International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 15th Jun 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-07

Title: CP-ABE :CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION DATA ACCESS CONTROL FOR CLOUD STORAGE

Volume 08, Issue 07, Pages: 143–155.

Paper Authors

B.NAGARANI ,P. SRILAXMI, A. LASMIKA

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CP-ABE :CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION DATA ACCESS CONTROL FOR CLOUD STORAGE

B.NAGARANI ,P. SRILAXMI, A. LASMIKA
[1,2] Dept of ECE, SV University, Tirupati, AP, India.
[3]PhD Scholar, Dr. MGR Educational and Research Institute, Tamilnadu.
srilakshmi.kalikanda@gmail.com, samu09.sam@gmail.com, anumolu.lasmika@gmail.com

Abstract—Secure cloud garage, which is an rising cloud carrier, is designed to guard the confidentiality of outsourced facts but also to offer flexible facts access for cloud users whose facts is out of bodily manage. Cipher text-Policy Attribute-Based Encryption (CP-ABE) is seemed as one of the maximum promising techniques that may be leveraged to comfortable the assure of the service. However, the use of CP-ABE may also yield an inevitable safety breach that's referred to as the misuse of get admission to credential (i.e. Decryption rights), because of the intrinsic "all-or-not anything" decryption feature of CP-ABE. In this paper, we look into the two principal cases of get right of entry to credential misuse: one is on the semi-trusted authority aspect, and the other is at the facet of cloud user. To mitigate the misuse, we propose the first responsible authority and revocable CP-ABE based cloud storage machine with white-field traceability and auditing, called crypto cloud. We additionally present the security evaluation and similarly exhibit the software of our system through experiments.

Index Terms—Secure Cloud Storage, Cipher text-Policy Attribute-Based Encryption, Access Credentials Misuse, Traceability and Revocation, Auditing.

1 INTRODUCTION

THE occurrence of cloud computing might also indirectly incur vulnerability to the confidentiality of outsourced information and the privateness of cloud users. A unique assignment here is on the way to assure that handiest legal users can gain get right of entry to to the information, which has been outsourced to cloud, at anywhere and whenever [3]. One naive solution is to hire encryption approach on the information previous to uploading to cloud. However, the answer limits further information sharing and processing. This is so due to the fact a facts proprietor wishes to download the encrypted records from cloud and similarly re-encrypt them for sharing (assume the statistics proprietor has no neighborhood copies of the data). A satisfactory-grained access manage over encrypted statistics is appropriate inside the context of cloud computing [11].

Ciphertext-Policy Attribute-Based Encryption (CPABE) [11] can be an powerful way to guarantee the confidentiality of statistics and provide high-quality-grained get admission to manage here. In a CP-ABE based cloud garage machine, as an instance, corporations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty individuals and travelling pupils of

