ANONYMOUS AUTHENTICATION AND SECURE DATA STORAGE USING DECENTRALIZED ACCESS CONTROL SCHEME

Vidyashree M[1], Sanjay Kumar N V[2]

[1]*PG Student, Dept. of CSE, Kalpataru Institute of Technology, (India)*

[2]*Assistant Professor, Dept. of CSE, Kalpataru Institute of Technology, (India)*

ABSTRACT

The new suburbanised access management theme for secure knowledge storage in clouds that supports anonymous authentication. Within the planned theme, the cloud verifies the genuineness while not knowing the user's identity before storing knowledge. The theme conjointly has the accessorial feature of access management within which solely valid users can measure and able to decipher the hold on info. The theme prevents replay attacks and supports creation, modification, and reading knowledge hold on within the cloud. we have a tendency to conjointly address user revocation. Moreover, our authentication and access management theme is suburbanised and strong, not like different access management schemes designed for clouds that square measure centralized. Cloud storage provides a extremely out there, simply accessible and cheap remote knowledge repository to purchasers who cannot afford to take care of their own storage infrastructure. Whereas several applications of cloud storage need security guarantees against the cloud supplier (e.g., storage of high-impact business knowledge or medical records), most services cannot guarantee that the supplier won't see or modify shopper knowledge. this can be mostly as a result of this approaches for providing security (e.g., encoding and digital signatures) diminish the utility and/or performance of cloud storage. User privacy is additionally needed so the cloud or different users don't grasp the identity of the user. The validity of the user who stores the info is additionally verified.

Keywords: Access Control, Authentication, Cloud Storage, Digital Signature, Valid Users.

I. INTRODUCTION

Cloud computing could be a quick growing paradigm during which computing resources area unit provided as services over the net and users will access the resources supported their payments. Analysis in cloud computing is receiving plenty of attention from each educational and industrial worlds. In cloud computing, users will source their computation and storage to servers (also known as clouds) victimization web. This frees users from the hassles of maintaining resources on-site. Clouds will offer many styles of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to assist developers write applications (e.g., Amazon's S3, Windows Azure). abundant of the info hold on in clouds is very sensitive, for instance, medical records and social networks. Security and privacy area unit therefore vital problems in cloud computing.

An area wherever access management is wide being employed is health care. Clouds area unit being employed to store sensitive data regarding patients to modify access to medical professionals, hospital workers, researchers, and policy manufacturers. it's vital to manage the access of knowledge so solely approved users will access the info. Access management is additionally gaining importance in on-line social networking wherever users (members) store their personal data, pictures, videos and share them with designated teams of users or communities they belong to. Access management in on-line social networking has been studied and such information area unit being hold on in clouds and its vital that solely the approved users area unit given access to those data.

Sahai and Waters[7] introduced attribute-based encoding (ABE) as a brand new suggests that for encrypted access management. In Associate in Nursing attribute-based encoding system ciphertexts aren't essentially encrypted to 1 explicit user as in ancient public key cryptography. Instead each users' personal keys and ciphertexts are going to be related to a group of attributes or a policy over attributes. A user is in a position to decode a ciphertext if there's a \match" between his personal key and therefore the ciphertext. In their original system Sahai and Waters conferred a Threshold ABE system during which ciphertexts were labeled with a group of attributes S and a user's personal key was related to each a threshold parameter k and another set of attributes S0. so as for a user to decode a ciphertext a minimum of k attributes should overlap between the ciphertext and his personal keys. one in every of the first original motivations for this was to style Associate in Nursing error-tolerant (or Fuzzy) identity-based encoding theme that might use biometric identities.

