OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Enhanced Privacy-Preserving Data Sharing Framework for Cloud Environments

BANDI OMUTYA PRABHA, D S K MAHALAKSMI[2]

#1. M.Tech Scholar in Department of Department of Artificial Intelligence & Data Science,
#2. Assistant Professor, Department of Artificial Intelligence & Data Science, Kakinada Institute Of Engineering & Technology or Women, AP, India.

Abstract—
Data sharing has never been simpler with the advances of cloud computing, and a precise investigation on the mutual data gives a variety of advantages to both the general public and people. Data sharing with countless must consider a few issues, including productivity, data respectability and security of data proprietor. Ring mark is a promising possibility to build a mysterious and bona fide data sharing framework. It enables a data proprietor to namelessly validate his data which can be put into the cloud for storage or investigation reason. However the exorbitant declaration confirmation in the conventional open key base setting turns into a bottleneck for this answer for be adaptable. Character based ring mark, which takes out the procedure of authentication check, can be utilized. In this paper, we further upgrade the security of ID-based ring mark by giving forward security: If a mystery key of any client has been endangered, all past produced marks that incorporate this client still stay substantial. This property is particularly vital to any substantial scale data sharing framework, as it is difficult to ask all data proprietors to authenticate their data regardless of whether a mystery key of one single client has been endangered. We give a solid and proficient instantiation of our plan, demonstrate its security and give an execution to demonstrate its reasonableness.

Keywords: *Access control, Key dissemination, Cloud computing, aggregate sharing, privacy preservation, shared authority, AES Algorithm.*

I. Introduction

Cloud services give incredible grounding to the clients to appreciate the on-request cloud applications without thinking about the neighborhood foundation restrictions. Amid the data getting to, various clients might be in a cooperative relationship, and in this manner data sharing winds up radiant to accomplish profitable advantages. The current security arrangements chiefly center around the verification to understand that a client's privative data can't be unapproved gotten to, yet disregard an unobtrusive protection issue amid a client testing the cloud server to ask for different clients for data sharing. The tested access ask for itself may uncover the client's protection regardless of whether or not it can get the data get to consents. A few schemes utilizing attribute-based encryption (SecCloud) have been proposed for access control of re-appropriated data in cloud computing. It empowers clients with restricted computational assets to re-appropriate their expansive calculation remaining tasks at hand to the cloud, and monetarily appreciate the huge computational power, transmission capacity, storage, and even suitable programming that can be partaken in a compensation for each utilization way. Regardless of the colossal advantages, security is the essential impediment that keeps the wide appropriation of this promising computing model, particularly for clients when their confidential data are expended and delivered amid the calculation. To battle against unapproved data spillage, delicate data must be encoded before re-appropriating to give end toend data confidentiality confirmation in the cloud and past. Notwithstanding, normal data encryption systems generally keep cloud from playing out any significant activity of the basic figure textpolicy, making the calculation over scrambled data a difficult issue. The proposed plan not just accomplishes versatility because of its progressive structure. Thus, there do exist different inspirations for cloud server to act unfaithfully and to return wrong outcomes, i.e., they may carry on past the established semi legitimate model.

