FINE GRAINED TWO SECURITY CAPABILITIES - CLOUD COMPUTING SERVICES PRIMARILY BASED ON NETWORKS

G. RADHA DEVI

Research Scholar

Department of Computer Science and Engineering

Sri Satya Sai University of Technology and Medical Sciences, Sehore, M.P., India.

Abstract – For net primarily based Cloud Computing Services we tend to introduce Fine Grained 2 issue Access management. The Basic Concept behind the Fine Grained 2 issue access management is getting the permission from 2 parties during this case we tend to consider 2 parties as user secret key and lightweight device. In 2 issue access system an attribute based management mechanism is enforced from the assistance of user secret key and light-weight security device. User must satisfy with this 2 for obtaining access to system. If anyone fails user can't get the access to the system. The access control system denies the access of the user to the system if multiple user have same attribute set price.

Key Words: Security, Cloud computing, Performance analysis, Access management, SEM

I. INTRODUCTION

Cloud computing is also a virtual host system that permits enterprises to get for, lease, sell, or distribute software system associated completely different digital resources over the net as AN on demand service. It not depends on a server or style of machines that physically exist; as a result of it should be a virtual system. There unit of measurement many applications of cloud computing, like info sharing info storage huge information management, medical system etc. End users access cloud-based applications through a magnetic flux unit browser, skinny client or mobile app whereas the business package code and user's info unit of measurement persevere servers at a foreign location. The benefits of web-based cloud computing services unit of measurement huge, that add the convenience of accessibility, reduced prices and capital expenditures, increased operational efficiencies, measurability, flexibility and immediate time to promote. although the new paradigm of cloud computing provides nice advantages, there unit of measurement meanwhile additionally problems concerning security and privacy particularly for web-based cloud services. As sensitive information is additionally keep at intervals the cloud for sharing purpose or convenient access; and eligible users might to boot access the cloud system for varied applications and services, user authentication has become an essential part for any cloud system. A user is required to login before working the cloud services or accessing the sensitive information keep at intervals the cloud. There are unit a unit two problems for the traditional account/password primarily based system. First, the normal account/password-based authentication is not privacy-preserving. However, it's well acknowledged that privacy could be a necessary feature that has got to be thought-about in cloud computing systems. Second, it's common to share a laptop among utterly completely different people. it should be straightforward for hackers to place in some spyware to seek out the login password from the web-browser. A recently planned access management model called attribute based access management is also a sensible candidate to tackle the primary downside. It not exclusively provides anonymous authentication but put together further defines access control policies supported utterly completely different attributes of the requester, setting, or the knowledge object. In associate attribute-based access system,1 each user includes a user secret key issued by the authority. In apply the user secret is keep at intervals the non-

public portable computer. After we ponder upper than mentioned second downside on web-based services, it's normal that computers are additionally shared by many users significantly in some massive enterprises or organizations. as an example, enable United States to have faith in the following two scenarios:

1) During a hospital, computers unit of measurement shared by completely different employees. Dr. Alice uses the computer in space A once she is on duty at intervals the daytime, while Dr. Bob uses a similar pc at intervals identical space once he is on duty at night time.

2) In an awfully university, computers at intervals the school man laboratory unit of measurement typically shared by completely different students. Consider a corporation – industrial, government, or military – where all employees (referred to as users) have sure authorizations. We tend to tend to assume that a Public Key Infrastructure (PKI) is obtainable and each one user have digital signature, additionally as en/decryption, capabilities. within the course of humanistic discipline routine everyday tasks, users profit of secure applications, like email, file transfer, remote log-in and net browsing. currently suppose that a trusty user (Alice) can one factor that warrants immediate revocation of her security privileges. as an example, Alice may be laid-off, or she might suspect that her personal key has been compromised. Ideally, straightaway following revocation, the key holder, either Alice herself or associate degree offender, got to be unable to perform any security operations and use any secure applications. Specifically, this might mean:

– The key holder cannot scan any secure email. This includes encrypted email that already resides on Alice's email server (or native host) and potential future email mistakenly encrypted for Alice though encrypted email may even be delivered to Alice's email server, the key holder got to be unable to rewrite it.

– The key holder cannot generate valid digital signatures on any longer messages. However, signatures generated by Alice before revocation might need to remain valid.

– The key holder cannot proof itself to company servers (and various users) as a legitimate user. Throughout the paper, we've a bent to use email as academic degree example application. whereas it is a widespread mechanism for all-purpose communication, our clarification jointly applies to various secure suggests that of data exchange.

