Token Based Authentication with Decentralized Access Control in Clouds

REMYA RAMAKRISHNAN*
Student
Dept of Computer Science Engineering
Bharath University, Chennai, India
SELAIYUR – 600073
remya.ramakrishnan@yahoo.com

Mr. MICHAEL
Assistant Professor
Dept of Computer Science Engineering
Bharath University, Chennai, India
SELAIYUR - 600073
micmgeo@yahoo.co.in

Abstract —
Replacement localized access management theme for secure information storage in clouds that supports anonymous authentication. Within the projected theme, the cloud verifies the credibility of the series while not knowing the user's identity before storing data. Our theme additionally has the value-added feature of access management during which solely valid user's area unit able to decode the keep data. The theme prevents replay attacks and supports creation, modification, and reading information keep within the cloud. We tend to additionally address user revocation. Moreover, our authentication and access management theme is localized and strong, not like alternative access management schemes designed for clouds that area unit centralized. The communication, computation, and storage overheads area unit reminiscent of centralized approaches.

Keywords- Access management, authentication, attribute-based signatures, attribute-based secret writing, cloud storage

I. INTRODUCTION

Cloud computing is that the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped image as AN abstraction for the advanced infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's information, computer code and computation. End users access cloud-based applications through an internet browser or a light- weight desktop or mobile app whereas the business computer code and user's information are hold on on servers at a foreign location. Proponents claim that cloud computing permits corporations to avoid direct infrastructure prices, and target comes that differentiate their businesses rather than infrastructure. Proponents additionally claim that cloud computing permits enterprises to urge their applications up and running quicker, with improved manageableness and fewer resources to fulfill unsteady and unpredictable business demand. In the business model exploitation computer code as a service, users are provided access to application computer code and databases. Cloud suppliers manage the infrastructure and platforms that run the applications. SaaS is typically spoken as "on- demand software" and is typically priced on a pay-per-use basis. SaaS suppliers typically worth applications employing a subscription fee. Proponents claim that the SaaS permits a business the potential to cut back IT operational prices by outsourcing hardware and computer code maintenance and support to the cloud supplier. this permits the business to allocate IT operations prices aloof from hardware/software defrayal and personnel expenses, towards meeting different IT goals. Additionally, with applications hosted centrally, updates are free while not the necessity for users to put in new computer code. One disadvantage of SaaS is that the users' information is hold on on the cloud provider's server. As a result, there may be unauthorized access to the information. Cloud computing depends on sharing of resources to attain coherence and economies of scale the same as a utility (like the electricity grid) over a network. At the inspiration of cloud computing is that the broader conception of converged infrastructure and shared services.

II. RELATED WORK

DACC: Distributed Access Control in Clouds

In this paper, we have a tendency to propose a brand new model for information storage and access in clouds. Our theme avoids storing multiple encrypted copies of same information. In our framework for

secure information storage, cloud stores encrypted information. The most novelty of our model is addition of key distribution centers (KDCs). We have a tendency to propose DACC (Distributed Access management in Clouds) formula, wherever one or additional KDCs distribute keys to information house owners and users. KDC might offer access to specific fields all told records. Thus, one key replaces separate keys from house owners. House owners and users are allotted sure set of attributes. Owner encrypts the information with the attributes its and stores them within the cloud. The users with matching set of attributes will retrieve the information from the cloud.

The theme is collusion secure as 2 users cannot along rewrite any information that none of them has individual right to access. DACC conjointly supports revocation of users, while not redistributing keys to any or all the users of cloud services. We have a tendency to show that our approach ends up in lower communication, computation and storage overheads, compared to existing models and schemes. The cloud is assumed to be honest. If this demand isn't doable to satisfy, then care ought to be taken, that the cloud doesn't modify the information that it contains. Below such circumstances, the credibleness of the information should be verified by the users. Also, it's going to be important to cover the identity of the users and house owners, at identical time offer their authentication. In DACC, the cloud learns the access structure utilized by the owner and also the attributes of the users.

Identity-Based Authentication for Cloud Computing

In this paper, Cloud computing could be a recently developed new technology for complicated systems with massive-scale services sharing among varied users. Therefore, authentication of each users and services could be a vital issue for the trust and security of the cloud computing. SSL Authentication Protocol (SAP), once applied in cloud computing, can become therefore difficult that users can endure a heavily loaded purpose each in computation and communication. supported the identity-based class-conscious model for cloud computing (IBHMCC) and its corresponding secret writing and signature schemes, conferred a brand new identity-based authentication protocol for cloud computing and services. Through simulation testing, it's shown that the authentication protocol is a lot of light-weight and economical than SAP, especially the lot of light-weight user aspect. Such benefit of our model with nice quantifiability is incredibly suited to the large scale cloud.