the college) can first specify get admission to coverage over attributes of a ability cloud user. Authorized cloud customers then are granted get right of entry to credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., scholar function, college member role, or visitor position), which can be used to gain get entry to the outsourced records. As a sturdy one-to-many encryption mechanism, CP-ABE offers a reliable approach to guard statistics saved in cloud, but also enables high-quality-grained get admission to manipulate over the statistics.Generally talking, the present CP-ABE based cloud garage structures fail to keep in mind the case in which get entry to credential is misused. For instance, a college deploys a CPABE based cloud garage system to outsource encrypted pupil facts to cloud beneath a few get admission to guidelines which can be compliant with the applicable facts sharing and privacy regulation (e.g., the federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act of 1992 (HIPAA)). The legitimate in fee on the business enterprise (e.g. College's protection supervisor) initializes the machine parameters and problems access credentials for all users (e.g., students, school individuals, and visiting students). Each employee is assigned with several attributes (e.G., "administrator", "senior manager", "economic officer", "tenured school", "tenure-track school", "non tenure-song school", "instructors", "adjunct", "traveller", and/or "college students"). Only the employees with attributes gratifying the decryption policy of the outsourced information are able to gain get right of entry to to the student information stored in cloud (e.g. Student admission materials).As we may additionally have known, the leakage of any touchy student information saved in cloud ought to bring about a variety of effects for the company and individuals (e.g., litigation, loss of competitive gain, and crook charges). The CP-ABE may additionally assist us prevent safety breach from outdoor attackers. But while an insider of the organization is suspected to dedicate the "crimes" related to the redistribution of decryption rights and the circulate of student records in plain layout for illicit monetary gains, how ought to we conclusively decide that the insider Is responsible? Is it also feasible for us to revoke the compromised get entry to privileges? In addition to the above questions, we have one more which is related to key technology authority. A cloud person's get right of entry to credential (i.E., decryption key) is typically issued via a semi-relied on authority based at the attributes the consumer possesses. How may want to we assure that this precise authority will not (re-)distribute the generated get entry to credentials to others? For instance, the organization safety official leaks a lecturer Alice's key to an interloper Bob (who is not the worker of the college). One potential answer to the question is to appoint multiple authorities. Nevertheless, this incurs extra cost in communication and infrastructure deployment and meanwhile, the hassle of malicious collusion amongst authorities remains. Therefore, we posit that adopting an accountable authority technique to mitigate the get right of entry to credential escrow problem is the preferred method.

Seeking to mitigate get admission to credential misuse, we advocate CryptCloud+, an accountable authority and revocable CPABE based cloud storage machine with white-container traceability and auditing. To the excellent of our know-how, this is the first practical approach to at ease satisfactory-grained access control over encrypted information in cloud. Specifically, in our paintings, we first present a CP-ABE based totally cloud garage framework.Using this (time-honored) framework, we endorse two responsible authority and revocable CP-ABE structures (with white box traceability and auditing) which are fully comfy within the standard model, referred to as ATER-CP-ABE and ATIR-CPABE, respectively. Based on the two systems, we gift the creation of CryptCloud that provides the subsequent capabilities.

1) Traceability of malicious cloud users. Users who leak their get admission to credentials may be traced and diagnosed.

2) Accountable authority. A semi-relied on authority, who (with outright authorization) generates and further distributes get admission to credentials to unauthorized user(s), may be diagnosed. This lets in addition movements to be undertaken (e.g. Criminal investigation or civil litigation for damages and breach of settlement).

3) Auditing. An auditor can decide if a (suspected) cloud person is guilty in leaking his/her get right of entry to credential.

4) "Almost" zero storage requirement for tracing. We use a Paillier-like encryption as an extractable dedication in tracing malicious cloud users and more almost, we do no longer want to maintain an identity desk of users for tracing (not like the technique utilized in [7]).

5) Malicious cloud users revocation. Access credentials for person traced and similarly decided to be "compromised" may be revoked. We design two mechanisms to revoke the "traitor(s)" effectively.

The ATER-CP-ABE provides an explicitly revocation mechanism wherein a revocation listing is precise explicitly into the set of rules Encrypt, whilst the ATIRCP- ABE offers an implicitly revocation wherein the encryption does now not need to realize the revocation list however a key replace operation is needed periodically.

This paper extends our in advance paintings (a conference version in [3]), as follows.

1) We gift a proper framework version of the proposed machine, designed for realistic cloud garage machine deployment.

2) We deal with a weak point inside the auditing technique of the conference version. Specifically, a malicious consumer might also change t id of his secret key in the convention model, and the auditing procedure will fail on this case. As a mitigation, we revise the important thing technology set of rules and add an audit listing to come across if the t id is changed.

3) We beautify the capability of the development (W.R.T. AAT-CP-ABE) proposed inside the convention model and in addition present more desirable constructions, specifically ATER-CP-ABE and ATIR-CP-ABE.

These constructions permit us to effectively revoke the malicious customers explicitly or implicitly. We additionally present the brand new definitions, approach and related materials of ATER-CP-ABE and ATIR-CP-ABE.

