Some Investigation on Attribute-Based Encryption (ABE) Techniques for Semi-Trusted Cloud Service Providers

R.Rajan,

Ph.D Research Scholar of SCSVMV University, Department of Information Technology Enathur, Kanchipuram, E-Mail: rajanrajavelu@gmail.com

Dr.G.Murugaboopathi,

Associate Professor Department of CSE, Kalasalingam University, Anand Nagar, Krishnankoil, Srivilliputtur (TK), Virudhunagar District, Tamilnadu, India Murugaboopathy, Email: gmurugaboopathi@gmail.com

Dr. N. Sankar Ram,

Professor and HOD of CSE, Rajalakshmi Engineering College, Thandalam, Chennai Email: nsankarram@gmail.com

Abstract

The association between data storage and web application suppliers can safeguard clients from securing their information and applications in a single cloud supplier in cloud computing. Currently, online access control measures can be applied just when information proprietors and cloud specialist organizations in space are equivalent to confide. Deplorably, this condition cannot be met in untrusted mists, where cloud suppliers may get to delicate data without approval. The more significant part of the prior examinations need end-client endorsements or unequivocal APIs and leave from current benchmarks. In this paper, we propose another approval plot (AAuth) for this sort of semi-believed cloud structure that expands on the OAuth standard by utilizing figure content strategy trait-based encryption and an ElGamal-like spread over the HTTP convention. This course of action gives encryption all through and tokens dependent on ABE to permit approval by the two specialists and proprietors and to move approach requirement from mists to goals. By client driven methodology, proprietors would have the option to control their information when it rests in semi untrusted distributed storage. The proprietors to specialists assigned a large portion of the cryptographic capacities, proprietors, can pick up calculation power from mists. Security examination shows that our framework continues the comparable security level as the first encryption conspire and shields clients from presenting their qualification to application suppliers. In our broad re-enactment, the more noteworthy overhead of AAuth's offset. Likewise, our framework works faultlessly with capacity suppliers by holding the suppliers' APIs in the standard way.

Keywords: *Attribute-Based Encryption, Cloud Computing, Semi-Trusted Cloud Service, New Authorization Scheme, Original Encryption Scheme*

1. INTRODUCTION

Cloud computing has become the most desired technology in today's world. With its many advantages like flexibility, virtual characteristic, storage space, accessibility and convenience in the accessibility of data, it has drawn the attention of internet users. With its widespread usage, the cloud has also attracted industries and companies to transform themselves onto the cloud platform.

One can avoid the problem of data management and maintenance while storing data in cloud servers. Due to its various applications in several fields, many researchers find it as a promising research field. One of the essential and noted cloud storage technology is online data. They were storing and sharing data on social networks online. Storing online health record data has become convenient with cloud servers. Data owners prefer to store their data on a cloud server and reduce physical components, time and money involved in storing data.

But this data can be made accessible to all users in the absence of protection mechanism. Hence it is highly essential to have the security factor present in the cloud service provider (CSP). Storing and securing data is the primary challenge in cloud computing.

Attribute-Based Encryption (ABE) algorithm is an efficient way of protecting data in cloud computing. In ABE, encryption technique secured data by using where the secret key for the same has utilized. In this method, the DO or the data owner would define the accessible structure, and the receiver can decrypt the data only if the attribute set matches with that of the access structure over the cypher text.

An encryption technology known as Cipher text-policy attribute-based encryption (CP-ABE) scheme provides the solution for most of the challenging problem. In this case, shared data files commonly called a multilevel hierarchy which has inherent characteristics, especially in military and healthcare. There has been no extensive discussion on the shared files having a hierarchy structure in Ciphertext Policy.

Attribute-Based Encryption. This paper proposes an encryption scheme which is attribute-based with efficient file hierarchy in cloud computing. A single access structure can be used basically to Layer access structures. Encryption operation is done subsequently on hierarchical files with the integrated access structure. Next forthcoming operation is the cypher text components sharing the files that are related to attributes. Therefore, it saved both storage operations on cypher text and cost factor related to time. Furthermore, the proposed system is entirely secure with proper solution and proved under the standard assumption. Also, in terms of encryption and decryption, it is very competent for the experimental simulation.

Cloud computing is changing into a great deal of transcendent thus, a ton of and a ton of touchy information is being brought together into the cloud for sharing, that delivers new difficulties for re-appropriated information security and privacy. Attribute-based encryption (ABE) could be a competitor to style fine-grained get to the framework as of late by the cryptologic approach that was broadly applied. ABE is being stigmatized for its high subject overhead because the procedure esteem develops with the multifaceted nature of the entrance equation. This deficiency turns out to be progressively pervasive in cell phones since they have obliged registering assets.

2. LITERATURE SURVEY

Cloud has become a leading technology due to its flexibility and storage capacity. Many companies are fascinated by this technology to change themselves into a cloud platform because it reduces time and money. Cloud computing provides various solutions for storage and computation services for large and small industries. The attribute-based encryption algorithm is an efficient way of protecting data in cloud computing. This technology must be used by our resources appropriately. Otherwise, it leads to high expenses [1].

Securing data in cloud computing is an essential factor because anytime the data in software hacking is possible. The biggest challenge is to protect this data from external users and hackers. A security protocol in the cloud is enhanced through various cryptographic algorithms to keep the information confidential. Crypto cloud service is a new technology which protects information integrity along with data sharing [2].

Cloud technology is adopted by many medical organizations to keep their patient’s electronic health records safely. It utilizes based encryption to encode the patients' records. This instrument moves the administration the board overhead from the patient to the clinical association and sends cloud-based; for the most part, HER administrations to the clinical providers [3]. Cypher content arrangement property based encryption is another plan proposed by distributed computing in which detailed data side from being uncovered on untrusted cloud servers has kept by the customer. It gives information to just approved clients. Deduplication could be a unique information compression technique to get rid of supernumerary copies of recurrent information and might be accustomed expertly cut back information cupboard space and communication overhead [4].

The appearance of distributed computing to send strategic application has expanded the estimation of a cloud. Then again, cloud security is confronting a few dangers from various assets. Security features like access control, a digital signature is forced inside a cloud environment to store cloud data. Attribute-based encryption is the best tool for accessing information in cloud computing. The main advantage of it is its vital strength which helps users to have secure encryption [5].