Authentication is important in Cloud Computing. SSL Authentication Protocol is of low potency for Cloud services and users. during this paper, we have a tendency to conferred associate degree identity based mostly authentication for cloud computing, supported the identity-based class-conscious model for cloud computing (IBHMCC) and corresponding secret writing and signature schemes. Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is a lot of economical and light-weight than SAP, particularly the lot of light-weight user aspect. This aligned well with the concept of cloud computing to permit the users with a median or low-end platform to source their procedure tasks to a lot of powerful servers.

Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems

In this paper, a number of the foremost difficult problems in knowledge outsourcing situation area unit the social control of authorization policies and also the support of policy updates. Cipher text-policy attribute-based cryptography may be a promising crypto logic resolution to those problems for implementing access management policies outlined by knowledge a information owner on outsourced data. Attribute-based access management defines a brand new access management paradigm whereby access rights area unit granted to users through the employment of policies that mix attributes along. The policies will use any style of attributes. Attributes are often compared to static values or to 1 another therefore sanctionative relation-based access management.

However, the matter of applying the attribute-based cryptography in associate outsourced design introduces many challenges with reference to the attribute and user revocation. This paper proposes associate access management mechanism victimization cipher text-policy attribute-based cryptography to enforce access management policies with economical attribute and user revocation capability. The fine-grained access management are often achieved by twin cryptography mechanism that takes advantage of the attribute-based cryptography and selective cluster key distribution in every attribute cluster. We tend to demonstrate the way to apply the planned mechanism to firmly manage the

outsourced knowledge. The analysis results indicate that the planned theme is economical and secure within the knowledge outsourcing systems.

Token-Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency

Secure outsourcing of computation to associate entrusted service supplier is changing into a lot of and a lot of vital. Pure science solutions supported absolutely homomorphism and verifiable encoding, recently planned, square measure promising however suffer from terribly high latency. Different proposals perform the full computation on tamper-proof hardware and typically suffer from an equivalent downside. Trustworthy computing (TC) is another promising approach that uses trustworthy software system and hardware parts on computing platforms to produce helpful mechanisms like attestation permitting the info owner to verify the integrity of the cloud and its computation. However, on the one hand these solutions need trust in hardware that's beneath the physical management of the cloud supplier, and on the opposite hand they still have to be compelled to face the challenge of run-time attestation.

In this paper we tend to concentrate on applications wherever the latency of the computation ought to be reduced, i.e., the time from submitting the question till receiving the end result of the computation ought to be as tiny as doable. to attain this we tend to show the way to mix a trustworthy hardware token (e.g., a science coprocessor or provided by the customer) with Secure operate analysis (SFE) to reason impulsive functions on secret (encrypted) knowledge wherever the computation leaks no info and is verifiable. The token is employed within the setup section solely whereas within the time-critical on-line section the cloud computes the encrypted operate on encrypted knowledge exploitation cruciform encoding primitives solely and with none interaction with different entities.

III. EXISTING SYSTEM

Existing work on access management in cloud area unit centralized in nature. Some theme uses a biracial key approach and doesn't support authentication. Some don't support authentication additionally. Earlier work by Zhao et al. provides privacy conserving documented access management in cloud. However, the authors take a centralized approach wherever one key distribution center (KDC) distributes secret keys and attributes to any or all users. Sadly, one KDC isn't solely one purpose of failure however tough to take care of as a result of the big variety of users that area unit supported in a very cloud atmosphere.

However, the theme failed to give user authentication. Alternative the opposite downside was that a user will produce and store a file and other users will solely browse the file. Write access wasn't permissible to users apart from the creator. We, therefore, emphasize that clouds ought to take a localized approach whereas distributing secret keys and attributes to users. It's additionally quite natural for clouds to own several KDCs in several locations within the world. The drawbacks of the prevailing system are:

It supports 1-W-M-Rmeans that just one user will write whereas several users will browse. Access management in cloud is usually centralized in nature. The identity of the user isn't protected against the cloud. Most of the schemes don't seem to be proof against replay attacks. Write access wasn't permissible to users apart from the creator.

IV. PROPOSED SYSTEM

We propose and by experimentation valuate an automatic system, known as Filtered Wall (FW), able to filter unwanted messages from on-line Social Network user walls. we have a tendency to exploit Machine Learning (ML) text categorization techniques to mechanically assign with every short text message a collection of classes supported its content. The system provides a strong rule layer exploiting a versatile language to specify Filtering Rules (FRs), by that users will state what contents, shouldn't be displayed we have a tendency to propose a replacement localized access management theme for secure knowledge storage in clouds that supports anonymous authentication.