4) Based on the brand new ATER-CP-ABE and ATIR-CPABE, we present CryptCloud+ which is an effective and sensible solution for at ease cloud storage.

5) We provide fashionable extensions (of our device) on the large universe, the multi-use, and the prime-order setting instances, in order that the solution added in this paper is more scalable in actual-international packages.

6) We comprehensively compare the performance of the proposed ATER-CP-ABE and ATIR-CP-ABE thru experiments.

Organization. In Section 2, we are able to gift associated paintings and describe our underlying technique. Section 3 outlines our framework version and design purpose. Section four provides the history understanding. In Sections five and 6, we outline ATER-CP-ABE and ATIR-CP-ABE, previous to imparting their buildings and security analysis in Sections 7 and eight. Section nine affords the proposed CryptCloud+, a comparative precis, and opinions.

2 RESEARCH WORK AND OUR APPROACH

2.1 Related Work

Cloud storage explores new programs of data storage, in order that statistics proprietor does take full obligation of statistics management “in nearby” no more [43]. However, because of the separation of information possession and records get right of entry to in cloud putting [4], the control of information, software program, bodily machines and structures need to be delegated to cloud provider carriers, in order that records proprietor handiest maintains little manipulate on digital machines [2], [6].

To guard the confidentiality of cloud facts, many cloud based fine-grained get admission to manage systems were introduced inside the literature [1], [2], [5], [4], [7]. Searchable encryption allows at ease seek over ciphertexts via using the pre-described keywords [2]. The records audit and deduplication enables customers to test the integrity of the outsourced information [53] and to take away storage redundancy [8].Cloud storage is also regarded as an excellent mixture with Internet of Things (IoT) [8], [6], [4]. This is because The cloud may provide considerable storage and computational assets for the devices of IoT (e.g., in e-fitness networks [5], [5] and vehicular DTN networks [6]) which are commonly resource constrained. However, this combination yields safety and privateness challenges.In the context of Attribute-Based Encryption (ABE), Sahai and Waters [4] to start with introduce the belief of ABE, that is sooner or later formalized by Goyal et al. [5]. Specifically, Goyal et al. Outline Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-BasedEncryption (CP-ABE). Since then, quite a number ABE schemes were proposed in the literature [9], [8], [1], [3], [7], [2]. While these schemes are designed to acquire higher efficiency, expressiveness and

protection, they do now not deal with traceability and revocation issues.

Li et al. Introduce the belief of responsible CP-ABE [3] to prevent unauthorized key distribution among colluded customers. In a later paintings [2], a consumer accountable multi-authority CP-ABE gadget is proposed. Liu et al. Also proposed white-field [7] and black-container [6] traceability 1 CP-ABE structures helping coverage expressiveness in any monotone access systems. Ning et al. [3], [2], [4], [6] recommend several practical CP-ABE systems with white-box traceability and black-container traceability. Deng et al. [11] provide a tracing mechanism of CP-ABE to discover the leaked access credentials in cloud garage system.A wide variety of attribute revocation solutions for CP-ABE systems have also been proposed within the literature, such as [2]. Sahai et al. [4] outline the hassle of revocable storage and provide a completely at ease production for ABE based on ciphertext delegation. Yang et al. [9] advise a revocable multi-authority CP-ABE gadget that achieves both ahead and backward protection. More these days, Yang et al. [5] recommend an attribute updating technique to achieve the dynamic alternate on attribute (inclusive of revoking preceding characteristic and re-granting formerly revoked attribute).However, the aforementioned research works do now not take into account the misbehavior of key generation authority, the feasibility of auditing, and the revocation (of misbehaver). These are the problems that we target to deal with on this paper.