An efficient system verifies the data in cloud computing. Attribute-based encryption scheme supports a single keyword search. It also supports a multi-keyword searchable encryption scheme which avoids unsuitable documents and by reducing the search scope. It can actualize property disavowal adequately by giving figure content updates to the incredible cloud server. It forestalls access by unlawful clients [6]. Attribute-based information sharing plan is a dependable innovation for cloud environments. It gives information get to control, information secrecy and information validation. This plan can oppose plot assault and replay assault. It partitions the clients as per their gatherings, and it would improve productivity and security of the information sharing [7].

To save messages from being read by outsiders, we need a security system. Attributed based encryption provides security to messages in different manners, depending on the characteristics of messages. This policy helps users to encrypt the data using keywords and decrypt the data using the same keywords. This policy can be improved in the future for more than one user with their key generation to provide security in terms of keys as well as messages [8].

New technology in cloud computing is class-based multi-storage encryption which solves issues in data security. It divides data into several classes, and different classes at different levels used different encryption schemes. It uses different keys for encryption and decryption. This algorithm improves the performance of security and data security [9]. To save personal health records of patients from being exposed to other servers, Attribute-based encryption had used. It keeps the data confidential. ABE maintains a high level of privacy. ABE helps see the data by not only patients but also other personal users with different professional roles, qualifications and affiliations [10].

For resource-restricted mobile users, A new attribute-based knowledge sharing theme had fancied in cloud computing. This topic expels a large portion of the calculation task by including framework open parameters. Its original design is to oversee calculation strength and powerless information security issues in cloud information sharing. It may disconnect cryptography modes and licenses anybody to imagine the legitimacy figure, messages before exorbitant [11]. In versatile distributed computing by presenting a cloud-based semi confided in power between portable clients and credit authorities, Multi authority trait-based encryption conspire is utilized. To scramble and unscramble a message by just client it was utilized. This plan ensures the security of encoded message and protection of versatile client [12].

Capacity based cryptographic information get to control is another strategy which guarantees just substantial clients to have re-appropriated information. Information security and access control are the most testing things in distributed computing. This plan secures redistributed information and its profoundly productive and safe under existing security models [13]. They utilize high applications to store information in the cloud. Another plan called "cloud information stockpiling administration "was invented.it helps spare information proprietors' calculation asset as well as gives a reasonable practical strategy for information proprietors to pick up trust in the cloud [14].

For information privacy and smooth access control in a distributed computing condition, A new scheme proposed called attribute-based proxy encryption and re-encryption. In any case, a plot assault of denied client and cloud server can disregard information secrecy. Secrecy is ensured by putting away and separating information documents into headers and body [15].

Identity-based encryption is a new scheme in which cloud computing is used. The sender using IBE directly decodes message with the receiver's identity. It focuses mainly on the issues of identity revocation [16]. Vehicular cloud computing is a new technology in cloud computing for vehicle drivers. Protecting data is an essential issue in VCC. It is a cryptography-based system that conducts smoother get to control. Security insurance in our plan spares information privacy, yet additionally, other security dangers in the new assistance model [17].

To check the respectability of the information, a plan called "Auditing Mechanism" is presented. The clients can have a productive and tie-down procedure to review their re-appropriated information. This system decreases computational and correspondence cost. It likewise ensures producing and substitution assaults without imperilling the secrecy of the put-away information [18].

3. SYSTEM MODEL

To forestall unapproved get to, a proprietor scrambles the information with an entrance arrangement characterized over open essential parts, at that point stores it in a server. On the off chance that the client wishes to utilize information, it demands a proprietor and specialists together to give an ABE-token. In this way, exclusively clients World Wellbeing Association fulfil the arrangement would translate the data document. We tend to accept that ceaselessly clients' declarations, the validation frameworks, e.g., client secret word databases, Dynamic Index/LDAP, are accessible for authorizers to confirm proprietors. In the meantime, all specialist organizations, i.e., authorizers, specialists, customers, and servers, register for open key endorsements from Testament Specialists (CA) to help SSL/TLS security channels.

Our semi-believed condition implies that albeit no element confides in the others, everybody confides in the convention. However, the singular substance may attempt a few dangers to assault the framework.

1. Let us acknowledge that the servers are trusted to give information benefits accurately, yet might be interested in delicate data and inclined to uncover information to ineligible gatherings.

2. The authority could deny proprietors' requests to give tokens or issue personal tokens to its plotters.

3. Consumers may endeavour to get unapproved documents from legitimate servers by creating tokens to get unapproved get to or resubmitting past tokens (replay assaults).

4. Deprived of client open key authentications, proprietors may propose tokens for the benefit of others.

5. Internet clients could dispatch the general system assaults on encoded data or tokens. Nonetheless, we tend to accept that the interchanges among CSPs territory unit secure and credible beneath SSL/TLS secure channels. Adversaries have just less registering capacity to break cryptographic natives. Light of the above examination, we next disclose how to build our plan and how to control the conventions.

3.1 Definitions and Notations

Building AAuth requires five principal parts: qualities, get to approaches, get to trees, meta-information, a changed CP-ABE plan and file documents as follows.

Traits AAuth parts the characteristic universe into two separate sets: limited and illustrative. The bound traits are obligatory and given by an authorizer in the interest of proprietors. Token limitations characterize the language structure, and semantics of kept ascribes and saved to separate them from illustrative characteristics, characterized beneath. Thus, an authorizer distributes the sentence structure as (trait) = (esteem), and the semantics are as per the following:

Record LOC = URI: a document identifier containing URL/total way/filename;

Proprietor = ownerId: the identifier of a record proprietor;

PERMIS = hr|wi: record authorizations, where 'r' perused just and 'w' is composed;

SEC-CLASS = h1 − 5i: a security class of a record, characterized in the climbing request;

TIMESLOT = yyyy/mm/dd/hh/nn: the digits of the year, month, date, hour, and moment in the timeslot.

Since our ABE-tokens are a lot of private keys, instead of issue a token for each document, different properties partake in like manner. It is increasingly adaptable and effective to give a token for different records or availabilities. Moreover, the granularity of availability and the fine-grained segments with * in a climbing request is balanced. Notwithstanding, every token of a similar document must have a similar granularity level. For barely any distributed storage, Document LOC qualities are not natural areas, for example, protests in a pail of Amazon S3. Then again, expressive qualities, which depict purchaser attributes, are characterized by authority(s) who screen and control the customer. We characterize the sentence structure of illustrative qualities as (attribute)@(rl)= (esteem), where (rl) is a URL of the power giving the property. Yet, specialists effectively depict the semantics of traits under their influence, at that point distribute in any open server.