To provide immediate revocation it's natural to initial assume about ancient revocation techniques. many revocation ways that are proposed; they will be roughly classified into two outstanding types:

1) Specific revocation structures like Certificate Revocation Lists (CRLs) and variations on the theme, and

2) Real time revocation checking just like the net Certificate standing Protocol (OCSP) and its variants. In every case, some trusty entities are ultimately accountable of corroborative user certificates. However, the upper than requirements for immediate revocation aren't attainable to satisfy with existing techniques. This could be primarily as results of they are doing not give fine-grained enough management over users' security capabilities. Supporting immediate revocation with existing revocation techniques would end in important performance price and intensely poor quality, as mentioned in Section eight. As since each revocation technique exhibits a singular set of execs and cons, the factors for selecting the foremost effective technique got to be supported the specifics of the target application surroundings. fast revocation and fine-grained management over users' security capabilities are the motivating factors for our work. However, the necessity for these choices is clearly not universal since many computing environments (e.g., atypical university campus) are relatively "relaxed" and do not warrant victimisation fast revocation techniques. However, there are voluminous government, company and military settings wherever fast revocation and fine-grained management.

II. RELATED WORK

Though the new paradigm of cloud computing provides nice blessings, there are within the in the meantime jointly problems regarding security and privacy notably for web-based cloud services. As sensitive info is additionally hold on within the cloud for sharing purpose or convenient access; and eligible users could in addition access the cloud system for varied applications and services, user authentication has become a vital component for any cloud system. A user is needed to login before mistreatment the cloud services or accessing the sensitive info hold on at intervals

the cloud. There are two problems for the conventional account/password based mostly system.

•First, the conventional account/password-based authentication isn't privacy-preserving. However, it's well acknowledged that privacy is a crucial feature that needs to be thought of in cloud computing systems.

•Second, it is common to share a computer among whole totally different individuals. it ought to be easy for hackers to place in some spyware to seek out the login countersign from the web-browser.

•In existing, despite the fact that the computer may even be locked by a countersign, it'll still be presumptively guessed or taken by undiscovered malwares.

To avoid these issues we tend to propose a fine-grained two factor access management protocol for web-based cloud computing services, using a light-weight security device. The device has the following properties: (1) it'll work out some light-weight algorithms, e.g. hashing and exponentiation; and (2) it's tamper resistant, i.e., it's assumed that no-one can burgled it to induce the key data keep at intervals. Advantages of projected System:

1)Our protocol provides a 2FA security

2)Our protocol supports fine-grained attribute-based access that has a good flexibility for the system to line fully totally different completely totally different} access policies in step with different eventualities. At the same time, the privacy of the user is additionally preserved.

III. PROPOSED WORK

We propose a fine-grained two-factor access management protocol for web-based cloud computing services, employing a light-weight security device. The device has the next properties: (1) it'll estimate some light-weight algorithms, e.g. hashing and exponentiation; and (2) its tamper resistant, i.e., it's assumed that no-one can burgled it to induce the key data keep inside. Advantages of planned System:

1) Our protocol provides a 2FA security

2) Our protocol supports fine-grained attribute-based access that provides a decent flexibility for the system to line fully different or completely different access policies in step with different eventualities. At an analogous time, the privacy of the user is in addition preserved. We look for recommendation from our approach as a result of the SEM style. the essential arrange is as follows: we tend to introduce a greenhorn entity, mentioned as a SEM (Security Mediator): associate online semi-trusted server. To sign or decipher a message, a consumer ought to first get a message-specific token from its SEM. whereas not this token, the user cannot accomplish the meant task. To revoke the user's ability to sign or decipher, the security administrator instructs the SEM to forestall issue tokens for that user's future request. At that instant, the user's signature and/or cryptography capabilities area unit revoked. For quality reasons, one SEM serves many users. we tend to stress that the SEM style is evident to non-SEM users, i.e., a SEM isn't involved in cryptography or signature verification operations. With SEM's facilitate, a SEM shopper (Alice) can generate customary RSA signatures, and decipher customary cipher text messages encrypted alongside her RSA public key. whereas not SEM's facilitate, she cannot perform either of these operations. This backwards compatibility is one in each of our main vogue principles. Another notable feature is that a SEM is not a very trustworthy entity. It keeps no shopper secrets and each one SEM computations unit of measurement checkable by its shoppers. However, a SEM is an element trustworthy since each signature supporter implicitly trusts it to possess checked the signer's (SEM's client's) certificate standing at signature generation time. Similarly, each encryptor trusts a SEM to look at the decryptor's (SEM's client's) certificate standing at message cryptography time. We have a bent to accept this level of trust low-cost, particularly since a SEM serves an outsized number of shoppers associated therefore represents associate organization (or a group). So as to experiment and gain sensible experience, we've a bent to prototyped the SEM design exploitation the popular OpenSSL library. SEM is enforced as a daemon method running on a secure server. On the buyer side, we've a bent to designed plug-ins for the Eudora and Outlook email shoppers for signing outgoing, and decrypting incoming, emails. every of these tasks unit of measurement performed with the SEM's facilitate. Consequently, language and cryptography capabilities are also merely revoked. It is natural to boost whether constant usefulness could be obtained with further ancient security approaches to fine-grained management

and fast piece of writing revocation, like Kerberos. Kerberos after all, has been respiration since the mid- 80s and tends to work fine in corporate-style settings. However, Kerberos is awkward in heterogeneous networks just like the Internet; its inter-realm extensions area unit robust to use and want a particular amount of manual setup. moreover, Kerberos does not inter-operate with modern PKI-s and does not provide universal origin authentication offered by public key signatures. On the opposite hand, the SEM style is completely compatible with existing PKI systems. in addition, the SEM is simply answerable for revocation. not sort of a Kerberos server, the SEM cannot forge user signatures or decipher messages meant for users. As we've a bent to debate later within the paper, our approach is not reciprocally exclusive with Kerberos-like intra-domain security architectures. we tend to claim that the SEM style is also viewed as a group of complementary security services. Authority it's accountable to come up with user secret key for each user in line with their attributes. Authority that performs the operate like transfer File and supply Download Permission Cloud Server: It provides services to anonymous licensed users. It interacts with the user during the authentication method.