In the projected theme, the cloud verifies the believability of the ser while not knowing the user's identity before storing knowledge. Our theme additionally has the accessorial feature of access management during which solely valid user's square measure able to decipher the hold on info. The theme prevents replay attacks and supports creation, modification, and reading knowledge hold on within the cloud. Moreover, our authentication and access management theme is localized and strong, not like different access management schemes designed for clouds that square measure centralized layer on their walls. The benefits of the projected system are:

The design is localized, which means that there will be many KDCs for key management. The identity of the user is protected against the cloud throughout authentication. It supports multiple browse and incites the information hold on in clouds. Revoked users cannot access knowledge once they need been revoked. The projected theme is resilient to replay attacks. An author whose attributes and keys are revoked cannot write back stale information.

V.SYSTEM ARCHITECTURE

A system design or systems design is that the abstract style that defines the structure and/or behavior of a system. Associate degree design description could be a formal description of a system, organized during a means that supports reasoning concerning the structural properties of the system.

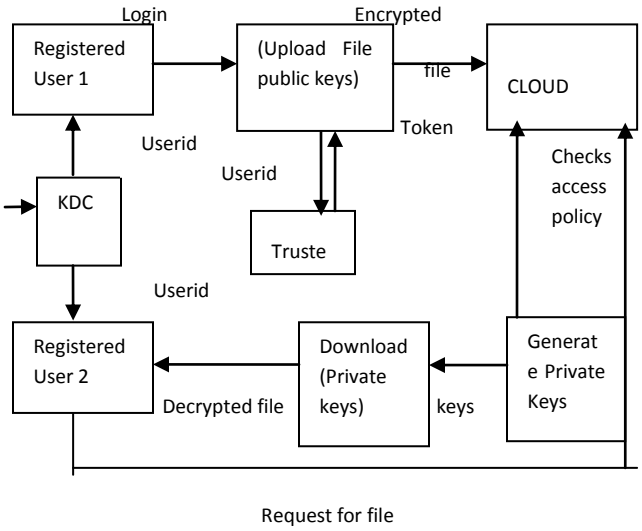

Fig 1. System Architecture

Implementation is that the most important stage in achieving a prosperous system and giving the user's confidence that the new system is viable and effective. Implementation of a changed application is to switch Associate in nursing existing one. This sort of language is comparatively straightforward to handle, provided there are not any major changes within the system. Each program is tested one by one at the time of development exploitation the info and has verified that this program coupled along within the approach per the program specification, the pc system and its setting is tested to the satisfaction of the user. The system that has been developed is accepted and tested to be satisfactory for the user. Initially as a primary step, the feasible sort of the appliance is to be created and loaded within the common server machine that is accessible to the complete user and therefore the server is to be connected to a network. The ultimate stage is to document the complete system that provides parts and therefore the in operation procedures of the system. Implementation is that the stage of the project once the theoretical style is clothed into a operating system. so it will be thought of to be the foremost crucial stage in achieving a prosperous new system and in giving the user, confidence that the new system can work and be effective.

The implementation stage involves careful designing, investigation of the present system and its constraints on implementations, coming up with of ways to realize amendment over and analysis of amendment over ways. Implementation is that the method of changing a brand new system style into operation. It's the section that focuses on user coaching, web site preparation and file conversion for putting in a candidate system.

VI. MODULE DESCRIPTION

The authors take a centralized approach wherever one key distribution center (KDC) distributes secret keys and attributes to any or all users. sadly, one KDC isn't solely one purpose of failure however tough to keep up as a result of the big range of users that square measure supported in an exceedingly cloud surroundings. It's simply not enough to store the contents firmly within the cloud however it'd even be necessary to confirm obscurity of the user. It's employed in some cases like once a user would really like to store some sensitive info however doesn't wish to be recognized. The user may wish to post a discuss an editorial, however doesn't wish his/her identity to be disclosed. However, the user ought to be able to sway the opposite users that he/ she may be a valid user WHO keeps the data while not revealing the identity. a part wherever access management is wide getting used is health care. Clouds square measure getting used to store sensitive info concerning patients to alter access to medical professionals, hospital workers, researchers, and policy manufacturers. It's necessary to regulate the access of information so solely licensed users will access the information. Using ABE, the records square measure encrypted beneath some access policy and keep

within the cloud. Users square measure given sets of attributes and corresponding keys. Only the users have matching set of attributes, will they rewrite the data keep within the cloud. Access management is additionally gaining importance in on-line social networking wherever users (members) store their personal info, pictures, and videos and share them with hand-picked teams of users or communities they belong to. Such information square measure being keep in clouds. It's vital that solely the licensed users square measure given access to the data.

