RETRIEVING SECURE ENHANCED AES BASED WATERMARKING DATA COLORING IN CLOUD COMPUTING ATMOSPHERE

MANSOORAHAMAD R[1], Mr.B.KKARUPPUSAMY[2],

[1]*Mphil Research Scholar, Department of Computer Science, CMS College Of Science and Commerce , Coimbatore, Tamilnadu, India.*

[2]*Assistant Professor, Department of Computer Science, CMS College Of Science and Commerce , Coimbatore, Tamilnadu, India.*

---***---

Abstract - *Variety of companies the usage of cloud computing has improved dramatically over the last few years because of the attractive capabilities including scalability, flexibility, fast start-up and coffee expenses. offerings supplied over the net are ranging from the use of provider's software program and hardware to handling safety and other troubles. a number of the biggest challenges at this point are supplying privateness and data protection to subscribers of public cloud servers. An green encryption approach provided in this paper can be used for secure get admission to to and storage of data on public cloud server, moving and searching encrypted records via communiqué channels whilst shielding information confidentiality. security has come to be an critical and vital paradigm in information services that supplied by way of various clouds. information want to be stored and manipulated very confidentially and without information breach.*

Cloud computing presents a service based totally on net for several shared resources and system software program across diverse environment. For cozy cloud garage the method of encryption of the data to the customers for various desires has been introduced with the aid of the delegated access control approach. typically garage in public cloud requires excessive verbal exchange, heavy load due to maximum storage and high computational charges. on this paper, we're implementing multi-cloud environment for secure garage where it acts as a public cloud and presents low fees, also it entails two- layer encryption over the information saved within the cloud. we are the use of an green AES algorithm which offers higher confidentiality and privateness for numerous users within the cloud and stores the statistics in multi-clouds where the users can retrieve with the keys later while delegating it via get admission to manipulate from the cloud. Securities as well as expenses are the peak troubles in this area of studies and that they range considerably, depending on the vendor.

To defend clouds, providers need to first secure virtualized datacenter assets, uphold person privateness, and hold records integrity. The authors propose using a consider-overlay network over more than one facts centers to implement a reputation gadget for setting up agree with between service companies and statistics owners. statistics coloring and software program watermarking techniques shield shared facts gadgets and vastly dispensed software program modules. those techniques guard multi-way authentications, enable unmarried sign-on within the cloud, and tighten get right of entry to manage for sensitive statistics in both public and private clouds. The proposed model is exceedingly efficient and secures underneath current security models. The authors tried to study the threats and attacks that possibly launch in cloud computing records garage and proposed a safety mechanism.

This paper offers a strong picture watermarking scheme based totally on a sample projection method. while we keep in mind the human visual system in our watermarking algorithm, we use the low frequency additives of image blocks for statistics hiding to attain excessive robustness in opposition to attacks. We use four samples of the approximation coefficients of the image blocks to construct a line segment inside the 2-D area. The slope of this line segment, that is invariant to the gain component, is employed for watermarking cause. We embed the watermarking code by using projecting the line section on some unique traces according to message bits. To design a most probability decoder, we compute the distribution of the slope of the embedding line segment for Gaussian samples. The performance of the proposed approach is analytically investigated and verified via several simulations. Experimental outcomes verify the validity of our model *and its high robustness towards common attacks in evaluation with similar watermarking strategies which are invariant to the gain assault.*

Key words:* *green AES , Multi clouds, statistics coloring, software watermarking.

1. INTRODUCTION

Cloud computing and storage solutions provide users and firms with numerous talents to shop and process their facts in 0.33 birthday party statistics centers. There are a number of protection problems/issues associated with cloud computing but these problems fall into large classes: safety problems confronted through cloud providers (corporations providing software program-, platform-, or infrastructure-as-a-service through the cloud) and security issues faced via their clients (businesses or companies who host programs or store information on the cloud).The responsibility is going both approaches, however: the provider ought to make certain that their infrastructure is comfy and that their customers' records and packages are blanketed at the same time as the consumer must take measures to give a boost to their application and use robust passwords and authentication measures. whilst an agency elects to shop records or host applications on the public cloud, it loses its potential to have physical access to the servers hosting its statistics. As a result, doubtlessly commercial enterprise sensitive and confidential information is at hazard from insider attacks. According to a latest Cloud safety Alliance document, insider attacks are the 0.33 biggest threat in cloud computing. Consequently, Cloud service carriers have to make certain that thorough background exams are conducted for employees who've physical get right of entry to the servers within the records middle. Moreover, data centres need to be often monitored for suspicious hobby. So as to preserve assets, reduce prices, and hold performance, Cloud provider carriers regularly shop more than one consumer's facts at the identical server.