II. Related Work

Shulan Wang et al. [1] proposed an enhanced twoparty key issuing convention that can ensure that neither key expert nor cloud service supplier can bargain the entire mystery key of a client exclusively. Additionally, creators present the idea of attribute with weight, being given to upgrade the declaration of attribute, which can not just stretch out the articulation from twofold to self-assertive state, yet in addition help the intricacy of access approach. Jianting Ning et al. [2] proposed another idea called auditable σ-time re-appropriated CP-ABE, which is accepted to be pertinent to cloud computing. According to their plan, costly blending activity acquired by decoding is offloaded to cloud and in the mean time, the rightness of the task can be examined effectively. Additionally, the thought gives σ-time fine-grained get to control. Cloud service supplier may confine a specific arrangement of clients to appreciate get to benefit for at most σ times inside a predetermined period. Suqing Lin et al. [3] proposed a more effective and nonexclusive development of ABE. This ABE is certain redistributed unscrambling based on an attribute-based key epitome instrument, a symmetric-key encryption plot and a responsibility conspire. At that point they demonstrate the security and the check soundness of our developed ABE conspire in the standard model. Sushmita Ruj et al. [4] proposed a decentralized access control conspire for secure data storage in clouds. It bolsters unknown validation. In this plan, the cloud confirms the legitimacy of the arrangement without knowing the clients personality before putting away data. This plan likewise has the element of access control in which just legitimate clients can unscramble the put away data. The plan anticipates replay assaults and backings creation, adjustment, and perusing data put away in the cloud. C. Wang et al. [5] propose a protected cloud storage framework supporting security safeguarding open inspecting. They further make greater our impact to enable the TPA to execute reviews for numerous clients in the meantime and professionally. Across the board security and introduction examination demonstrate the proposed schemes are provably secure and to a great degree proficient. Boyang Wang et al. [6] propose a novel open inspecting system for the respectability of shared data in view of efficient client repudiation. By using the possibility of intermediary re-marks, their framework permits the cloud tore-signature obstructs in the interest of realistic clients amid client denial, with the goal that current clients don't require downloading and re-marking hinders independent from anyone else. In this way, an open verifier has been everlastingly splendid to review the honesty of shared data without recovering the entire data from the cloud, regardless of whether some piece of collective data have been re-marked by the cloud. Moreover, our system can bolster bunch reviewing by confirming a few evaluating errands in the meantime. David Cash et al. [7] give the primary clarification giving confirmations of hopelessness to dynamic storage, where the customer can do easygoing peruses/composes on any area inside her data by working a productive convention with the server. Sooner or later in time, the customer can execute a productive review convention to ensure that the server keeps up the most up to date release of the customer data.

III. End User Security Issues

End Users need to get to assets inside the cloud and may remember of get to understandings like adequate utilize or irreconcilable circumstance. The customer association have some component to discover powerless code or conventions at passage focuses like servers, firewalls, or cell phones and transfer fixes on the local frameworks when they are found. The cloud ought to secure from any client with noxious expectation that will imagine to access data or pack up an administration.

Security-as-an administration

In Cloud condition the security given by clients utilizing cloud administrations and the cloud specialist co-ops (CSPs). Security-as-an administration is a security given as cloud administrations and it can gave in two strategies: In first strategy anybody can changing their conveyance techniques to incorporate cloud administrations includes built up data security sellers. The second technique Cloud Service Providers are giving security just as a cloud benefit with data security organizations. All the security organizations, against malware sellers required in the conveyance of SaaS concerning email sifting thus on.[9]

Program Security

In a Cloud domain, remote servers are utilized for calculation. The customer hubs are utilized for info/yield operations, and for approval and validation of data to the Cloud. A standard Web program is stage in-ward customer programming valuable for all users all through the world. This can be classified into various sorts: Software-as-a-Service (SaaS), Web applications, or Web 2.0. TLS is utilized for data encryption and host validation The Legacy Same Origin Policy is the inclusion of scripting dialects into Web pages for get to rights for scripts. In is to permit get to peruse or compose operations a similar starting point on substance, to deny yet from the diverse birthplace any entrance on substance. Beginning means an "a similar application", it can be characterized with space name, convention, port in a web. Be that as it may, a few issues with the SOP, yet it could be comprehended with "birthplace" definition. On account of WWW it's not working legitimately. Security prerequisites for to ensure both data amid transport, and to validate the server's area name in Web applications is TLS. Attacks on Browser-based Cloud Authentication are one of the security issue with program based conventions in Cloud Computing and it is not skilled to create cryptographically substantial XML tokens. In this way, it can conceivable with a trusted outsider. Login is unrealistic at a server because of the less qualifications in program, So HTTP forward it to the Passport login server. In the wake of entering username and secret key from client, then the Passport server change over this verification into a Kerberos token, it can diverted to the asking for server from other HTTP divert. Kerberos tokens are not clear to the program is the security issue with Passport, and it ensured by the SOP. Be that as it may, any attacker can get to those tokens then he gets to all administrations of the casualty. Secure Browser-based Authentication is the circumstance is not recommended, but rather we can perform for better outcomes by joined SOP and TLS for secure FIM conventions. In Cloud Computing by utilizing TLS Browser Enhancements are exceptionally constrained in a confirmation focus. It is impractical for XML Signature, the program can be included many Web Service functionalities by essentially stacking a suitable JavaScript library amid runtime. Along these lines, the program security API can include the upgrades XML Encryption and XML Signature. [8]