2.2 Our Approach An overview of the technique we use to recognise the traceability of malicious cloud users, responsible authority, auditing and malicious cloud customers revocation is briefly brought beneath (please see Sections 7 and eight for more technical information).As previously mentioned, to hint malicious cloud users leaking get admission to credentials, we use a Paillier-like encryption [8] as an extractable commitment to gain white-field traceability. Specifically, the extractable commitment allows us to dedicate the identity of a consumer while he/she requests for access credential. The commitment is seemed as a part of the credential. Due to the hiding and binding approach Of the Paillier-like extractable commitment, a person cannot reveal and in addition “adjust” the identity that is “encoded” in the credential. The set of rules Trace permits us to use a trapdoor for the commitment to get better the user’s identity from the corresponding credential. We statement that the get admission to credential wishes to perform an get entry to credential sanity take a look at (i.e., using the important thing sanity take a look at algorithm) previous to the tracing step. The get entry to credential sanity test is a deterministic algorithm [3], [4], that is used to determine if the credential is well formed throughout decryption. Leveraging the commitment, we will no need to hold an identity desk, which is in contrast to the approach added in [7]. This lets in us to “reduce” extra storage cost for tracing.In order to achieve responsible authority, an get right of entry to credential is together determined by means of each the authority and the corresponding user. This prevents the authority from having “absolute”

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

manage over the credential. The consumer is allowed to attain the credential uac (consistent with his/her attributes and identification) from the authority by means of the usage of a comfortable get admission to credential technology protocol. But the authority does not understand which get entry to credential the user obtains. If the authority (re-)distributes the credential u~ac belonging to the registered user (with get right of entry to credential uac) with none permission of the user, with all however a negligible probability, u~ac will range from uac that the consumer holds. The access credential pair (uac; u~ac) will form a cryptographic proof of the misbehavior of the authority. We be aware that the similar method also can be used to enable an auditor to decide if a consumer accused of credential leak is guilty. We expect that the auditor should be honest and credible (e.g., an external KPMG or PwC). We offer two effective revocation mechanisms to revoke the malicious customers explicitly or implicitly, inspired through [4], [9]. For express revocation, we specify a revocation listing RL explicitly into the algorithm Encrypt. During the execution of the algorithm KeyGen, the grasp secret key is cut up into parts: one for get admission to control and the different for revocation. For malicious customers who are in RL, they'll fail to decrypt any new cipher text as the sub master mystery key similar to revocation part can not be canceled out in decryption. For implicit revocation, the Encrypt operation does not want to understand the revocation listing. Instead, an algorithm KeyUpdate periodically problems the update key for all non-revoked customers. We hire a (random secret) first diploma polynomial (i.e., f(w) = Øw+α) and f(1); f(t) to share the master secret key between the name of the game key and the update key, wherein f(1) is used for access control and f(t) is for revocation. For malicious users who're in RL, considering that they cannot reap the update keys, they cannot decrypt any new cipher text. The property of revocability is completed by combining the traceability and the revocation mechanisms described above. Specifically, the traceability mechanism ensures that when a user is recognized malicious (i.e. Leaking credential), his/her identification might be placed in a revocation list. By the usage of the specific and implicit revocation strategies we added with the revocation listing, we make certain that any "new" ciphertext can't be decrypted with the aid of the "revoked" users

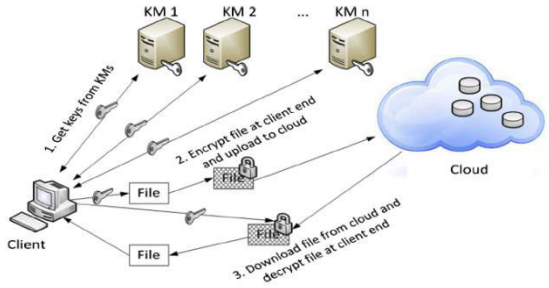

Fig. 1 CP-ABE based cloud storage system

3 FRAMEWORK MODEL AND DESIGN GOAL

Fig. 1 describes our CP-ABE primarily based cloud garage gadget, with the following key entities:

Data owners (DOs) encrypt their information below the applicable get admission to policies prior to outsourcing the (encrypted) data to a public cloud (PC).

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

PC shops the outsourced (encrypted) information from Dos and handles information get entry to requests from data customers (DUs)

Authorized DUs are able to get entry to (e.G. Down load and decrypt) the outsourced records.