Cloud computing is generation which isn't always product however more than carrier provision. it is the mixture of computing and services. It believes in something –anywhere idea and provides offerings thru net at single browser. 5 important component of cloud environment may be listed underneath; 1. information: It the collection of uncooked material which may be beneficial won't. 2. storage: this is the organized set of facts for clean get admission to, replace and control reason. It considers datacentres, disk, faucets for storage motive and database servers for agency of information. 3. patron Networks: It consists of diverse gadgets like PDA, smart cellphone, I-cellphone, computer systems, laptops and so on. it is able to categorized as cellular client, assume and thick consumer. four. programs & Computing: applications are the human or system advanced computing program facilitates to fulfill the requirement and execution of undertaking. further, it requires Computing, that is the purpose of orientated interest creating series of steps the use of algorithms. 5. Virtualization: it's miles the creation of virtual version as opposed to actual. It enables to get admission to resources and services. Cloud customers are most concerned about whether or not statistics-middle owners will abuse the gadget by means of randomly the usage of private datasets or freeing touchy statistics to a 3rd party without authorization. Cloud protection hinges on a way to set up agree with among these provider carriers and information proprietors. To address these issues, we propose a recognition-primarily based agree with-management scheme augmented with information coloring and software program watermarking. records approximately associated trust models is to be had somewhere else.

2. REVIEW OF LITERATURE

Brinkman et al. [16] evolved an set of rules for searching databases in XML format. Goh [17] used a trapdoor generated by way of a secret key in his efficient comfortable searching approach over encrypted information and evolved a secure indexing version.

Boneh et al. [18] devised a searchable public key encryption schema based on a sequential search at the server. Authors evolved strategies; one is primarily based on bilinear maps, and any other on trapdoor permutations. Dai et al [19, 20] developed a PKI-primarily based encryption technique that allowed clients direct access to cloud records and proposed dynamic control of allotted assets and get right of entry to to them by means of remote actors.

Kan Yang et al. [21] designed comfy data get entry to manipulate mechanism for a couple of authority cloud garage and revocation method which offers ahead in addition to backward security. A decentralized get entry to control approach to help anonymous authentication changed into proposed by means of Ruj et al. [22].

Bamiah et al. [23] evolved on fly encryption of statistics at storage server, and used a multi-component authentication schema for get right of entry to control mechanisms and safety controls. AlZain et al. [24] and Akshay et al. [25] performed survey related to cloud security issues and addressed feasible answers for those issues.

Ateniese et al.[3] proposed a proxy re encryption technique that is a secure distributed storage scheme. The blocks of content are encrypted by using statistics proprietor with symmetric content keys.

Naor et al.[7] offered symmetric key primitives in an untrusted storage surroundings. This scheme is based totally on pre-key distribution mechanism using blom[8] scheme. This reduces the general public key cryptography in software program as a service model.

Kai Hwang et. Al.[3] illustrates records coloring and software watermarking techniques prevents shared information objects and extensive dispensed software modules. these strategies precautions multi-manner authentications enable single sign on within the cloud and tighten get entry to control for touchy information in public and personal clouds .through implementing this concept cloud providers can enforce the records-coloring mechanism, proposed recognition machine to relaxed statistics middle get entry to at a crude-grained degree, relaxed records get admission to at a first-rate-grained document level.

Nasrin Khanezaei, et. al. [4] explores that cloud frameworks is one of the principal application phenomena for today's improvement. right here, they explores the recent troubles and cope with safety as the one of the essential subject for cloud computing. warranty approximately safety services not handiest enables to hold privacy and originality of records however keep user agree with on carrier vendors. To put into effect the safety mechanism with cloud surroundings they makes use of AES and RSA algorithm with key sharing mechanism

2.1 Database Management in the Cloud:

The total price of statistics management is five to 10 instances better than the initial acquisition fee. As a end result, there may be a growing interest in outsourcing database management responsibilities to third events that may offer those duties for tons lower price because of the economy of scale. This new outsourcing version has the blessings of decreasing the cost for running Database management device (DBMS independently [1]. A Cloud database control system (CDBMS) is a disbursed database that provides computing as a carrier instead of a product. it's miles the sharing of sources, software program, and data between multiply gadgets over a network that's by and large the internet.

2.2 Cloud Computing Attacks

a. Denial of Service (DoS) attacks: A few security experts have argued that the cloud is extra susceptible to DoS attacks, because it is shared by using many users, which makes DoS assaults a great deal more adverse.

b. Side Channel attacks An attacker ought to attempt to compromise the cloud by placing a malicious virtual device in close proximity to a goal cloud server after which launching a side channel attack.

c. Authentication attacks: Authentication is a susceptible factor in hosted and digital offerings and is often focused. there are numerous exceptional ways to authenticate customers; as an instance, based totally on what someone is aware of, has, or is. The mechanisms used to comfortable the authentication method and the techniques used are a frequent target of attackers.

d. Man-in-the-middle cryptographic attacks: This assault is achieved while an attacker places himself between two users. each time attackers can location themselves in the communique's course, there is the opportunity that they could intercept and regulate communications.

e. Inside-job: This type of assault is whilst the person, employee or staffs who's informed of how the system runs, from purchaser to server then he can implant malicious codes to spoil the entirety within the cloud device.