Validation

In the cloud condition, the essential reason for get to control is client validation and get to control are more imperative than any time in recent memory since the cloud and the greater part of its data are available to everywhere throughout the Internet. Confided in Platform Module (TPM) is a broadly accessible and more grounded validation than username and passwords. Confided in Computing Groups (TCG's) is IF - MAP standard about approved users and other security issue progressively correspondence between the cloud supplier and the client. At the point when a client is reassigned or terminated, the client's uniqueness administration framework can report the cloud supplier continuously so that the client's cloud get to can be revoked or adjusted inside seconds. In cloud any let go client is logged, they can be instantly disengaged. [5] Trusted Computing empowers verification of customer hubs and different gadgets for enhancing the security in cloud computing. The oftentimes focused on attack is confirmation in facilitated and virtual administrations. The protected components are utilized to the confirmation procedure for continuous focus of attackers by various approaches to validate users in light of various data know by the client.

IV. The Most Important Security Issue - Authentication In The Cloud Environment

All of the security threats mentioned above take place in the absence of proper authentication mechanism and could be avoided if one deploys any of the following authentication mechanisms [8].

1) Working of Authentication on a private network

While logging on to the machine and then trying to access a resource, either a file server or database, it needs to be assured that ourlogin credentials are valid. If it is a Windows machine, this authentication is performed by a component called the Local Security Authority Subsystem Service (“LSASS”). If we run Windows Task Manager and list the running processes for all users, we see a program called "lsass.exe". Similarly, in a Linux/UNIX/Mac machine, it is called "lsassd"[9].

Authentication of a user could be done in either one of two ways: using local credentials or using Active Directory (“AD”) credentials. If the machine is "joined" to AD, we will typically log on with the AD account. If the machine is not joined to AD it is in work group mode and we log on using local credentials. With latter, the username and password are validated against account information stored on user‟s own machine[10]. In the AD case,LSASS authenticates the user‟s credentials using the Kerberos protocol to talk to an AD domain controller.Kerberos is an essential thing to mention for authentication. It can authenticate credentials without ever transmitting the password in either clear or hashed form. This is important because it makes it impossible to perform offline password cracking. Kerberos also supports single sign-on, which forms the base for any authentication check. Once we are logged on to the machine, we have a special "ticket" that can be used to acquire additional tickets for other services.

2) Identity management

At the core of an identity management system are policies defining which devices and users are allowed on the network and what a user can accomplish, depending on his device type, location and other factors[11]. The solution for ID management in Cloud is Cloud ID which links the confidential information of the users to their biometrics and stores

it in encrypted manner[2]. Making use of an encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

3) Authentication techniques

Existing User Authentication Techniques are shown in the figure below which takes different criteria to authenticate the users in Cloud[12].

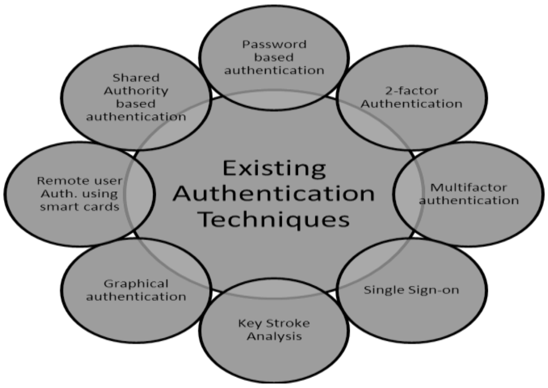

Password based authentication
2-factor Authentication
Multifactor authentication
Single Sign-on
Key Stroke Analysis
Graphical authentication
Remote user Auth. using smart cards
Shared Authority based authentication
Existing Authentication Techniques

Figure : User Authentication Techniques

Password based Authentication is also called single-factor authentication. In this method, user should insert username and password to login to the system and can access to the data in cloud service provider. This mechanism in present may not be considered the best security practice as leaked passwords can lead to data breaches[13].

Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized, such as a security code[14].

Single Sign-On(“SSO”) is a session/user authentication process that permits a user to enter a name and password in order to access multiple applications. Credentials for authorization are stored on a dedicated SSO policy server.Although single sign-on is a convenience to users, it present risks to enterprise security. If an attacker gains control over a user's SSO credentials, he will be granted access to every application the user has rights to, which increases the amount of potential damage[13].

Key Stroke Analysis uses the fashion and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the user's typing pattern for future authentication [15].