3.2 Defined Policy to access the file

To encode ensured information with t to approaches, we initially characterize the strategy in a Boolean arithmetical articulation that consolidates bound and graphic traits together at the root hub. Subsequently, the polynomial math is built by ANDing each limited quality term and the entire arrangement of clear trait terms as follows:

Approach A = [FILE-LOC] AND [OWNER] AND [SEC-CLASS] AND [PERMIS] AND [TIMESLOT] AND [(OWNER@AUTHOR) OR (Elucidating Boolean algebra)].

To disregard the descriptive term when a proprietor gets to his information, a unique characteristic 'OWNER@AUTHOR' would be OR with the unmistakable term. Consequently, a proprietor must demand 'OWNER@AUTHOR' from an authorizer when the proprietor needs a token that doesn't rely upon distinct qualities.

3.3 Tree Structure of Access permission,

we can construct an entrance tree as per a monotonic access approach as in the accompanying calculation.

1. To make a tR-degree polynomial qR(·), staring with the root hub, a calculation sets the point at zero qR(0) = s for a mystery esteems ∈Zpand arbitrarily picks other (tR − 1) focuses.

2. For different hubs x, the calculation sets qx(0) = qparent(x)(index(x)) and arbitrarily picks other (tx− 1) focuses to characterize tx-degree polynomial qx(·).

3. At each leaf hub x, a related property att(x) is allowed to hub x.

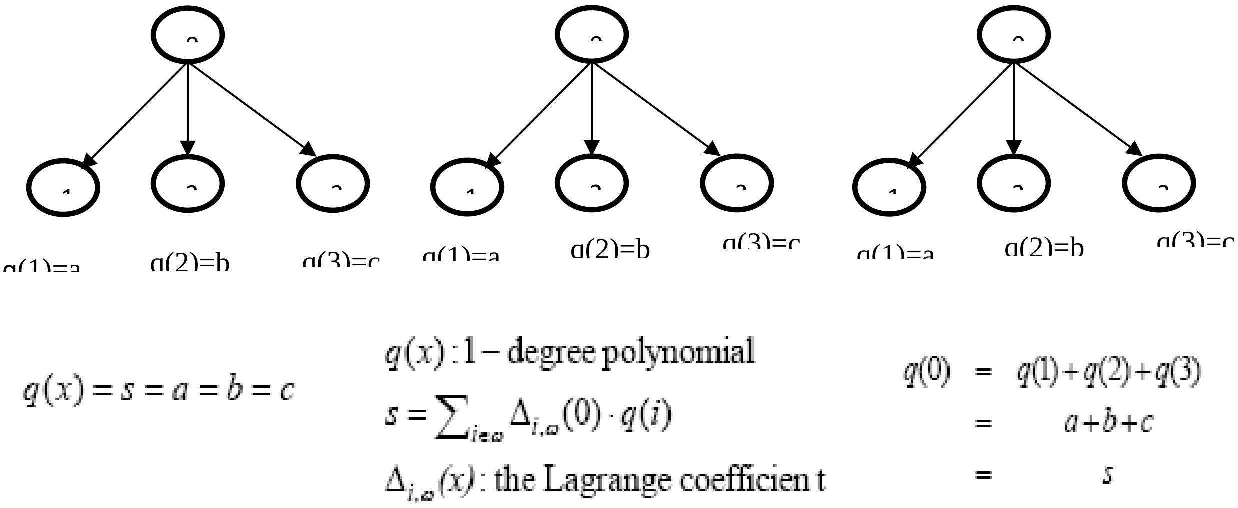
q(1)=a
q(2)=b
q(3)=c
q(1)=a
q(2)=b
q(3)=c
q(1)=a
q(2)=b
q(3)=c
$q(x) = s = a = b = c$
$q(x)$: 1 – degree polynomial
$s = \sum_{i \in \omega} \Delta_{i,\omega}(0) \cdot q(i)$
$\Delta_{i,\omega}(x)$: the Lagrange coefficien t
$q(0) = q(1)+q(2)+q(3)$
$= a+b+c$
$= s$

Fig.1: (1, 3),(2, 3), and (3, 3) Threshold gates

Here parent(x) signifies the parent hub of hub x, att(x) indicates the property-related with hub x if x is a leaf hub, index(x) means a record number related with hub x and the file number appointed exceptionally and ascendant along the tree from the root hub (list = 0) to the last leaf hubs. Accordingly, the entrance strategy A, comprising of both bound and distinct characteristics, would change over to an entrance tree as appeared in Fig.2.