3. ANALYZING SECURITY TROUBLES IN CLOUD AND PROPOSED SOLUTIONS

There are 5 styles of problems improve while discussing safety of a cloud. 1. records issues 2. privacy troubles three. loss of accept as true with 4. Securing statistics in Transmission five service company safety issues. The general public cloud computing environment supplied with the aid of the cloud dealer and make certain that a cloud computing decision satisfies organizational protection and privacy needs.

first off, on every occasion a statistics is on a cloud, all people from anywhere anytime can access records from the cloud in view that records can be commonplace, non-public and sensitive statistics in a cloud. So at the same time, many cloud computing carrier client and provider accesses and adjust statistics. Consequently there may be a want of some statistics integrity method in cloud computing. Secondly, facts stealing are one of the significant issue in a cloud computing surroundings. Many cloud service provider do not provide their very own server alternatively they accumulate server from different service companies because of it's far cost affective and flexible for operation and cloud company. So there's a miles probability of statistics may be stolen from the external server. Thirdly, records loss is a commonplace problem in cloud computing. If the cloud computing service provider shut down his offerings due some financial or criminal hassle then there may be a lack of records for the user. Furthermore, statistics can be misplaced or harm or corrupted because of leave out going on, herbal catastrophe, and fireplace. Secrecy issues The cloud computing service provider must ensure that the customer private statistics is nicely secured from other carriers, purchaser and person. As maximum of the servers are external, the cloud carrier issuer have to make certain who's accessing the facts and who's keeping the server so that it enable the provider to defend the patron's non-public facts.

3.1 Security Demanding Situations

With cloud applications, agencies can use offerings and facts from any bodily vicinity. out of doors get right of entry to can be insecure and lift questions about privateness, confidentiality, integrity and demanded a trusted computing environment wherein statistics confidentiality, authentication with get entry to manage may be maintained. The complete cloud environment increases certain issues which may be indexed underneath:

- information security
- identity and access control
- Key control
- virtual machine safety

inside the current machine numerous elements based on encryption had been proposed for get entry to control over encrypted group with a exceptional symmetric key. users could be issued keys for the data's which might be reachable. as the statistics owner doesn't manage a duplicate of the facts, every time the user dynamics change, the owner desires to down load the records for decryption, and re-encrypt it with the brand new keys for importing.

This development need to be practically carried out to all of the encrypted statistics objects with the similar key. it's miles bungling while the facts set to be re-encrypted is big.

To issue new keys, the proprietor desires to installation personal verbal exchange channels by means of the customers. The privacy and the identification of customers are not taken into account. Consequently it may study sensitive facts about the agency and their customers. It requires the owner to enforce all the ACPs by using encryption, each first of all and ultimately after customers are brought or revoked. these kinds of encryption activities have to be achieved at the owner that as a result incurs excessive verbal exchange and computation price.

3.2 Encryption of cloud:

Jing-Jang Hwang et al. [5], has proposed an enterprise version for cloud computing for information safety the usage of facts encryption and decryption algorithms. in this method cloud service issuer has answerable for records storage and facts encryption/decryption obligations, which takes more computational overhead for system of statistics in cloud server. the primary disadvantage of this method is, there may be no control.

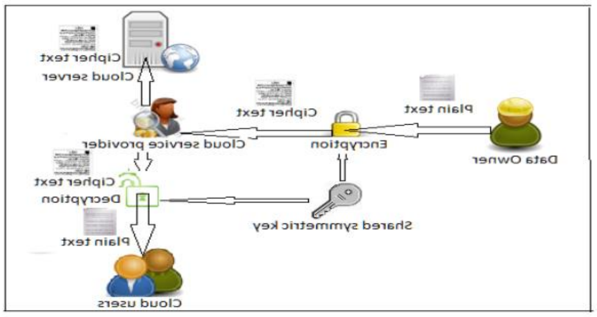

Fig-1 Block Diagram of Data Encryption and Decryption in Cloud System

Junzuo et al. [6], proposed an attribute based totally Encryption (ABE) and verifiable information decryption method to provide facts protection in cloud primarily based machine. They were designed the statistics decryption set of rules primarily based at the person requested attributes of the out sourced encrypted data. one of the fundamental efficiency drawbacks of this technique is, cloud carrier company has greater computational and garage overhead for verification of user attributes with the outsourced encrypted statistics. while third party auditor we are able to reduces the garage, computation, and verbal exchange overheads of the cloud server, which improves the efficiency of the cloud facts garage.

Fatemi Moghaddam et al. in [7], mentioned the overall performance of six exclusive symmetric key RSA information encryption algorithms in cloud computing environment. they have proposed separate cloud servers; one for records server and different for key cloud server and the records encryption and decryption process at the patron aspect. the main drawback of this method is to keeping separate servers for records safety in cloud, which creates a extra storage and computation overheads.

3.21. Various Encryption based solutions

A. Symmetric key cryptography (SKC) based solutions:
Symmetric-key algorithms are a category of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there can be a simple transformation to move among the 2 keys. The keys, in practice, constitute a shared secret between or more parties that may be used to hold a private information link.
Vimercati et.al.[6] Proposed an answer for securing outsourced information on semi-depended on servers based totally on symmetric key derivation strategies , that can acquire best-trained get right of entry to control. Lamentably, the complexities of report creation and consumer supply/revocation operations are linear to the range of legal customers that is much less scalable.

