive in unchangeable disbursed system, the place there are solely a set of Users with a acknowledged set of services. The cloud server is accountable for the distribution of international secret key and world public key for every criminal person in the system. Cloud storage server cut up into two server such as cloud storage server, cipher textual content transformation server. However, the cloud server is no longer worried in any attribute administration and the advent of secret keys that is related with attributes. CTS is divide secret key into transformation key (denoted by way of tk) and El Gamal-type secret key (denoted with the aid of DK). DK is stored secret in person side. Tk is maintained in CTS and transferred from person to CTS server.



### 6.2.3 Security Model:

The cloud server shops the owners' information and affords records get right of entry to provider to users. It generates the decryption token of a cipher textual content for the consumer by way of the use of the secret keys of the person issued through the CTS. User Revocation starts offevolved with the instinct of the consumer revocation operation as follows. Whenever there is a consumer to be revoked, the statistics proprietor first determines a minimal set of attributes besides which the leaving user's get entry to shape will in no way be satisfied.

Data encryption as

It divides the facts into countless records aspects as  $m=m_1, \dots, m_n$

It encrypts information elements with unique content material Keys  $k=k_1, \dots, k_n$  with the aid of the use of symmetric encryption methods.

It then defines an get entry to shape  $M_i$  for every content material key  $k_i$  and encrypts it via strolling the encryption algorithm Encrypt.

### 6.2.4 Secure Data sharing:

Each person is assigned with CTS. Each consumer can freely get the cipher texts from the server in tightly closed manner. To decrypt a cipher text, every person may additionally publish their secret key TK issued by using some CTS collectively and saved the key DK in person facet and ask it collectively at the time of decryption token for some cipher text. Upon receiving the decryption token, the consumer can decrypt the cipher textual content via the use of its DK. Only when the user's attributes fulfill the get entry to coverage described in the cipher text, the server can generate the right decryption token. The secret keys and the world user's public key can be saved on the server; subsequently, the consumer Data proprietor now not want to post any secret keys if no secret keys are up to date for the in addition decryption token generation. It objectives to permit the customers with eligible attributes to decrypt the complete information saved in the cloud server. However it can't restrict the customers from getting access to the data's which are now not available to them. That is it can't restrict the records get admission to manipulate to the approved users.

Data sharing as:

Decrypt algorithm makes use of the public parameters, modified cipher text, and cipher text for verification.  $PK = (G, G_T, e, g, u, v, d, g^a, e(g, g)^\alpha, T_i = g^{s_i} = g \forall i, H)$

$$CT = ((A, \rho), \hat{c}, c^{\wedge}, C_1, C_1^{\wedge}, C(1, i), D(1, i), C_2, C_2^{\wedge}, C(2, i), D(2, i), i)$$

$$CT' = (T=C, T_1=C_1, T_1^{\wedge}, T_2^{\wedge}=C_2, T_2')$$

$$RKs = z$$

### 6.2.5 Key Revocation:

In this module, overcome the key revocation trouble at the time of consumer revoked from group. The team key is generated for every consumer based totally on facts owner. If the consumer trade the information owner means, crew key is robotically updated. And key up to date file is ship to all current customers in crew and also overcome the key leakage problem.

### 6.2.6 Evaluation criteria:

In this module we can consider the overall performance of the machine the use of the overall performance metrics such as storage overhead, conversation price and computation efficiency. The storage overhead is one of the most massive troubles of the get admission to manage scheme in cloud storage systems. In our scheme, except the storage of attributes, CTS additionally wishes to shop a public key and a secret key for every consumer in the system. Thus, the storage overhead on CTS in our scheme is additionally linear to the quantity of in the system. The conversation price of the everyday get admission to manage is nearly the same. The verbal exchange value of attribute revocation is linear to the quantity of cipher texts which comprise the revoked attribute. We examine the computation effectivity of each encryption and decryption in two criteria: the variety of authorities and the wide variety of attributes per authority.



VII. RESULTS



Cloud User

Home | New User

**New User**

Name

Contact No.

E-mail

Username

Password

Confirm Password

Cloud User

Cloud User

Home | Request | Logout

**Search Cloud Data**

Site

Sno	Data Owner	Data	Action
1	divesh	data	<a href="#">Send Request</a>
2	divesh	data	<a href="#">Send Request</a>

Cloud User



Cloud

Sno	Data Owner	User	Request File	Txkey	Date	Verification
1	divesh	raj	3000.jpg	rajf3000	13-11-2015	Check

## VIII.CONCLUSION

A novel framework of accomplishing grain get admission to manage for sharing non-public data. Considering in part honest cloud servers, it argues that to absolutely understand the concept, sufferers shall have entire manage of their personal privateness thru encrypting their archives to permit fine-grained access. The framework addresses the special challenges delivered via a couple of statistics proprietors and users, in that considerably limit the complexity of key administration whilst decorate the privateness ensures in contrast with preceding works. It makes use of ABE to encrypt the cloud data, so that consumer can permit get right of entry to no longer solely by means of non-public users, however additionally a number of customers from public Data proprietor mains with one-of-a-kind expert roles, qualifications, and affiliations. We viewed a new requirement of ABE with outsourced decryption: Verifiability. It is used to adjust the authentic mannequin of ABE with outsourced Decryption. This ABE scheme with Verifiable outsourced decryption and proved that it is invulnerable and verifiable .Multiple key protection scheme does no longer remember on random oracles. A bendy get entry to manage for encrypted statistics saved in cloud is provided. It eliminates Decryption overhead for customers in accordance to attributes .This Data transformation is assured to shop in cloud. This impervious attribute primarily based cryptographic method for sturdy records protection that's being shared in the cloud.

## IX.FUTURE ENHANCEMENT

In future, we can prolong ABE to enforce quite a number algorithms to supply elevated protection in cloud environments and additionally analyze the quite a number attributes to encrypt the data.

## REFERENCES

- [1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology (Lecture Notes in Computer Science)*, vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
- [2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.
- [3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.
- [4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography (Lecture Notes in Computer Science)*, vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.
- [5] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2013, pp. 463–474.
- [6] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2007, pp. 456–465.
- [7] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theoretical Comput. Sci.*, vol. 422, pp. 15–38, Mar. 2012.
- [8] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. 20th USENIX Secur. Symp.*, 2011, p. 34.
- [9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
- [10] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Advances in Cryptology (Lecture Notes in Computer Science)*, vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 465–482.



**INNO**  **SPACE**  
SJIF Scientific Journal Impact Factor

**Impact Factor: 8.165**

**doi**<sup>®</sup>  
**cross** **ref**

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 **9940 572 462**  **6381 907 438**  **ijircce@gmail.com**



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details