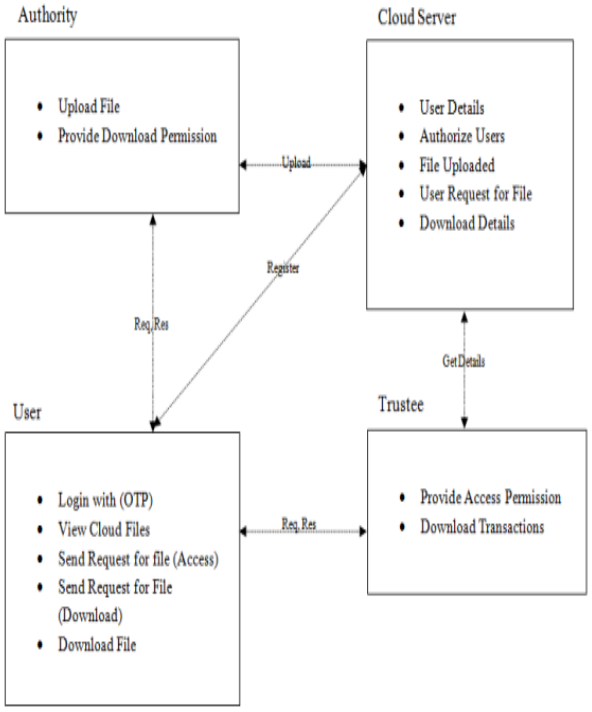

Fig 3.1: Framework

Cloud Server that performs the perform like User Details, Authorize Users, File Uploaded, User Request for File, Download Details User: it's the player that creates authentication with the cloud server. every user incorporates a secret key issued by the attribute-issuing authority and a security device initialized by the trustee. User that performs the function like Login with (OTP),View Cloud Files, Send Request for file (Access),Send Request for File, Download File. Trustee: It is accountable for generating all system parameters and initializes the safety device. Trustee performs the activities like give Access Permission, Download Transactions.

IV. CONCLUSION

In this paper, we have given a fresh 2FA (including each user secret key and a light-weight security device) access control system for web-based cloud computing services. Based on the attribute-based access management mechanism, the planned 2FA access system has been well-known to not entirely enable the cloud server to limit the access to those users with a similar set of attributes but in addition preserve user privacy. careful security analysis shows that the planned 2FA access system achieves the required security wants. Through performance analysis, we tend to incontestable that the development is “feasible”. We tend to leave as future work to improve the efficiency whereas keeping all nice choices of the system. New approach to certificate revocation and fine-grained management over security capabilities rather than revoking the client’s certificate our approach revokes the client’s ability to perform scientific discipline operations like signature generation and cryptography. This approach has several blessings over ancient certificate revocation techniques:

1. revocation is fast – once its certificate is revoked, the shopper won't decipher or sign messages,
2. with binding signature linguistics, there is not any ought to validate the signer’s certificate as a locality of signature verification, and
3. our revocation technique is obvious to the peers since it uses commonplace RSA signature and cryptography formats.

REFERENCES:

[1] M. H. Au and A. Kapadia, “PERM: Practical reputation based blacklisting without TTPS,” in Proc. ACM Conf. Comput. Commun. Secur. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929– 940.

[2] M. H. Au, A. Kapadia, and W. Susilo, "BLACR: TTP-free blacklistable anonymous credentials with reputation," in Proc. 19th NDSS, 2012, pp. 1–17.
[3] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic kTAA," in Proc. 5th Int. Conf. SCN, 2006, pp. 111–125.
[4] 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 Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.
[5] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in Proc. 12th Annu. Int. CRYPTO, 1992, pp. 390– 420.
[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.
[8] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004.
[9] J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.
[10] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), Chicago, IL, USA, Nov. 2009, pp. 131– 140.
[11] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in Proc. 3rd Int. Conf. Secur. Commun. Netw. (SCN), Amalfi, Italy, Sep. 2002, pp. 268–289.
[12] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 56–72.
[13] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in Proc. ICICS, 2014, pp. 274–289.
[14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security mediated certificateless cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.
[15] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.
[16] R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 1751, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer-Verlag, 2000, pp. 354–373.
[17] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in Proc. EUROCRYPT, 2002, pp. 65–82.
[18] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.
[19] M. K. Franklin, in Proc. 24th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 2004.

About Author

G. Radha Devi
Research Scholar
Department of CSE
SSSUTMS, Bhopal