Semi-relied on authority (AT) generates system parameters and issues get admission to credentials (i.E., decryption keys) to DUs.

Auditor (AU) is depended on by way of other entities, takes price of audit and revoke approaches, and returns the trace and audit outcomes to DOs and DUs.

The PC is sincere-but-curious inside the sense that it is able to curiously acquire greater data approximately the outsourced (encrypted) facts however will not deviate from the specification (i.e. Efficaciously executing obligations assigned via DOs). AT is semitrustedinside the experience that it can (re)distribute get right of entry to credentials to individuals who are unauthorized but generate gadget parameters (to be shared with AU) honestly. A fully depended on AU continues a duplicate of the system parameters shared by way of AT.DOs encrypt their statistics to save you unauthorized access. Authorized DUs can also deliberately leak their access credentials, which includes selling credentials to a 3rd-birthday party. In exercise, get admission to credentials are possibly to attract capability buyers (in black market), and the system traitors (selling the credentials) might also by no means had been stuck. For simplicity, we assume DOs ought to decide that their outsourced information were abnormally accessed, and the trace method could in addition get right of entry to the leaked get admission to credentials. Our purpose is to endorse an responsible authority and revocable CryptCloud with white-field traceability and auditing to gain the following requirements:

1) Security ensures have to be supplied – defensive the confidentiality of the statistics and the ability of get entry to control over encrypted statistics;
2) Computation have to be cost-effective – minimizing the computation value spent on hint and revocability; and
3) Audit, hint and revoke tactics need to be efficient - shortening the time in catching a device betrayer.

4.Terminologies for Binary Tree

Let L = {1…….f1)D be the sets of leaves and nodes for a whole binary tree, respectively. For a leaf l 2 L, Path(l) D denotes the set of all nodes on the path from node l to the foundation (which includes l and the basis). For RL L, we define Cover(RL) D as follows: (1) Mark all nodes in Path(l) for all l 2 RL. (2) Set Cover(RL) because the set of all unmarked youngsters of the marked nodes. It may be proven to be the minimal set that carries no node in Path(l) for l 2 RL but consists of at the least one node in Path(l) for l =2 RL. It is thought that jCover(RL)j jRLj(log(f=jRj) + 1) [4], [29].

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

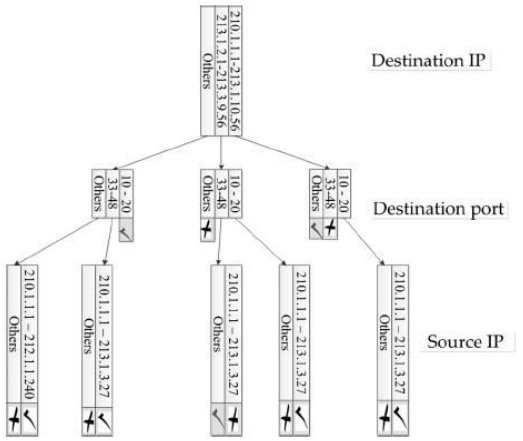

Fig. 3. Design of tree-rule firewall using IP address and port ranges

5 THE MODEL OF ATER-CP-ABE

5.1 Definition

An Accountable Authority and Explicitly Revocable CPABE with White-Box Traceability and Auditing (ATER-CPABE) is a CP-ABE scheme this is capable of keep the misbehaving authority responsible, to hint malicious user via given decryption key, to decide whether or not the suspect is guilty, and to explicitly revoke malicious person. We revise the algorithms Setup, Encrypt and Decrypt presented in the convention model [5] by means of together with a revocation listing to reap the revocation of malicious user explicitly. We will now describe our ATER-CP-ABE scheme, which consists of the following algorithms:

Setup(; U) ! (pp; msk): On enter a safety parameter and the characteristic universe description U, it outputs the public parameters pp and the master secret key msk. It also initializes an empty revocation list RL.