B. Public key cryptography (PKC) based solutions:
PKC based solutions were proposed because of its potential to separate write and study privileges. To recognize fine-grained get entry to manipulate, the conventional public key encryption (PKE) primarily based schemes proposed by means of J. Benaloh, M. Chase, E.Horvitz, and ok. Lauter [1] of their work "affected person managed encryption guarantees the privacy of electronic clinical information. They purpose the solution state of affairs and shows how public and symmetric primarily based encryption used , drawback in their solution is either incur excessive key management overhead, or require encrypting more than one copies of a report using exclusive customers' keys.

C. Attribute Based Encryption based solutions:
A number of works used ABE to understand high-quality-grained get right of entry to control for outsourced records, mainly; there has been an growing hobby in making use of ABE to secure electronic healthcare records (EHRs). Narayan et al. proposed an attribute-based infrastructure for EHR structures, wherein each affected person's EHR files are encrypted the usage of a broadcast variation of Cipher text-ABE (CP-ABE)[4].But, the ciphertext length grows linearly with the number of unrevoked customers.

In [3], Akinyele et al. investigated using ABE to generate self-protective EMRs, which could both be saved on cloud servers or mobile telephones so that EMR will be accessed whilst the health provider is offline. disadvantage is tool dependency and revocation isn't supported. different common downside of all above solutions is hassle of key-escrow as they bear in they consider single trusted authority.

3.2 PROPOSED METHOD

This paper is in general related to works in cryptographically enforced access manage for outsourced information and attribute based totally encryption. To recognise quality-grained get right of entry to control, the conventional public key encryption (PKE) based schemes either incur high key control-guys overhead, or require encrypting a couple of copies of a report the use of specific users‟ keys. to improve upon the scalability of the above solutions, one-to-many en-crypt ion techniques such as ABE can be used.

The usage of public cloud servers to store purchaser's facts makes secure sharing of facts a challenge. of data stored on the public server data access policies must be enforced. The cryptographic technique proposed in this work addresses this problem. Secret keys are kept by the data owner. Data must be encrypted before storing on a server, and the only way a client can access data s by supplying the corresponding decryption key.

The main aim is to create a system which can defend itself from outside and inner assaults. structure of the proposed cryptographic garage carrier shown on figure 2 and consists of the subsequent entities: entities: data owner, client and cloud service provider.

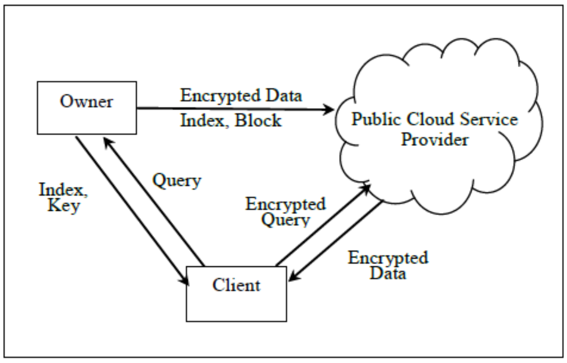

Fig 2. Architecture of the proposed cryptographic storage service

Data owner:

The information owner module is chargeable for encrypting the data. After encrypting the records by the proposed approach, the information owner sends statistics to cloud garage server. The facts are saved in the public part of the data garage server. information owner wishes get right of entry to the cloud server handiest for loading and updating encrypted information.

Clients:

Trusted parties wishing to get entry to the cloud records by means of encrypted identifier provided by means of the data proprietor. handiest the legitimate customers are allowed to get right of entry to and shop facts with self-belief. to use the carrier the following tasks might be accomplished: Figure 6 depicts the Authentication of the client performed by the proprietor (person call, password) then consultation password sent to the purchaser e mail or mobile telephone. Then the customer downloads software which permits him to execute queries at the records without exposing the consequences of the queries to the cloud service company. using the utility the patron may be able to decrypt the cipher (encrypted original facts) obtained from the cloud server. There's no need to download all the encrypted records, decrypt it and search locally. Clients wishing to search over the facts generated by way of the proprietor (multiple readers/single writers) should run this application separately.

Cloud Service Provider:

Provides data service and other computation and communication services on its premises. Encrypted records from data owners are stored at the statistics servers. Proposed machine permits a user with insufficient resources to go looking encrypted information at the public cloud server whilst protecting the privacy of the statistics. all the records should be encrypted earlier than garage. positive computations can be completed over the encrypted facts to find out whether or not a block of encrypted facts incorporates precise word(s) without disclosing every other records about the authentic text.

The audit service is achieved by means of TPA tracking. now and again the TPA may additionally have probabilities to hide anomaly information to cloud customers. to overcome this downside, we advise dynamic audit provider in the cloud. on this approach consumer sent query request to server and that server fits the person query and key-word if it's far fit, person can precede the system in any other case, the consumer is automatically/ untrusted and sends intimation about anomaly detection to cloud user. So that it can secure the cloud storage data.