Graphical Authenticationsystem works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). A graphical password is easier than a text-based password for most people to remember.

Authentication using smart card: A biometric authenticated card which allows the user with both logical and physical access is a long cherished dream of any corporation. The connection of a smart card chip is via direct physical contact with a machine which could read smart cards. However, USB tokens are way more easy and convenient to carry, less susceptible to breakage and could be read by any PC having USB ports.

Shared Authority based privacy preserving authentication protocol (“SAPA”)is attractive for multi-user collaborative cloud applications. Shared access authority is attained by anonymous access request matching mechanism with security and privacy considerations i.e., authentication, data anonymity, user privacy, and forward security[16].

IV. Design Objectives of Authorized Method and Algorithm

The main design objectives of the schema include:

♦ A safe key dispersion with no secure communication channel. The user gets the private key from Certificate authorities with the public key. [9]

♦ The group users can provide fine-grained access control of the group manager.

♦ The group user can revoke from the dynamic groups safely with the influence of the polynomial function.

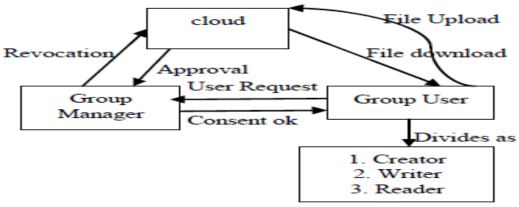
♦ The number of the user revoked is independent of the existing user in dynamic groups getting the private key.

A. Scheme Representation

The System model consists of the Group Manager, Group user, and the Cloud [6]. The Group member or group users can divide as creator, reader and writer. The system setup is as follows

Step1: Set up the Cloud Server
Step2: Confirm the Group Manager
Step3: Select Group Member with privileges
Step4: Group Member Registration
Step5: Key Distribution for Group Member & Group Manager
Step 6: Data Read/Write/Create
Step 7: Revocation procedures

The work flow of the system model is



B. Methodology

Preliminaries:

[1] Bilinear Maps: Let G1 and G2 be additive cyclic groups of the same prime order q. Let $e: G1 x G2 \rightarrow G2$ denote a bilinear map constructed with the following properties:

1. Bilinear: $\forall$ a, b $\in$ Z*q and P,Q $\in$G1, e(aP,bQ) = e(P,Q)ah

• 2. Non generate: There exists a point Q such that e(Q.Q)$\neq$ 1.

• 3. Computable: There is an efficient algorithm to compute e(P,Q) for any P,Q $\in$ G1.

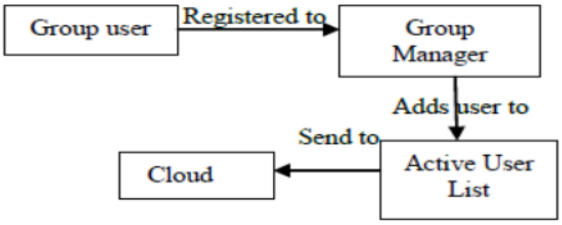
C. Asymmetric Encryption Algorithm

Step 1: Select two Prime Numbers P and Q
Step 2: Compute N=p*q Compute φ(N)=(p-1)*(q-1)
Step 3: Choose e such that 1<e<φ(N) and e and N are Co prime
Step 4: Computer a value for d such that (d *e) % φ(N)=1
Step 5: Public key is (e, N) Private Key is (d, N)

The unbalanced Encryption systems empower the group manager to dynamically increment new client and in the meantime saves the prior figured data. Along these lines, recently joined users can straightly unscramble data files without reaching with the proprietors. So that there will be no compelling reason to change client unscrambling keys.

D. Framework Entities Work

1. Client Registration For client enlistment of client part has an ID. The group manager includes the client ID into the group client list, which will be utilized as a part of following. After enrollment, client acquires a private key, with will be utilized for group mark and record decoding. While amid enlistment itself, the client separates themselves as a maker or an author or a peruser.

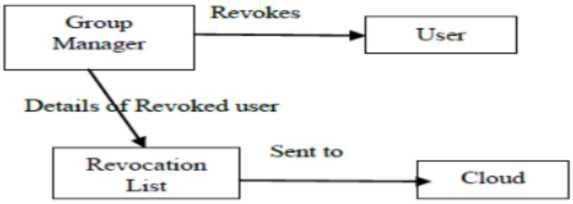


2. Transfer Files the File transfer is done just by the group Manager or an administrator.

3. Files Update Moreover, the maker and author just can do altering of the data with the assent of the group manager. The peruser can just utilize the data content with approval.