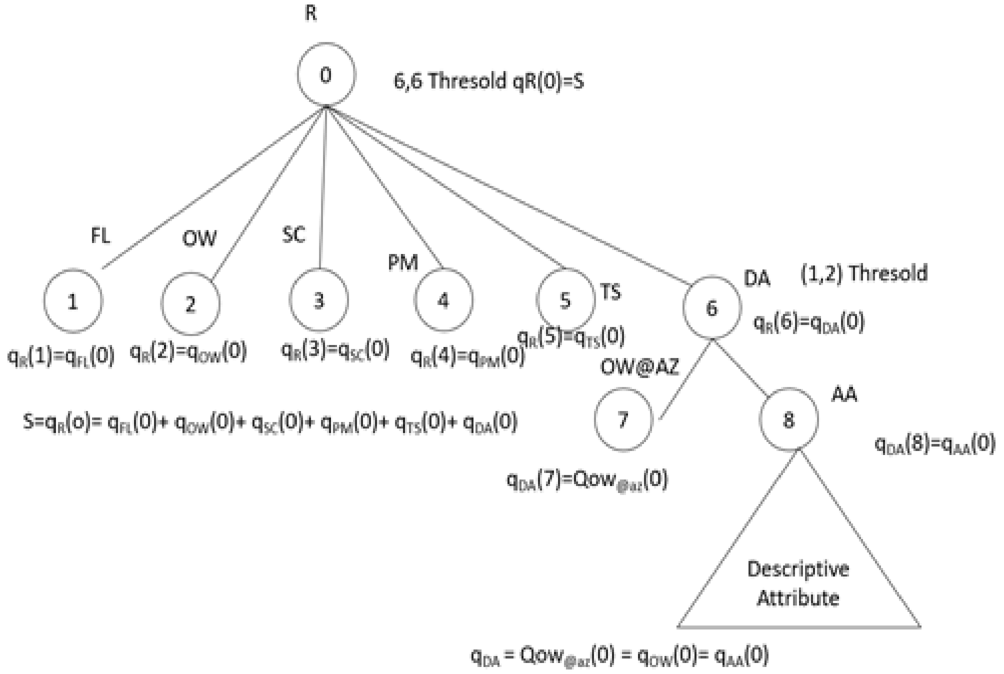

Fig.2: Top level of an AAuth access tree

ISSN: 2233-7857 IJFGCN

3.4 Flow Architecture

The general engineering of the proposed framework portrays as Fig.3 and Fig.4. Right now, the client needs to enrol to turn into a part in the cloud, when they enlisted client needs to pick a few characteristics and give some client characterized ascribes to encode their strategy record made while document transferring process, quality scrambled by the ElGamal calculation. In the wake of completing the strategy-setting technique, the confirmation technique ill e performed among client and ey chief abuse finishing the arrangement setting process; the validation procedure would perform among client and principal administrator utilizing Diffie-Hellman Algorithm. From that point onward, the client encodes their document utilizing mystery key which is given by the cloud, because of client qualities and afterwards it transfers into the cloud and arrangement record produced all the while. Presently Key director separates the mystery key into n shares (s1, s2… sn) and put away in various key troughs (k1,k2,… kn) . From that point forward, principal supervisors encoded the spilt key and sent the open key to the enlisted client in the cloud. On the off chance that clients need to download their documents in the cloud, at that point, they would send solicitations to the principal director with suitable characteristics. The Key-Manager would check their properties after that validation procedure and afterwards check the arrangement records. After that, Key-Manager would give decoded I-th offer to the client. Presently clients would get their mystery key and decode by utilizing their mystery key and afterwards download their records in the cloud.

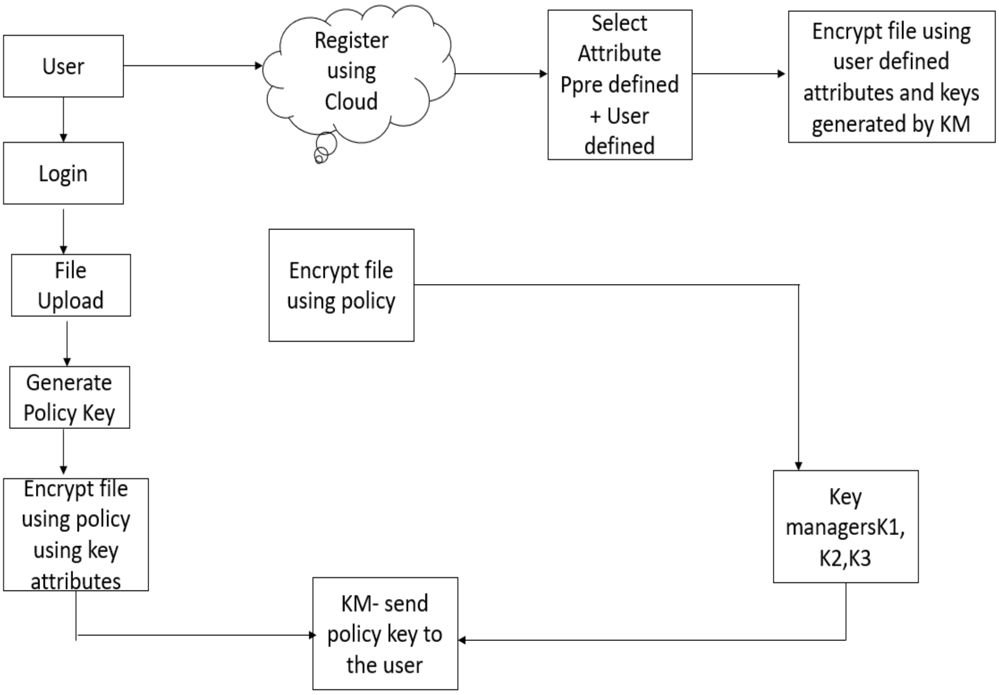
User
Register using Cloud
Select Attribute Ppre defined + User defined
Encrypt file using user defined attributes and keys generated by KM
Login
File Upload
Encrypt file using policy
Generate Policy Key
Encrypt file using policy using key attributes
Key managersK1, K2,K3
KM- send policy key to the user

Fig.3: File Upload by Owner

ISSN: 2233-7857 IJFGCN

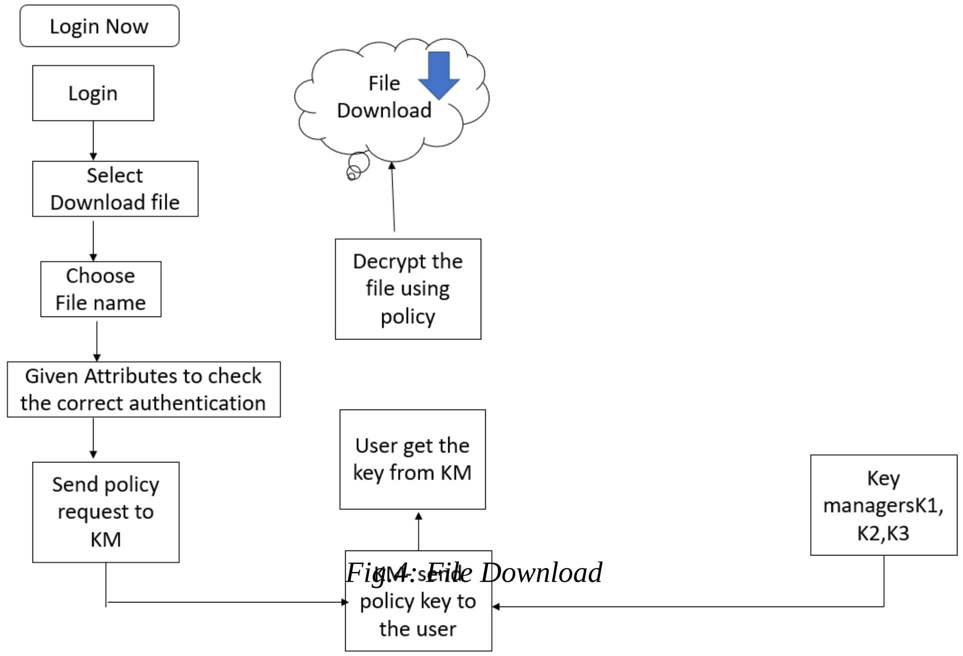
Login Now
Login
Select Download file
Choose File name
Given Attributes to check the correct authentication
Send policy request to KM
File Download
Decrypt the file using policy
User get the key from KM
KM send policy key to the user
Key managersK1, K2,K3