KeyGen(pp; msk; identification; S) ! Skid;S: This is an interactive protocol among AT and a consumer U. Common inputs to both AT and U are pp and a fixed of attributes S for a consumer with identity id. The non-public input to AT is msk. In additional, AT and U can also use a chain of random coin tosses as private enter. At the quit of the protocol execution, U is issued a secret key skid;S similar to id and S. Encrypt(pp; m;A;RL) ! Ct: On enter pp, a plaintext message m, an access structure A over the universe of attributes, and a revocation listing RL, it outputs a ciphertext..

Decrypt(pp; skid;S; ct) ! M or ?: On input pp, a mystery key skid;S, and a ciphertext ct, it outputs the plaintext m if the characteristic set S of sk satisfies the access shape of ct and identification =2 RL. Otherwise, it out puts ?.

KeySanityCheck(pp; sk) ! 1 or 0: On input pp and a secret key sk, it outputs 1 if sk passes the important thing sanity check. Otherwise, it outputs zero. The key sanity test is a deterministic set of rules [13], [14], that is used to guarantee that the secret key is properly-formed within the decryption manner.

Trace(pp; msk; sk) ! Identity or input pp, msk and a mystery key sk, it first assessments whether or not sk is properly-formed which will similarly determine whether or not sk wishes to be traced. A mystery key sk described as wellformed if KeySanityCheck(pp; sk) ! 1. For a wellformed sk, it extracts the identification from sk. It then outputs an identity with

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

which the sk friends, and places it inside the revocation list RL. Otherwise, it outputs a symbol now not want to be traced.

Audit(pp; skid; sk identification) ! Guilty or harmless: This is an interactive protocol among U and AU to decide whether or not a user is responsible or harmless.

5.2 Security

The ATER-CP-ABE scheme is cozy if the subsequent 3 requirements are glad.

1) It should satisfy the usual semantic safety belief for CP-ABE, particularly: ciphertext in distinguishability below chosen plaintext attacks (IND-CPA).

2) It is intractable for the authority to create a decryption key sk such that the set of rules Trace (taking sk as enter) outputs an identity id and the algorithm Audit (taking identity as input) comes to a decision that the corresponding consumer is guilty.

3) It is infeasible for a consumer to create a decryption key such that the set of rules Audit suggests that the user is harmless.

The Key Sanity Check game. As of [36], the Key Sanity Check game for ATER-CP-ABE is defined by the following game between an attacker and a simulator. On input a security parameter _, a simulator invokes an attacker A on A returns the public parameters pp, a ciphertext ct and two different secret keys skid;S and s~kid;S corresponding to the same set of attribute S for a user with identity id. A wins the game if

(1) **KeySanityCheck**(pp; skid;S) !->1.
(2) **KeySanityCheck**(pp; s~kid;S) ->1.
(3) **Decrypt**(pp; skid;S; ct) 6=?.
(4) **Decrypt**(pp; s~kid;S; ct) 6=?.
(5) **Decrypt**(pp; skid;S; ct) 6= **Decrypt**(pp; s~kid;S; ct).

The advantage of A in the above game is defined as Pr[A wins]. The intuition of "Key Sanity Check" is captured by combining the notion given in the above game and **KeySanityCheck** and **Decrypt** (defined in this section) [36].

6. THE PROPOSED CRYPTCLOUD

Based on ATER-CP-ABE and ATIR-CP-ABE, we recommend the Crypt Cloud+. The machine works as follows. AT first generates the machine parameters to setup the gadget and shares the whole machine parameters (including public and non-public parameters) with AU. It then publishes the public parameters. Also, AT generates get admission to credentials (i.e. Decryption keys) for DUs consistent with their identities and attributes.DOs encrypt their facts beneath get admission to policies (which might be chosen through themselves) after which outsource the encrypted records to PC. Any authorized DU is able to decrypt the outsourced ciphertexts to access to the underlying information. A DU is allowed if the set of attribute he/she possesses satisfies the get admission to policy defined over the outsourced information. At a few point, a valid get entry to credential may be offered on line, together with in an underground discussion board. As lengthy as the credential is placed or while a DO sends a hint request (when he/she unearths that his/her data have been changed or accessed by using others), AU calls the hint system to