The primary disadvantage of the Sahai-Waters [7] threshold ABE system is that the edge linguistics aren't terribly communicative and so area unit limiting for coming up with a lot of general systems. Goyal et al. introduced the thought of a lot of general key-policy attribute-based encoding system. In their construction a ciphertext is related to a group of attributes and a user's key is related to any monotonic tree access structure. the development of Goyal[7] et al. is viewed as Associate in Nursing extension of the Sahai-Waters[7] techniques wherever rather than embedding a Shamir secret sharing theme within the personal key, the authority embeds a a lot of general secret sharing theme for monotonic access trees. As a lot of sensitive information is shared and hold on by third-party sites on the net, there'll be a requirement to encode information hold on at these sites. One disadvantage of encrypting information, is that it is by selection shared solely at a coarse-grained level. In many distributed systems a user ought to solely be able to access information if a user posses an exact set of credentials or attributes. Currently, the sole technique for implementing such policies is to use a trusty server to store the info and mediate access management. However, if any server storing the info is compromised, then the confidentiality of the info are going to be compromised.

The main aspects of the paper area unit as follows:

1) Distributed access management of knowledge hold on in cloud so solely approved users with valid attributes will access them.

2) Authentication of users UN agency store and modify their information on the cloud.

3) The identity of the user is shielded from the cloud throughout authentication.

4) The design is redistributed, which means that there is many KDCs for key management.

5) The access management and authentication area unit each collusion resistant, which means that no 2 users will interact and access information or demonstrate themselves, if they're severally not approved.

6) Revoked users cannot access information when they need been revoked.

7) The projected theme is resilient to replay attacks. A author whose attributes and keys are revoked cannot write back stale data.

8) The protocol supports multiple browse and pen the info hold on within the cloud.

9) The prices area unit akin to the prevailing centralized approaches, and therefore the high priced operations area unit principally done by the cloud

II. RELATED WORK

Our projected privacy protective documented access management theme makes use of use 2 protocols ABE(Attribute primarily based Encryption) and ABS (Attribute primarily based Signing).While obligatory Access Controls (MAC) square measure applicable for construction secure military applications, Discretionary Access Controls (DAC) square measure usually perceived as meeting the safety process wants of business and civilian government. The paper[11] argues that reliance on DAC because the principal technique of access management is unwarranted and inappropriate for several industrial and civilian government organizations. The paper describes a sort of non-discretionary access management role-based access management (RBAC)[5] that's a lot of central to the secure process wants of non-military systems then DAC.

This paper[4], supported the identity-based graded model for cloud computing (IBHMCC) and its corresponding secret writing and signature schemes, given a brand new identity-based authentication protocol for cloud computing and services. Through simulation testing, it's shown that the authentication protocol is additional light-weight and economical than SAP, specially the additional light-weight user aspect. Such benefit of our model with nice quantifiability is incredibly suited to the huge scale cloud Attribute primarily based secret writing (ABE)[7] determines coding ability supported a user's attributes. during a multi-authority ABE[9] theme, multiple attribute-authorities monitor totally different sets of attributes and issue corresponding coding keys to users, and encryptors will need that a user get keys for applicable attributes from every authority before decrypting a message.

III. SYSTEM ARCHITECTURE

Consider the subsequent situation: A student, Alice, desires to send a series of reports concerning some malpractices by authorities of University X to any or all the professors of University X, analysis chairs of universities within the country, and students happiness to Law department all told universities within the province.

Alice needs to stay anonymous whereas business all proof of malpractice. She stores the knowledge within the cloud. Access management is vital in such case, so solely licensed users will access the information. Alice will shield the information in encrypted format and while not knowing the cryptography key no one will access the information. it's conjointly necessary to verify that the knowledge comes from a reliable supply. the issues of access management, authentication, and privacy protection ought to be resolved at the same time.

We propose our privacy protective documented access management theme. per our theme a user will produce a file and store it firmly within the cloud. This theme consists of use of the 2 protocols ABE(Attribute primarily based Encryption) and ABS (Attribute primarily based Signing). There square measure 3 users, a creator, a reader and author. Creator Alice receives a token γ from the trustee, UN agency is assumed to be honest. A trustee may be somebody just like the centralized UN agency manages welfare numbers etc. On presenting her

id (like health/social insurance number), the trustee offers her a token γ. There square measure multiple KDCs (here 2), which might be scattered. as an instance, these may be servers in several components of the globe. A creator on presenting the token to 1 or a lot of KDCs receives keys for encryption/decryption and signing language.