Fig 4: File Download

3.4.1 Elgamal Algorithm

In this proposed method, the ElGamal algorithm has used for attribute-based encryption. Using this attribute keys has generated. ElGamal is a public-key cryptosystem technique. ElGamal algorithm had used for encrypting and decrypting the file in the cloud environment by the users. In cryptography, the ElGamal encryption scheme is an uneven key encryption algorithm. In this method, using attributes generate a secret key. That secret key had used for policy file encryption for the security purpose.

3.4.2 Diffie-Hellman Algorithm

In this proposed method, this algorithm had used for the authentication process between the user and key management. It is a technique for making a common mystery numeric key over an open channel with potential spies. The two heroes don't have any (genuine) power over what the real number their mystery key is. (The key will at that point had utilized in an asymmetric key calculation, for example, DES and AES—see the following week's talks). Let $G = (Z/pZ) *$ be the multiplicative components mod p and is a cyclic gathering of request $p - 1$. In this manner, it has a generator g, $(Z/pZ)*= \{g, g2 , g3 , . . . gp-1\}$. Utilizing this calculation produces a mystery key between the client and key administration. That mystery key had utilized for scrambling the document during the transfer process.

Shamir's (k,n) secret sharing algorithm In this proposed method, this algorithm used for the necessary splitting of a secret key and stored in multiple key managers and reconstruct the keys for security purposes. Shamir's Mystery Sharing is a calculation in cryptography. It is a sort of mystery sharing, where a mystery is isolated into parts, giving every member its remarkable part, where a few or every one of them had required for remaking the mystery.

3.4.3 Mathematical Definition

The goal is to divide secret S (e.g., a safe combination) Into pieces of data S1,…., Sn in such a way that:

1. Knowledge of any K or more Si pieces makes S easily computable.
2. Knowledge of any K-1 or fewer pieces Leaves S completely undetermined (in the sense that all its possible values are equally likely).

This scheme is (K, n) threshold scheme. If k=n, then all participants should recreate the secret. In this method, the secret key splits and send to the multiple key managers. The multiple vital managers generate a public key and private key using split keys, and then public key only send to the user for decrypting purpose when user want to download the file.

3.4.4 RSA Algorithm

RSA algorithm has widely used for the public key algorithm. RSA is a chunk cypher, where each message has mapped to an integer.

RSA algorithm involves three steps:

a) Key generation
b) Encryption
c) Decryption

Steps:

Select two distinctive prime numbers an and b for security purposes, the whole numbers an and bought to be picked indiscriminately and ought to be of comparable piece length.

Register n=a*b. Figure Euler's totient work, (n)=(a-1)*(b-1). choose a whole number e, with the end goal that 1<e <(n1) and a most noteworthy basic divisor of e, (n) is 1. Presently 'e' is discharged as a clear key example. Presently decide d. d is the multiplicate opposite of e mod(n). D kept as a private key segment, and open key comprises of modulus n and the clear example.

The confided in power (TA), and the intermediary in interceded CPABE plans can utilize this convention to match up to their renouncement records through a stable channel. The convention is push-based with the accompanying suspicions and objectives:

1. The intermediary is continuously on the web,

2. The believed authority may not generally be on the web, and

3. The disavowal rundown of an intermediary should consistently be state-of-the-art, so denial promptly upheld. We accept that there is an out-of-band channel that had utilized to transmit essential offers after a crucial age. The protocol uses 4 types of messages, each consisting of a task indicator, the payload, digital signature and timestamp. The integrity and the source of a message checked the signature contains the public key of TA and the signed hash of the other three fields.

Creation of Public Key and Master Key Phase

```
Let: $G_0$ be a cyclic group of prime order p
        e : $G_0 \times G_0 \rightarrow G_T$ be a bilinear map
        U = {$att_1$, . . . ,$att_n$} be a set of attributes     //predefined and user defined attributes of files
        $S_i$ = {$v_i$,1,...,$v_i$,$n_i$ } be a set of possible values for $att_i$ where $n_i = |S_i|$
        PK be an ABE public key
        MK be an ABE master key
        Do:
        choose $g_1$, h ∈R G0 choose y ∈R $Z_p$
        Y ← $e(g_1, h)_y$
        for all i∈ [1, n] do
        for all $j \in [1, ni]$ do
        choose $t_i,j \in R\ Z_p$
        $T_{i,j} \leftarrow g_1\ t_i,j$
        end for
        end for
        PK ← $(e, g_1, h, Y, \{T_i,j\}i\in[1,n],j\in[1,n_i])$
        MK ← $(y, \{t_i,j\}i\in[1,n],j\in[1,n_i])$
        return PK,MK
```

Key Generation Phase

```
Keygen (PK, MK, L, $I_u$)
 Let: Iu be a unique identity of a user
 $L = [L_1, L_2,...,L_n]$ (where $Li \in S_i$) be an attribute list of a user
$sk_{LIu},1$ be the mediator decryption key share for $I_u$ with attribute list L
$sk_{LIu},2$ be the user decryption key share for $I_u$ with attribute list L
Do:
choose $r \in R\ Z_p$
$Y \leftarrow e(g_1, h)_y$
for all $v_{i,j}\in L$ do choose $r_{i,j}\in R\ Z_p$
end for
$d_0 \leftarrow h_y /g_1^r$
$d_1 \leftarrow g_1 / vi_{,j}$
 $\sum L\ ri,j\ vi,j\ / \sum L\ t_{i,j}$
$d_2 \leftarrow g_1$
$r- vi,j \sum L\ ri,j\ vi,j\ / \sum L\ ti,j\ )$
$sk_{LIu,1} \leftarrow d_1$
$sk_{LIu,2} \leftarrow (d_0, d_2)$
return $sk_{LIu,1}, sk_{LIu,2}$
```