In our work we use the two-layer encryption for storage of records throughout multi-clouds in place of a unmarried public cloud. Especially, it provides a better way for various updates, user locations, and modifications of the data. The system goes through one additional phase compared to the existing system. Also, it provides several functions based on the decomposition or splitting of data to store across various clouds, which are finally retrieved by the user with the help of keys

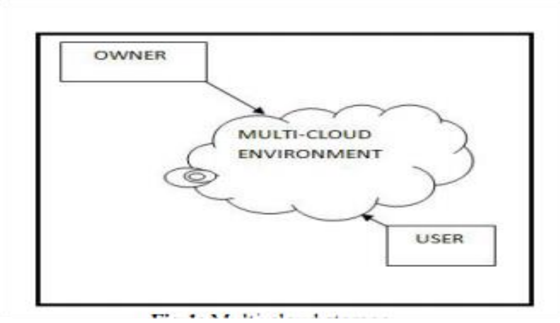

Fig 3 Multi-cloud storage

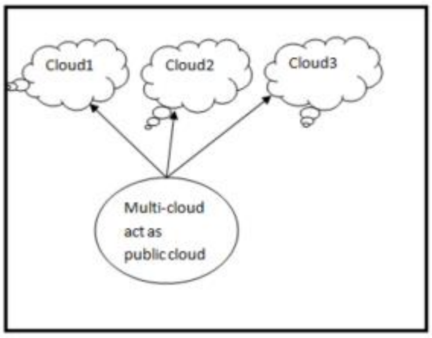

Fig 4 -cloud splitting

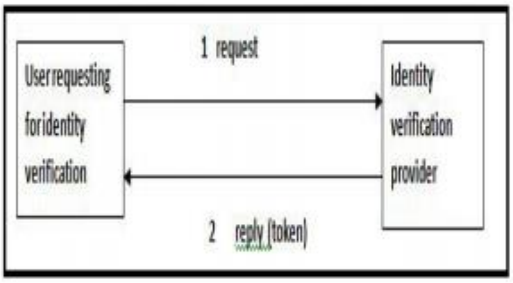
1 request
User requesting for identity verification
Identity verification provider
2 reply (token)

Fig 5. Two layer encryption in multi-cloud Environment

Identity token providence: IdP's issue identity tokens to Users based on their identity attributes.

Policy decomposition: The Owner decomposes each ACP into at most two sub ACPs such that the Owner enforces the minimum number of attributes to assure confidentiality of data from the Cloud.

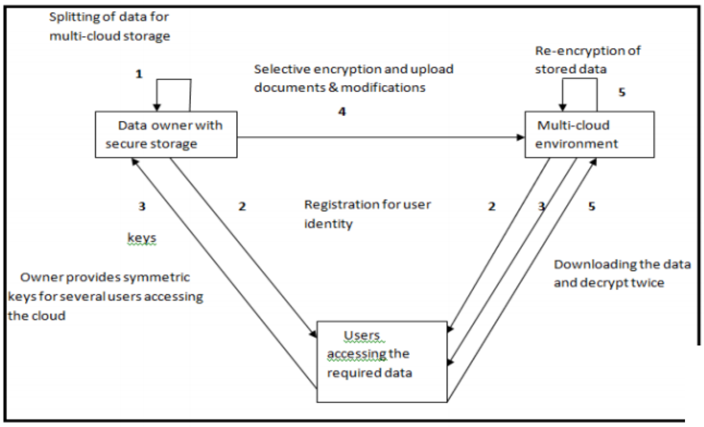
Splitting of data for multi-cloud storage
1
Selective encryption and upload documents & modifications
4
Re-encryption of stored data
5
Data owner with secure storage
Multi-cloud environment
3
keys
2
Registration for user identity
2
3
5
Owner provides symmetric keys for several users accessing the cloud
Downloading the data and decrypt twice
Users accessing the required data

Fig 6 Session of Client Authentication

Identity token registration: Users register their identity tokens in order to obtain secrets to decrypt the data that they are allowed to access.

Data encryption and uploading: The Owner encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the keygen algorithm and the remaining sub ACPs to the Cloud.

Data downloading and decryption:

Users download encrypted statistics from the Cloud and decrypt the information the usage of the derived keys. The customers decrypt the facts twice.

Information Coloring and software Watermarking in cloud computing provides the use of shared files and datasets, an adversary could compromise privacy, security, and copyright in a cloud computing environment.

Deyi Li and his colleagues propose The trust model which offers a second order fuzzy membership function for protecting data owners[13]. We extend this model to add unique data colors to protect large datasets in the cloud.

We consider cloud security a community property. To guard it, we combine the advantages of secured cloud storage and software watermarking through data coloring and trust negotiation.

Figure 7 illustrates the data coloring concept. The woman's image is the data object being protected. Figure 7 shows the forward and backward color-generation processes. We add the cloud drops (data colors) into the input photo (left) and remove color to restore the original photo (right).

The coloring process makes use of 3 records characteristics to generate the shade: the expected price (Ex) relies upon at the facts content, whereas entropy (En) and hyper entropy (He) add randomness or uncertainty, which are unbiased of the facts content material and acknowledged only to the statistics owner. Collectively, those 3 functions generate a collection of cloud drops to shape a unique "colour" to those providers or other cloud users can't discover. We can use records coloring at various security stages based on variable cost function applied. We can apply the method to protect documents, images, video, software, and relational databases. The color-matching process assures that colors applied to user identification match the data colors. This can initiate various trust-management events, including authentication and authorization. Virtual storage supports color generation, embedding, and extraction.