4. Record Deletion The document or data put away in the cloud are erased by either the group manager or the part who transferred the record into the server.

5. Deny client from the group User repudiation is performed by group manager by executing a polynomial capacity done by group manager alone. Once the client is revoked from the group, then the group part r can't be capable get to the cloud assets and its data.



V. Proposed System

To solve the security issues in cloud; other user can't read the respective users data without having access. Data owner should not bother about his data, and should not get fear about damage of his data by hacker; there is need of security mechanism which will track usage of data in the cloud. So that before store data into cloud the data owner will encrypt data using blowfish algorithm and stored into cloud. The data consumer will retrieve data from the cloud and decrypt using blowfish algorithm. Before performing encryption and decryption process each users will verify by cloud service for the purpose of authentication. In this paper we are using identity based digital signature schema for authentication of users. The implementation procedure of identity based digital signature schema is as follows.

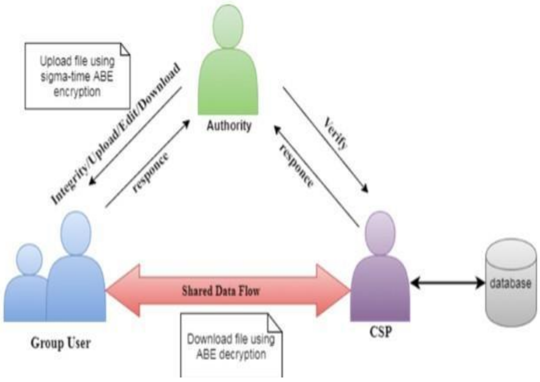

Upload file using sigma-time ABE encryption
Integrity/Upload/Edit/Download
responce
Authority
Verify
responce
Group User
Shared Data Flow
CSP
database
Download file using ABE decryption

Fig. Proposed system Architecture

AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix.

The AES Encryption consists of four different stages they are

Substitute Bytes: Uses an S-box to perform a byte-by-byte substitution of the block

Shift Rows: A Simple Permutation

Mix Columns: A substitution that makes use of arithmetic overGF(9)

Add Round Key: A Simple Bitwise XOR of the current block with the portion of the expanded key

AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

VI. Conclusion

In this paper present an effect approach for performing authentication of data consumers and also provide more privacy of shared data in a cloud. Before performing sharing of data each user will verify by the cloud service for the purpose of authenticated user or not. After completion of authentication process the cloud service will send authentication status to individual users in cloud and also send secret key. Before sharing data in the cloud the data owner will stored data into cloud in the form of cipher format. So that by converting data into cipher format the data owner will user blowfish encryption process stored data into cloud. If any user will retrieve data from the cloud and decrypt that using blow fish algorithm will get original plain format data. By implementing those concepts we improve efficiency of authentication process and also provide more privacy of shared data in cloud.

References

[1]. J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of smart grid. IEEE Transactions on Cloud Computing, 3(2):233–244,2015.

[2]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang. A secure and expressive ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Future Generation Computer Systems, 52(C):95–108, 2015.

[3]. K. Liang, L. Fang, D. S. Wong, and W. Susilo. A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds. Concurrency and Computation: Practice and Experience, 27(8):2004–2027, 2015.

[4]. K. Liang, J. K. Liu, R. Lu, and D. S. Wong. Privacy concerns for photo sharing in online social networks. IEEE Internet Computing, 19(2):58– 63, 2015.

[5]. K. Liang and W. Susilo. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Transactions on Information Forensics and Security, 10(9):1981–1992, 2015.

[6]. K. Liang, W. Susilo, and J. K. Liu. Privacy-preserving ciphertext multisharing control for big data storage. IEEE Transactions on Information Forensics and Security, 10(8):1578–1589, 2015.

[7]. J. Liu, X. Huang, and J. K. Liu. Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute based signcryption. Future Generation Computer Systems, 52:67–76, 2015.

[8]. X. Liu, J. Ma, J. Xiong, and G. Liu. Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data. International Journal of Network Security, 16(6):437–443, 2014.

[9]. H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences, 275(11):370–384, 2014.

[10]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie. A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, 9(10):1667–1680, 2014.