Encryption Phase: Encryption (m, W, P_K)

```
Let
$W = [W_1, W_2,...,W_n]$ (where $W_i\in S_i$) be an access policy W
$C_W$ be a ciphertext encrypted under the access policy W
Do: choose $s \in R\ Z_p$
$C_2 \leftarrow g1^s$
$C_1 \leftarrow m \cdot Y^{\ s}$
$C_3 \leftarrow (\ vi,j \sum WTi,j\ )^s$
$C_W \leftarrow (W, C_1, C_2, C_3)$
return $C_W$
```

Decryption Phase

```
Decrypt(CW , W, $sk_{LIu,2}$, $C\hat{}_W$ )
Let
$C\hat{}_W$ be a valid decryption token for a ciphertext with policy W
$C_W$ be a ciphertext encrypted under the access policy W
$sk_{LIu,1}$ be a mediator key share for Iu with attribute list L that satisfies W
$sk_{LIu,2}$ be a user key share for Iu with attribute list L that satisfies W m be a plaintext message derived from $C_W$
Do:
$C\ _W \leftarrow e(C_3, d_2) = e(g_1, g_1)\ s(r- v_{i,j} \sum W\ r_{i,j}\ )$
```

ISSN: 2233-7857 IJFGCN

```
$\tilde{C} \leftarrow e(C2, d0) \cdot C\ W \cdot \hat{C}W = e(g_1^s, h_y)$
$m \leftarrow C2\ \tilde{C} = m \cdot e(g1,h)^{ys} / e(g_{1s},h_y)$
return m’
```

Token Computation Phase

```
ComputeToken ($C_W$, Iu, $sk_{LIu,1}$)
Let
$\hat{C}_W$ be a decryption token for a ciphertext with policy W
$sk_{LIu,1}$ be a mediator key share for $I_u$ with attribute list L that satisfies W
Do: $\hat{C}_W \leftarrow e(C_3, d1) = e(g_1, g_1)^{s \sum vi,j \in W\ ri,j}$
return $\hat{C}_W$
```

Add-attribute

The TA sends this message to the intermediary in the wake of calling the Arrangement calculation. Its payload contains the total number of qualities and the name and length of each characteristic. Upon receipt and check of the message, the intermediary would store the symbolic names in its database.

Include client

This message sent after the TA calls the Keygen calculation. Its payload made out of the number of usernames, the usernames and the ascribes related to each username. The intermediary stores the client data in the database if the message had checked.

Renounce

This message sent when the TA refreshes the renouncement list. This message had utilized to repudiate traits for the entire framework or chose clients as it were. Its payload contains an extension field to show if it is framework full or specific, the quantity of credits to repudiate and usernames influenced if the degree isn't framework wide.

SYSTEM SETUP AND IMPLEMENTATION

The examinations had performed with the applications and the FTP server introduced on a similar machine with an Intel Center i7 6600U processor and 16 GB usable Slam. The investigations had directed utilizing a Wi-Fi association with the most significant download speed of 1Mbps and most extreme transfer speed of 0.6Mbps up to 8GB transfer. The FileZilla FTP server had introduced to help FTP locally. A MySQL 5.5.11 server is running introduced privately had utilized for the database of the confided in power. The information associations with the customer and server accelerate to 5 MB. The arrangement cost in non-interceded plans is essentially the time required by the real arrangement calculation while the arrangement cost in intervened conspires additionally incorporates an opportunity to refresh the databases and send refreshes utilizing attachments. The standard handling time for framework arrangement relies predominantly upon the expense of the calculation for little and enormous estimations of N or the number of framework traits.

Table 1: Average system setup time by No. of Attributes

Number of attributes	Algo setup Execution time in sec (Existing)	Algo setup Execution time in sec (Proposed)

16	2	1.5
32	4	3.7
64	6	5
128	12	10
256	25	17

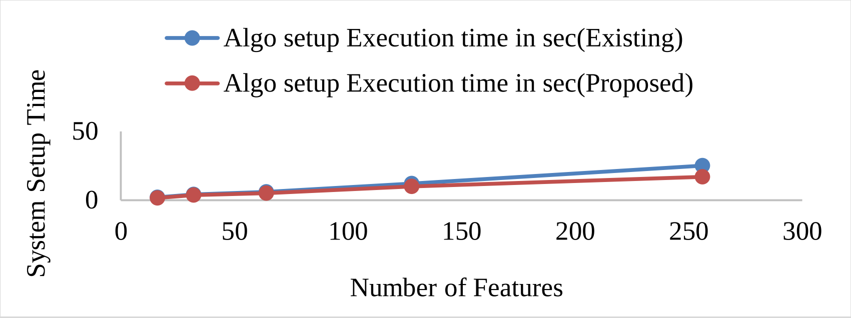

Fig.5: Average system setup time by No. of Attributes

Fig.5 and Table 1 show the Average system setup time by No. of AttributesIn the X-axis we plot the Number of Features, and in the Y-axis, we plot the required system setup time. The existing algorithm had Mediated Constant Ciphertext-Policy ABE (MCCP-ABE), and the proposed one is ABE token-based OAuth protocol. The proposed system reduces the time taken to set up the system than the existing algorithm when the number of features had increased.

Table 2: Avg Key Generation time by Number of Attributes

Number of attributes	Avg Key generation time in sec (Existing)	Avg Key Generation time in sec (Proposed)
16	2	1.5
32	4	3.7
64	6	5
128	12	10
256	25	17

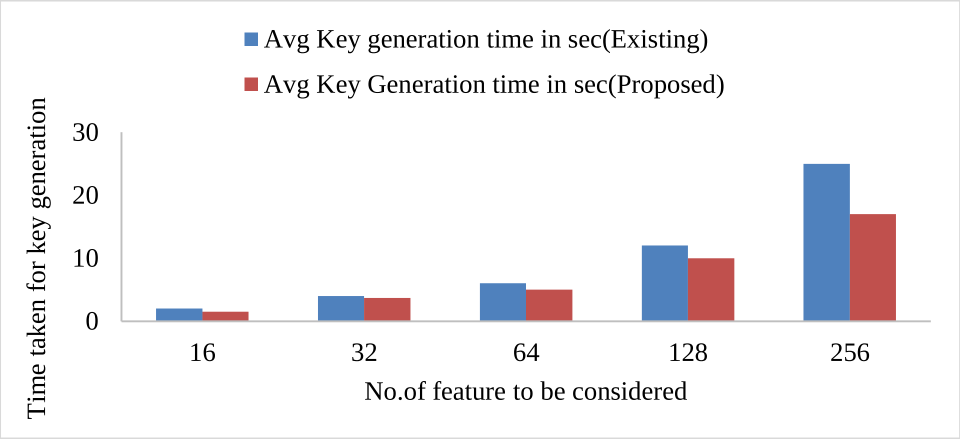

Fig.6: Avg Key Generation time by Number of Attributes

Fig.6 and Table 2 has obtained the value from the time taken for the key generation with the number of attributes added in the algorithm. In the X-axis, we plot the Number of Features, and in the Y-axis, we plot the time required for key generation. The existing algorithm had Mediated Constant Ciphertext-Policy ABE (MCCP-ABE), and the proposed algorithm is ABE token-based OAuth protocol. The proposed system reduces the time taken for key generation than the existing algorithm when the number of features had increased.