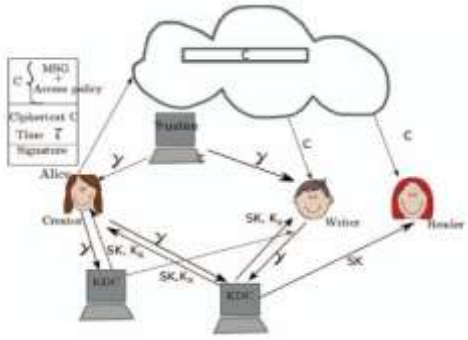

Fig. 1. A Secure Cloud Model

The model consists of 3 users a creator, a reader and a author. Creator Alice receives a token γ from the trustee, WHO is assumed to be honest. A trustee is somebody just like the federal WHO manages social welfare numbers etc. On presenting her id (like health/social insurance number), the trustee offers her token γ. There multiple KDCs (here 2), which may be scattered. parenthetically, these is servers in several elements of the planet. A creator on presenting the token to 1 or a lot of KDCs receives keys for encryption/decryption and linguistic communication. within the fig SKs square measure secret keys given for cryptography, Kx square measure keys for linguistic communication. The message seasoning is encrypted below the access policy X. The access policy decides WHO will access the information hold on in cloud.

The creator decides on a claim policy Y, to prove her genuineness and signs the message underneath this claim. The ciphertext C with signature is c, and is shipped to the cloud. The cloud verifies the signature and stores the ciphertext C. once a scaner desires to read, the cloud sends C. If the user has attributes matching with access policy, it will decode and obtain back original message. Write yield within the same method as file creation. By designating the verification method to the cloud, it relieves the individual users from time overwhelming verifications. once a scaner desires to read some knowledge hold on within the cloud, it tries to decode it exploitation the key keys it receives from the KDCs. If it's enough attributes matching with the access policy, then it decrypts the knowledge hold on within the cloud

IV. REAL LIFETIME EXAMPLE

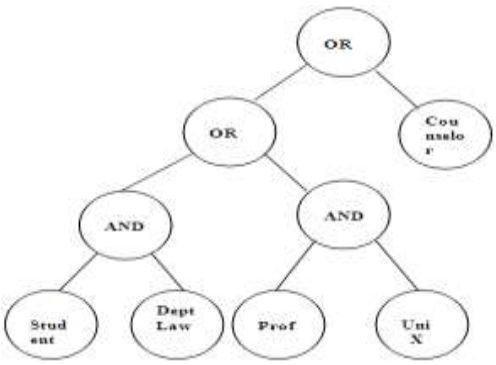

Fig. 2. Example of Claim Policy

We currently return the matter we tend to explicit within the introduction. we'll use a relaxed setting. Suppose Alice could be a student and needs to send a series of reports regarding malpractices by authorities of University X to all or any the professors of University X, analysis chairs of universities X,Y,Z and students happiness to Law department in university X. She needs to stay anonymous, whereas business enterprise all proof. All data is hold on within the cloud. it's necessary that users shouldn't be able to understand her identity, however should trust that the knowledge is from a legitimate supply. For this reason she additionally sends a claim message that states that she "Is a law student" or "Is a student counselor" or "Professor at university X".