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

perceive the traitor(s). If there exists a DU being recognized as the traitor but claims to be innocent, then AU may also name the audit system to make a in addition judgment. The malicious traitor can be revoked explicitly or implicitly next to the findings. Specifically, we allow and 0 be the ATERCP- ABE and the ATIR-CP-ABE schemes respectively. Letλ = f;0g, and our CryptCloud+ works as follows.

System Setup: AT setups the system. It runs (pp; msk) ->:Setup(λ; U) to generate device public parameter pp and grasp secret key msk. It shares pp and msk with AU, prior to publishing pp and keeping msk secret.

_ **Cloud User Enrollment**: After the request of a DU to join the system has been approved, the DU is assigned an unique identity id and an attribute set S which describes the DU. AT generates a secret access credential uac according to the identity id and attribute set S for the DU as follows. It calls skid;S _:**KeyGen**(pp; msk; id; S), sets the DU's secret access credential as uacid;S = skid;S and sends uacid;S to the DU.

_ **File Outsource**: A DO takes the following steps to outsource the data to the PC. The data is first encrypted under a symmetric encryption (e.g. AES) with a randomly chosen symmetric session key mskey 2 GT , and the resulting ciphertext is ct.

The DO then defines an access policy A (represented by an LSSS (A;) and encrypts the random chosen symmetric session key mskey by calling ctskey _:**Encrypt**(pp;mskey; (A; _); _) (where_ = fRL; xg). Finally, the outsourced file is formed as ctskeyjjct, where ctskey and ct are the header and the main body of the file, respectively.

_ **File Access**: When a DU requests an outsourced file, the PC returns the requested file ctskeyjjct to the DU. The DU calls mskey

_:**Decrypt**(pp; skid;S; ctskey) (using his/her secret access credential uacid;S = skid;S) to recover the symmetric session key mskey. The DU uses mskey to decrypt ct and obtains the mainbody of the file.

_ **Access Credential Update**: If the underlying construction is ATIR-CP-ABE 4, then the system needs to include an additional access credential update procedure. It calls skx;RL

_:**KeyUpdate**(pp; msk; x;RL), sets the update access credential for time period x as uacx;RL = skx;RL, and sends uacx;RL to all unrevoked DUs.

_ **Trace**: When AU finds a secret access credential uac is being sold online or receives a trace request from a DO, it runs id _:**Trace**(pp; msk; uac) to find out who the leaker is.

_ **Audit**: When a DU with identity id is traced as the leaker but claims innocence, it sends an audit request along with his/her access credential uacid to AU. Upon receiving the audit request, AU calls guilty or innocent

:**Audit**(pp; uacid; uac id) to determine whether the (accused) user is indeed innocent, where uac_ id is the leaked access credential.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