Table 3: Avg Encrypt and upload 32 kb jpg file by number of attributes

Number of attributes	Avg time to encrypt and upload a 32kb jpeg image in sec (Existing)	Avg time to encrypt and upload a 32kb jpeg image in sec (Proposed)
16	0.6	0.5
32	1.1	1
64	2.1	2.1
128	5.1	4
256	8.3	7.9

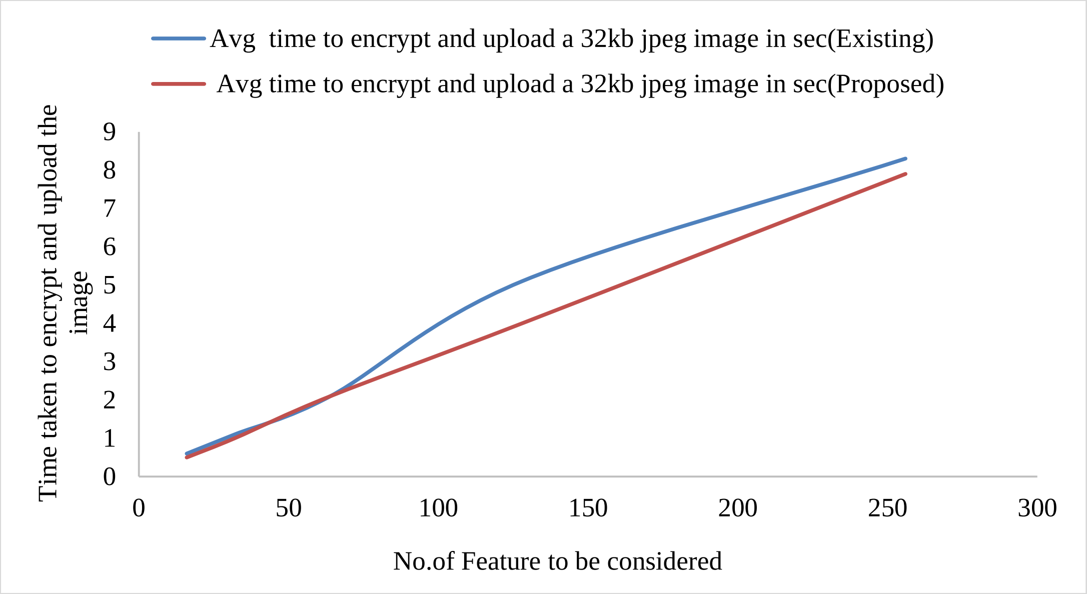

Fig.7: Avg Encrypt and upload 32 kb jpg file by number of attributes

Fig.7 and Table 3 had prepared to obtain the value from the time taken for encrypting the 32 kb image and upload the same in the cloud with the number of attributes added in the algorithm. In the X-axis, we plot the Number of Features, and in the Y-axis, we plot the time taken to encrypt and upload the image. The existing algorithm had Mediated Constant Ciphertext-Policy ABE (MCCP-ABE), and the proposed algorithm is ABE token-based OAuth protocol. The proposed system reduces the time taken to encrypt and upload the 32kb image in the cloud than the existing algorithm when the number of features had increased.

Table 4: Average download and decrypt time for 32kb image by several attributes

Number of attributes	Avg time to download and decrypt a 32kb jpeg image in sec (Existing)	Avg time to download and decrypt a 32kb jpeg image in sec (Proposed)
16	1.5	1
32	2.5	1.5
64	3	1.8
128	5	4.3
256	9	8

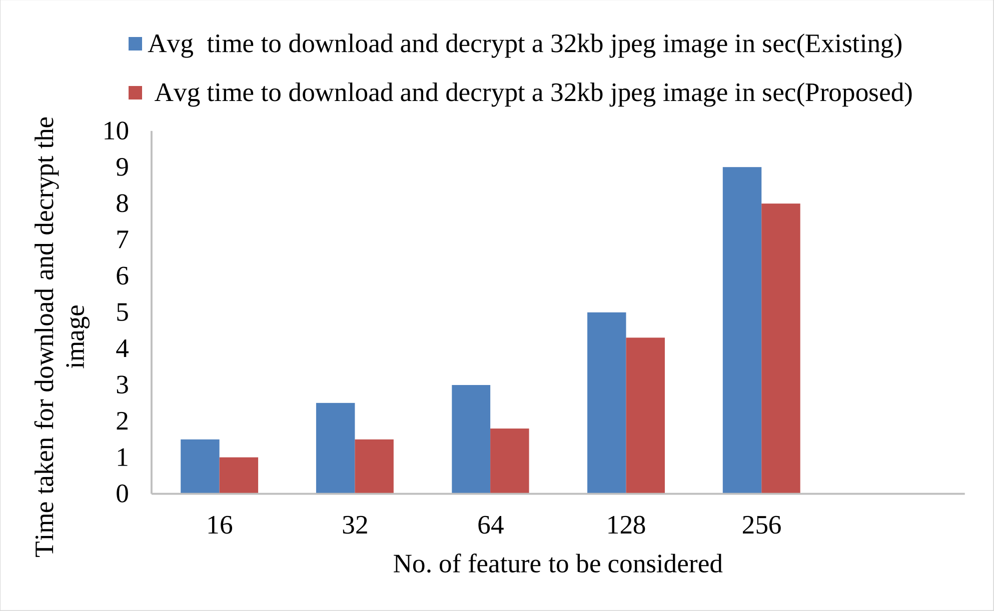

Fig.8: Average download and decrypt time for 32kb image by the number of attributes

Fig.8 and Table 4 had prepared to obtain the value from the time taken for downloading the 32 kb image from the cloud and also decrypt with the number of attributes added in the algorithm. In the X-axis, we plot the Number of Features, and in the Y-axis, we plot the time taken to download and decrypt the image. The existing algorithm had Mediated Constant Ciphertext-Policy ABE (MCCP-ABE), and the proposed algorithm is ABE token-based OAuth protocol. The proposed system reduces the time taken to download the 32 kb image from the cloud and decrypt than the existing algorithm when the number of features had increased.