The tree comparable to the claim policy is showninFigure2. The leaves of the tree consists of attributes and also the intermediator nodes consists of Boolean operators. during this example the attributes ar "Student", "Prof", "Dept Law", "Uni X", "Counselor". The on top of claim policy will be written as a Boolean operate of attributes as ((Student AND Dept Law) OR (Prof AND Uni X)) OR (Student Counselor). Boolean functions also can be delineate by access tree, with attributes at the leaves and AND (∧) and OR (∨) because the intermediate nodes and root. Boolean functions will be reborn to LSSS matrix as below: Let v[x] be oldsters vector. If node x=AND, then the left kid is (v[x]|1), and also the right kid is (0,...,1). If x=OR, then each kids even have unchanged vector v[x]. Finally, pad with 0s before, specified all vectors ar of equal length. The proof of validity of the formula is given in [13]. exploitation this formula, the span program for this policy is

M=

$$\begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{pmatrix}$$

An assignment v=(v1, v2, v3, v4, v5) satisfies this span program if vM = (1, 0). The cloud ought to verify that Alice so satisfies this claim. Since she could be a pupil, v=(1, 1, 0, 0, 0) and could be a valid assignment. As a legitimate user she will be able to then storeall the encrypted records underneath the set of access policy that she has determined. The access policy just in case of Alice is ((Prof AND Uni. X) OR (Research Chair AND ((Uni X OR Uni Y) OR Uni Z)) OR ((Student AND Dept Law)AND Uni X).

Later once a legitimate user, say Bob needs to change any of those reports he additionally attaches a group of claims that the cloud veryfies. let's say, Bob could be a analysis chair and may send a claim "Research chair" or "Department head" that is then verified by the cloud. It then sends the encrypted information to the Bob. Since Bob could be a valid user and has matching attributes, he will decipher and find back the knowledge. If Bob needs to browse the contents while not modifying them, then there's no ought to attach a claim. He are able to decipher on condition that he's a academic in University X or an exploration chair in one among the schools X,Y,Z or a student happiness to Department of Law in university X.

The students will have credentials from the university and conjointly a department. ab initio Alice goes to a trustee to Illustrate the Canadian health service and presents her a insurance variety or agency presents her a welfare variety. Eitheror each of those trustees will offer her token(s)γ=(u,Kbase,K0,ρ).With the token she approaches the KDCs within the university X and department D and obtains the key keys for cryptography and for keys Kx and Kentucky for sign language the assess policy. she will conjointly access the general public keys APK [i] of alternative KDCs. the whole method is carried on within the following way:A. Data Storage in

clouds. Let the info be denoted by flavorer,X is that the access policy- ((Prof AND Uni. X) OR (Research Chair AND ((Uni X OR Uni Y) OR Uni Z)) OR((Student AND Dept Law)AND Uni X) Alice encrypts the info and obtains the ciphertext C=Enc(MSG,X).Alice conjointly decides on a claim policy Y that is shown in Figure two. From the matrix, v=(1,1,0,0,0) will be calculated. The values of Y,W,S1,S2,S3,S4,S5,P1,P2 will be calculated. μ=H(MSG||Y). this time stamp τ is hooked up to the ciphertext to stop replay attacks. The signature σ is calculated as ABS.Sign. The ciphertext c=(C,τ,σ,Y) is then send to the cloud. The cloud verifies the signature usingthe perform ABS.Verify as given in Equation (11). If Alice has valid credentials then the ciphertext (C,τ) is keep, else it's discarded.

Suppose Bob desires to access the records keep by Alice. Bob then decrypts the message seasoner exploitation his secret keys exploitation perform ABE.Decrypt. Writing return like file creation. it's to be noted that the time τ is additional to the information in order that though Bob's credentials area unit revoked, he cannot write stale information within the cloud.

V. CONCLUSION

The work presents the information of cloud security access. the prevailing system doesn't give the users with the authorization and secret writing techniques of secured storage in cloud. we have a tendency to propose a decentralised model that keeps the anonymous believability of the user. The cloud doesn't grasp the identity of the user WHO stores info, however solely verifies the user's credentials. Key distribution is completed during a decentralized manner.

REFERENCES

[1] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556 563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[4] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[5] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy. , pp. 321–334, 2007.

[9] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.

[10] Matthew Green, Susan Hohenberger and Brent Waters, "Outsourcing the Decryption of ABE Ciphertexts," in USENIX Security Symposium, 2011.