1. User Enrollment: Initially the Key Distribution Center is made. As we tend to are proposing the localized approach the Key Distribution Center isn't centralized. Several range Key Distribution Center will be created. Every server can have its own range of users. Then the Key Distribution Center can add its users in step with their several places. As we tend to are victimization localized approach any range of Key Distribution Center will be created and conjointly n range of users will be accessorial to that. The users give their own per Different variety of KDC's area unit created and to register a user details. KDC name, KDC id and KDC countersign area unit given as input to make KDC. Inputs can save in an exceedingly info and to register a user details given a input as username and user id. Once KDC given a user id to a user, the user can listed the non-public details to KDC's given a input as user name, user id, countersign etc. The KDC are verify the user details and it'll insert it in an exceedingly info. Whereas adding every user the Key Distribution Center can offer distinctive use rid to any or all the individual users. Conjointly it specifies the user name and therefore the position of the various users. In their theme, a author will send its message and proper signature even once it now not has access rights. In our theme a author whose rights are revoked cannot produce a replacement signature with new time stamp and, thus, cannot write back stale info.sonal data for this method.

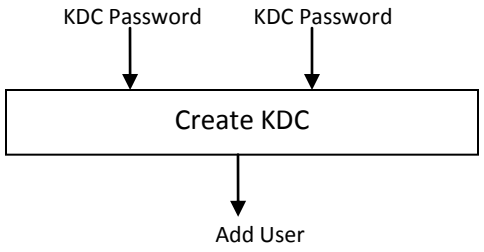

Fig 2 .User Enrollment

2. Token Generation: Users have Associate in nursing initial level Registration method at the online finish. The users offer their own personal info for this method. The server successively stores the knowledge in its info. Users receive a token from the trustee, World Health Organization is assumed to be honest. A trustee will be somebody just like the federal World Health Organization manages social welfare numbers etc. On presenting her id (like health/social insurance number), the trustee offers her a token.

After user registration the user will perform some actions. To perform any operation the user has got to generate a token. For this initial the user login into the user details. Then the user chooses the action to be performed. To perform any action the user wants a token which may be generated by the trustee. Here Trustee is that the any government or non-public organization that manages all the users from totally different Key Distribution Center. Once the user requests for the token the trustee can check the use rid of the various user as trustee is managing all the registered users from totally different Key Distribution Centers.

VII. CONCLUSION

In our planned system we've got bestowed a decentralized access management technique with anonymous authentication, that provides user revocation and prevents replay attacks. The cloud doesn't understand the identity of the user WHO stores data, however solely verifies the user's credentials. Key distribution is finished in an exceedingly decentralized means. 1-W-M-R implies that just one user will write whereas several users will browse. M-W-M-R implies that several users will write and skim. we have a tendency to see that the majority themes don't support several writes that is supported by our scheme. Our theme is strong and decentralized; most of the others area unit centralized. Our theme conjointly supports privacy protective authentication, that isn't supported by others. We have a tendency to compare the computation and communication prices incurred by the users and clouds and show that our distributed approach has comparable prices to centralized approaches. Our theme authenticates a user WHO desires to write down to the cloud. A user will solely write provided the cloud is in a position to validate its access claim. Associate in nursing invalid user cannot receive attributes from a KDC, if it doesn't have the credentials from the trustee. If a user's credentials

area unit revoked, then it cannot replace knowledge with previous stale knowledge, therefore preventing replay attacks.

ACKNOWLEDGEMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, Principal, and HOD of Computer Science & Engineering, Dr. K.P. Kaliyamurthie, Bharath University, and Chennai for their motivation and constant encouragement. The author would like to specially thank Dr. A.Kumaraval for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

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

[2] N. Cao, W. Lou, J. Li, Q. Wang, and C. Wang,, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM.* , pp. 441–445, 2010.

[3]M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[4] Y. Dai, H. Li, L. Tina, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing, pp. 157-166, 2009.

[5] J. Hurl and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July1, 2011.

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

[7] Q. Liu, G. Wang, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[8] A. Kayak, S. Ruj and I. Stojmenovic, , "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[9] A. Nayak, S. Ruj and M. Stojmenovic, "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.

[10] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.