1. CONCLUSION

The availability of internet bandwidth on a broad scale paved the way for practical computing services. Cloud invented to meet the requirements of data storage. Cloud computing refers to the distribution of various IT services over the internet. It offers various benefits for organizations and end-users. It altogether decreases the expense of renouncement in MC-CP-ABE by taking out costly calculations in monotonous critical age from influenced properties while refreshing an enormous number of keys. Results likewise indicated that our plan requires more opportunity for arrangement, critical age, and decoding because of extra assignments, however distinction in cost from the alterations is basically because of information base inquiries and transmission through an intermediary and not because of extra calculations in our development. The proposed conspire utilizes a solitary trusted inside a gathering of clients. Future examination on the chance of utilizing increasingly expressive access structure had suggested. Because of the outcomes, we demonstrated that proposed framework necessarily diminishes the expense of repudiation in MC-CP-ABE by dispensing with costly calculations in dull key age from influenced qualities when an enormous number of keys must have refreshed. Results likewise demonstrated that our plan requires more opportunity for arrangement, critical age and decoding because of extra assignments. The distinction in cost from alterations are chiefly because of database inquiries transmission through an intermediary and not because of the extra calculations in our development. For this, we suggest that future work would concentrate on streamlining the database and intermediary server associations for the proposed framework. The proposed conspire utilizes a solitary confided in power inside a gathering of clients. Future investigation on the chance of utilizing increasingly expressive access structures had prescribed. We additionally suggest for future work a progressively intensive investigation of the semantic security of the proposed convention framework.

REFERENCES

[1]. R.Rajan, G.Murugaboopathi, C.Parthasarathy. (2017). Providing Triple-Key Benefits with Designated Mining and Freedom from Danger Informatics for User Data. Journal of Advanced Research in Dynamical and Control Systems. Vol. 9. Sp– 16 / 2017. Page: 966-979.

[2]. R.Rajan, G.Murugaboopathi, C.Parthasarathy. (2017). Analysis and assessment of various cryptographic techniques based on a variety of features. International Journal of Engineering & Technology, 7 (1.9) (2018) 28-33.

[3]. Joshi, M., Joshi, K. P., &Finin, T. (2019). Delegated Authorization Framework for EHR Services using Attribute-Based Encryption. *IEEE Transactions on Services Computing*.

[4]. Youn, T. Y., Jho, N. S., Rhee, K. H., & Shin, S. U. (2019). Authorized Client-Side Deduplication Using CP-ABE in Cloud Storage. *Wireless Communications and Mobile Computing*, *2019*.

[5]. Balamurugan, B., & Krishna, P. V. (2014). An extensive survey on usage of attribute-based encryption in the cloud. *Journal of emerging technologies in web intelligence*, *6*(3), 263-272.

[6]. Sun, J., Ren, L., Wang, S., & Yao, X. (2019). Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage. *IEEE Access*.

[7]. Eltayieb, N., Wang, P., Hassan, A., Elhabob, R., & Li, F. (2019). ASDS: Attribute-based secure data sharing scheme for a reliable cloud environment. *Security and privacy*, *2*(2), e57.

[8]. Deshmukh, J., & Bhandari, G. (2019). A Review Paper on Attribute-Based Encryption for Message Privacy in Cloud. *Asian Journal for Convergence in Technology (AJCT)*.

[9]. Mouleeswaran, S. K., & Devi, K. (2019). Class-Based Multi-Stage Encryption for Efficient Data Security in Cloud Environment Using Profile Data. *International Journal of Computer Communication and Informatics*, *1*(1), 22-29.

[10]. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.

[11]. Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, *72*, 1-12.

[12]. Li, F., Rahulamathavan, Y., Rajarajan, M., & Phan, R. C. W. (2013, March). Low complexity multi-authority attribute-based encryption scheme for mobile cloud computing. In *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering* (pp. 573-577). IEEE.

[13]. Hota, C., Sanka, S., Rajarajan, M., & Nair, S. K. (2011). Capability-based cryptographic data access control in cloud computing. *International Journal of Advanced Networking and Applications*, *3*(3), 1152-1161.

[14]. Wang, C., Ren, K., Lou, W., & Li, J. (2010). Toward publicly auditable secure cloud data storage services. *IEEE Network*, *24*(4), 19-24.

[15]. Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2013). Identity-based encryption with outsourced revocation in cloud computing. *IEEE Transactions on Computers*, *64*(2), 425-437.

[16]. Do, J. M., Song, Y. J. & Park, N. (2011, May). Attribute-based proxy re-encryption for data confidentiality in cloud computing environments. In *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering* (pp. 248-251). IEEE.

[17]. Xue, K., Hong, J., Ma, Y., Wei, D. S., Hong, P., & Yu, N. (2018). Fog-aided verifiable privacy-preserving access control for latency-sensitive data sharing in vehicular cloud computing. *IEEE Network*, *32*(3), 7-13.

[18]. El Ghoubach, I., Abbou, R. B., &Mrabti, F. (2019). A secure and efficient remote data auditing scheme for cloud storage. *Journal of King Saud University-Computer and Information Sciences*.

[19]. Jayarajan, P., Kanagachidambaresan, G.R., Sundararajan, T.V.P. et al. J Supercomput (2018). http://sci-hub.tw/10.1007/s11227-018-2582-4

[20]. A KARTHIKEYAN∗, P G KUPPUSAMY†, AND IRAJ S AMIRI* (2020). SECURED IDENTITY BASED CRYPTOSYSTEM APPROACH FOR INTELLIGENT ROUTING PROTOCOL IN VANET, Scalable Computing: Practice and Experience, ISSN 1895-1767, Volume 21, Issue 1, pp. 41–46, DOI: 10.12694:/scpe.v21i1.1608