Combining secure data storage and data coloring, we can prevent data objects from being damaged, stolen, altered, or deleted. The computational complexity of the three data characteristics is much lower than that performed in conventional encryption and decryption calculations in PKI services.

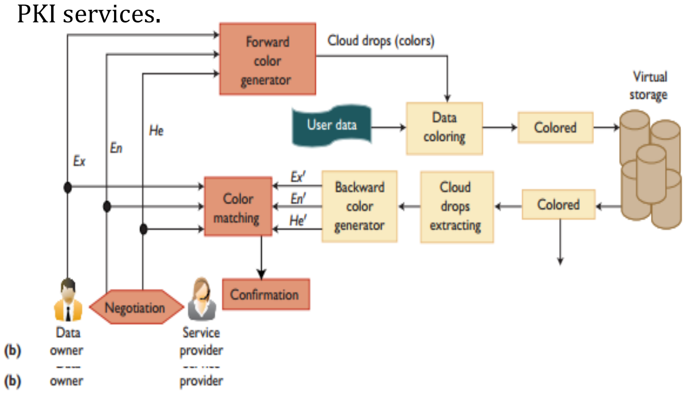

Fig 7.Details involved in the color-matching process

The watermark based scheme incurs a totally low overhead within the coloring and decoloring tactics. The En and He capabilities' randomness ensures records owner privateness. These characteristics can uniquely distinguish distinctive statistics objects

AES comprises three block ciphers, AES-128, AES-192 and AES-256. each cipher encrypts and decrypts records in blocks of 128 bits the use of cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to address extra block sizes and key lengths, however the functionality changed into not followed in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must realize and use the equal mystery key All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

We proposed a high-ability records-hiding scheme for binary pictures authentication based totally at the interlaced morphological binary wavelet transforms. the relationship between the coefficients received from exclusive transforms is applied to become aware of the perfect places for watermark embedding such that blind watermark extraction may be done.

Processing cases that are not intersected with each other are employed for orthogonal embedding in this sort of manner that now not best can the potential be considerably improved, but the visible distortion also can be minimized. outcomes of comparative experiments with different methods improve the existing scheme's superiority in being able to gain larger capacity at the same time as preserving suitable visible distortion and coffee computational price.

The goal of authentication is to ensure that a given set of records comes from a legitimate sender and the content integrity is preserved .hard authentication rejects any amendment made to a multimedia signal, while gentle authentication differentiates legitimate processing from malicious tampering this paper focuses on tough authenticator watermark-based totally authentication.

Specifically, we investigate the problem of data hiding for binary images in morphological transform domain. Generally speaking, data hiding in real-valued transform domain does not work well for binary images due to the quantization errors introduced in the pre/post-processing In addition; embedding data using real-valued coefficients requires more memory space. The idea of designing an interlaced transform to identify the embeddable locations is motivated by the fact that some transition information is lost during the computation of a single transform and there is a need to keep track of transitions between two and three pixels for binary images data hiding. Specifically, we process the images based on 2 2 pixel blocks and combine two different processing cases that the flip ability conditions of one are not affected by flipping the candidates of another for data embedding, namely “orthogonal embedding”.

```
For a = 1 to j do
    $hk_a$ = hash(k,r,p)
    f=$hk_a$ mod g
    $r_a \longrightarrow G_k$
End For
For f =1 to g do
    sort tuples in $G_k$ according to their primary key
    Embed watermarks to all tuples in $G_k$
End for
```

Embedding Watermarking algorithm

```
For m =  1 to x do
    $b^{m}{}_{1}$ = XOR(f,$r_1.B_m$,$r_2.B_m$.......$r_v.B_m$)
    // exclude the least 2 significant bits of all values
    $Z^{m}{}_{1}$=extractbits($b^{m}{}_{1}$,v)
    For j = 1 to v do
        $Z^{m}{}_{1}(j) \longrightarrow$ least significant bit of $r_j.B_{P(j)}$
    End for
End for
For j = 1 to v do
    $b^{j}{}_{2}$ = hash(f, ,$r_1.B_m$,r2.$B_m$.......$r_j.B_m$)
    // exclude the least 2 significant bits of all values
    $Z^{m}{}_{2}$=extractbits(bm$_2$,v)
    For m = 1 to x do
        $Z^{m}{}_{2}(m) \longrightarrow$ next least significant bit of rj.$B_m$
    End for
End for
```