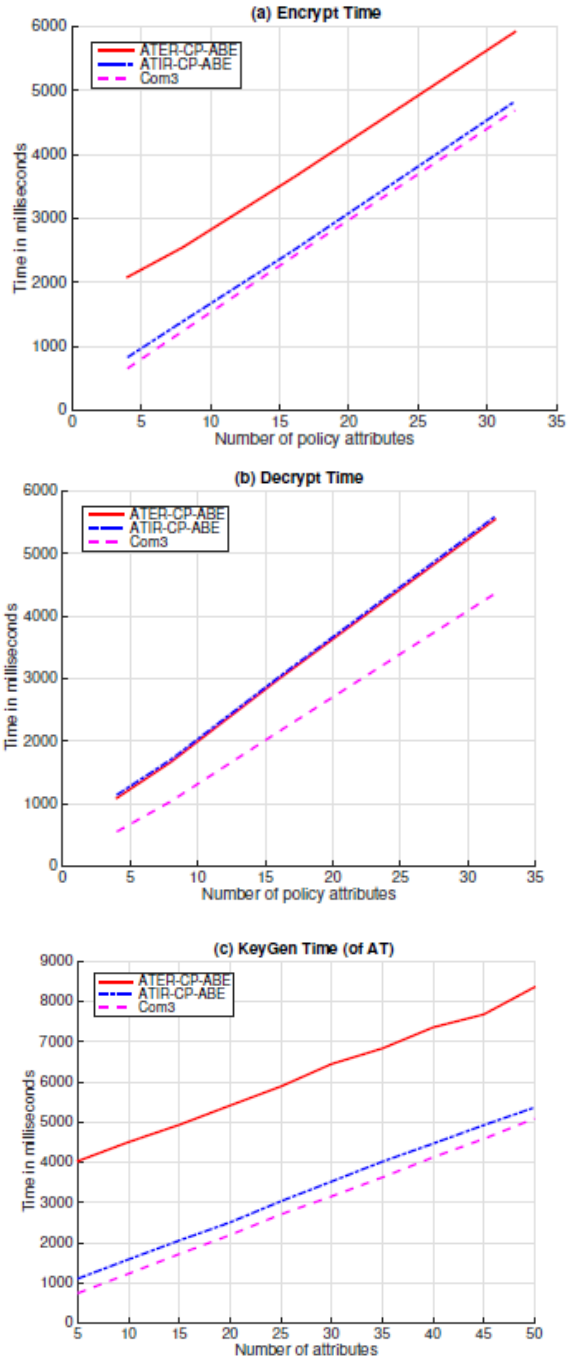

Fig:3 Experimental Results

7. CONCLUSION AND FUTURE WORK

In this paper, we've addressed the venture of credential leakage in CP-ABE primarily based cloud storage device via designing an accountable authority and revocable CryptCloud which supports white-box traceability and auditing (known as CryptCloud). This is the first CP-ABE based totally cloud garage device that simultaneously helps white-field traceability, responsible authority, auditing and effective revocation. Specifically, CryptCloud allows us to hint and revoke malicious cloud customers (leaking credentials). Our approach can be extensively utilized in the case wherein the users' credentials are redistributed with the aid of the semi-trusted authority. We word that we can also want black-container traceability, which is a stronger perception (in comparison to white-field traceability), in CryptCloud. One of our destiny works is to don't forget the black-field traceability and auditing. Furthermore, AU is assumed to be absolutely trusted in CryptCloud. However, in exercise, it may not be the case. Is there any manner to reduce trust from AU? Intuitively, one approach is to appoint a couple of AUs. This is comparable to the method used in threshold schemes. But it will require extra communication and deployment value and in the meantime, the hassle of collusion amongst AUs stays. Another potential approach is to appoint comfortable multi-birthday celebration computation in the presence of malicious adversaries. However, the performance is likewise a bottleneck. Designing efficient multi-celebration computation and decentralizing accept as true with amongst AUs (whilst maintaining the equal stage of security and efficiency) is likewise a part of our future paintings. We use Paillier-like encryption to serve as an extractable commitment to attain white-container traceability. From an abstract view factor,

any extractable dedication can be employed to attain white-container traceability in principle. To enhance the performance of tracing, we might also employ a greater mild-weight (pairing-suitable) extractable dedication.Also, the hint set of rules in CryptCloud+ desires to take the grasp mystery key as enter to attain white-box traceability of malicious cloud customers. Intuitively, the proposed CryptCloud+ is private traceable5. Private traceability best lets in the tracing algorithm to be run through the device administrator itself, even as partial/full public traceability permits the administrator, authorized users and even anybody with out the secret records of the gadget to meet the hint. Our destiny paintings will consist of extending CryptCloud+ to offer "partial" and completely public traceability with out compromising on performance.

REFERENCES

[1]. Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

[2]. Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3]. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4]. Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[5]. Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[6]. Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.

[7]. Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8]. Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.

[9]. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10]. Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.

[11]. Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching

my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.