Data encryption method

```
For m =  1 to x do
    : $b^{m}{}_{1}$ = XOR(f,$r_1.B_m$,$r_2.B_m$.......$r_v.B_m$)
    // exclude the least 2 significant bits of all values
    $Z^{m}{}_{1}$=extractbits($b^{m}{}_{1}$,v)
    For j = 1 to v do
        $Z^{m}{}_{1(j)} \longleftarrow$least significant bit of $r_j.B_{P(j)}$
    End for
    if $Z^{m*}{}_{1} \neq Z^{m}{}_{1}$ then $V^{m}{}_{1}$= false
    Else $V^{m}{}_{1}$= true
    End if
End for
For m =  1 to x do
    If ($V^{m}{}_{1}$= false) and ($V^{p(m)}$= false)
    end if
end for
For j = 1 to v do
    $b^{m}{}_{2}$ = hash(f, ,$r_1.B_m$,$r_2.B_m$.......$r_j.B_m$)
    // exclude the least 2 significant bits of all values
    $Z^{m}{}_{2}$=extractbits($b^{m}{}_{2}$,v)
    For m = 1 to x do
        Zm1(j)$\longleftarrow$ next least significant bit of rj.B(j)
    End for
    if $Z^{m*}{}_{2} \neq Z^{m}{}_{2}$ then $V^{m}{}_{2}$= false else $V^{m}{}_{2}$= true
    End if
End for
```

Data Decryption method

4. RESULT:

This table 1 s show the comparison of existing and proposed method accuracy and time period based we calculated the values ,each node and data storage fast and upload and download based the accuracy and time period calculated .

Table -1: Comparison of existing and proposed method accuracy and time period

S.NO	ALGORITHM	ACCURACY	TIME PERIOD
1	CSP	98.3	3.4
2	AES	92.3	2.2
3	EAES watermark	97.6	1.3

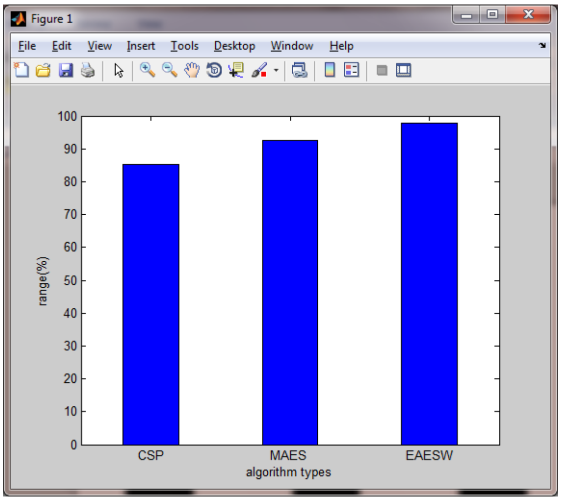

Chart -1 : Accuracy comparison of algorithms based on their percentage of range for data storage in clouds

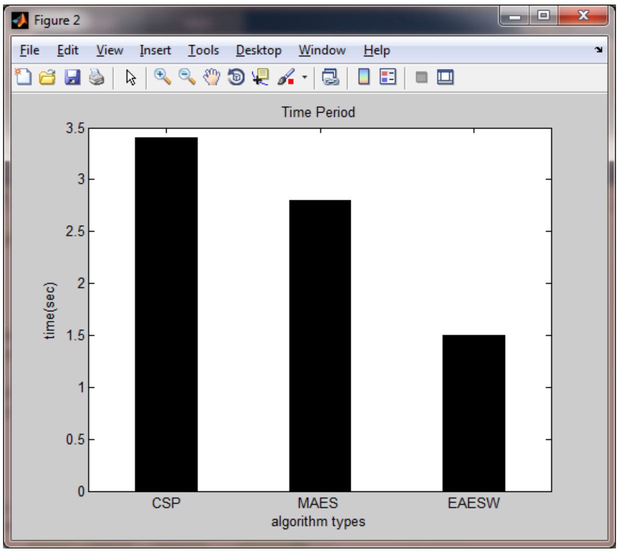

Chart -2. Accuracy comparison of algorithms based on time period for data storage in clouds

5. CONCLUSIONS

One of the core services furnished by using cloud computing is data garage. This poses new challenges in creating relaxed and dependable statistics storage and gets admission to centers over faraway service vendors inside the cloud The security of data storage is one of the necessary tasks to be addressed before the blueprint for cloud computing is accepted. We present a completely unique method for privacy maintaining of records garage in multi-cloud surroundings. It also provides numerous advancements in cloud computing because of its technical capabilities. The feature work might also contain load-balancing in multi-cloud environment for maximum garage and accuracy for diverse customers. Cloud computing is a growing paradigm as an allowing generation to supply on-call for and elastic storage and computing talents, while getting rid of the possession need for hardware. but numerous privacy and protection act demand strong protection of the cloud users, which in turn increases the complexity to expand privacy-maintaining cloud offerings. The privateness retaining the use of delegated get entry to control in multi-cloud promises the critical competencies required for a sturdy, value-powerful, and at ease cloud security implementation.

We proposed a delicate watermarking scheme for relational databases. The watermarks are embedded right into a relational database at the group basis under the control of a secure embedding key. The embedded watermarks form a watermark grid which can detect and localize any modifications made to the database and also be able to recover true data from modified cells. Experimental consequences confirmed that proposed scheme is cozy and proper information healing failure chance could be very teeny. Security analysis confirmed that it's far very hard for an attacker to regulate the database without affecting the embedded watermarks, and the safety upper sure turned into given. destiny work will attention on designing a watermarking scheme which could embed watermarks to non-numeric attributes. For this motive we are able to choose two answers. the primary answer is to reform the shape of hash function so it is able to be given non numeric inputs. The second one answer would be another mechanism as opposed to using a hash functions.

REFERENCES

[1] [1] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEE International Conference on Information Reuse and Integration (IRI), 2012.

[2] [2] Rakshit, A. , et. Al, "Cloud Security Issues", 2009, IEEE International Conference on Services Computing

[3] [3] M.S.B. Pridviraju et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5206 – 5209

[4] [4] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," ACM Trans. Inf. Syst. Secur., vol. 5, no. 3, pp. 290–331, 2002.

[5] [5] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in VLDB '2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment, 2003, pp. 898–909.

[6] [6] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy- preserving approach to policy-based content dissemination," in ICDE '10: Proceedings of the 2010

IEEE 26th International Conference on Data Engineering, 2010.

[7] [7] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy reencryption with delegating capabilities," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09. New York, NY, USA: ACM, 2009, pp. 276–286.

[8] [8] C.-K. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng, "Con- ditional proxy broadcast re-encryption," in Proceedings of the 14th Australasian Conference on Information Security and Privacy, 2009, pp. 327–342.

[9] [9] J.-M. Do, Y.-J. Song, and N. Park, "Attribute based proxy reencryption for data confidentiality in cloud computing environments," in Proceedings of the 1st International Conference on Computers, Networks, Systems and Industrial Engineering. Los Alamitos, CA, USA: IEEE Computer Society, 2011, pp. 248–251.

[10] [10] L. Bussard, G. Neven and F.S. Preiss, "Downstream Usage Control," In proceedings of 2010 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 22-29, 2010.

[11] [11].K. Hwang, G. Fox, and J. Dongarra, Distributed Systems and Cloud Computing: Clusters, Grids/P2P, and Internet Clouds, Morgan Kaufmann, to appear, 2010.

[12] [12]. K. Hwang, S. Kulkarni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," IEEE Int'l Conf. Dependable, Autonomic, and Secure Computing (DASC 09), IEEE CS Press, 2009.

[13] [13]. J. Nick, "Journey to the Private Cloud: Security and Compliance," tech. presentation, EMC, Tsinghua Univ., 25 May 2010.

[14] [14]. S. Song et al., "Trusted P2P Transactions with Fuzzy Reputation Aggregation," IEEE Internet Computing, vol. 9, no. 6, 2005, pp. 24–34.

[15] [15]. "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, Apr. 2009; www. cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.

[16] [16]. T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.

[17] [17]. J. Rittinghouse and J. Ransome, Cloud Computing: Implementation, Management and Security, CRC Publisher, 2010.

[18] [18]. X. Lou and K. Hwang, "Collusive Piracy Prevention in P2P Content Delivery Networks," IEEE Trans. Computers, July 2009, pp. 970–983.

[19] [19]. C. Clark et al., "Live Migration of Virtual Machines," Proc. Symp. Networked Systems Design and Implementation, 2005, pp. 273–286.

[20] [20]. L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Trans. Knowledge and Data Eng., July 2004, pp. 843–857.

[21] [21]. R. Zhou, and K. Hwang, "Power Trust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, Apr. 2007, pp. 460–473.

[22] [22]. C. Collberg and C. Thomborson, "Watermarking, Tamper-Proofing, and Obfuscation-Tools for Software Protection," IEEE Trans. Software Eng., vol. 28, 2002, pp. 735–746.

[23] [23]. D. Li, C. Liu, and W. Gan, "A New Cognitive Model: Cloud Model," Int'l J. Intelligent Systems, Mar. 2009, pp. 357–375. 14. D. Li and Y. Du, Artificial Intelligence with Uncertainty, Chapman & Hall, 2008.

[24] [24] Masayuki Okuhara et al, "Security Architecture for Cloud Computing", FUJITSU Sci. Tech. J., Vol. 46, No. 4, pp. 397-402 (October 2010).

[25] [25] Sun Microsystems, Inc., "Introduction to Cloud Computing Architecture", White Paper, 1st Edition, June 2009

[26] [26] Gerald Kaefer, "Cloud Computing Architecture", Corporate Research and Technologies, Munich, Germany, Siemens AG 2010, Corporate Technology.

[27] [27] Peter Tseronis, "Cloud Computing Overview: A Federal Government and Agency Perspective", Architecture Plus Seminar -Cloud Computing, Web 2.0 and Beyond: A Vision of Future Government Operations, August 13, 2009

[28] [28] Kangchan Lee, "Cloud Computing", Vice Chairman of ITU-T FG Cloud Chairman of Mobile Cloud WG in CCF in Korea, ETRI.

[29] [29] VeriSign, "Digital ID, A Brief Overview", A VeriSign White Paper, 2004 VeriSign, http://www.verisign.com/static/005

BIOGRAPHIES

Mr. MansoorAhamad, Currently pursuing Mphil research scholar, Department of Computer Science, CMS college of science and commerce-Coimbatore. E-mail: mansoorahamad7@gmail.com

B.Karuppusamy, Assistant Professor, Department of Computer Science, CMS College of science and commerce. Coimbatore – 641 049. Email: bkaruppusamy@rediffmail.com