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

COPY RIGHT

IJIEMR Transactions, online available on 10 April 2019.

Link : http://www.ijiemr.org

Title:- High Quality Fine Grained Authentication In Pipeline Communication Using Distributed Computing.

Volume 08, Issue 04, Pages: 96 - 103.

Paper Authors

G. SHIRISHA, S.GEETHA REDDY

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

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

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

HIGH QUALITY FINE GRAINED AUTHENTICATION IN PIPELINE COMMUNICATION USING DISTRIBUTED COMPUTING

[1]G. SHIRISHA, [2]S.GEETHA REDDY
[1]Dept of ECE, SV University , Tirupati, AP, India.
[2]Dept of ECE, SV engineering college for womens, Tirupati, AP, India.

Sirishaece73@gmail.com sangatigeethareddy@gmail.com

ABSTRACT- In this paper, we gift some other fine-grained two-component verification (2FA) get right of entry to control framework for online distributed computing services. In unique, in our proposed 2FA get admission to manipulate framework, a function primarily based get right of entry to manipulate component is actualized with the want of both a client thriller key and a lightweight safety machine. As a patron can not get entry to the framework in the occasion that they do not maintain each, the aspect can upgrade the security of the framework, particularly in the ones conditions in which numerous clients have a comparable PC for electronic cloud services. Likewise, best based totally manipulate in the framework too empowers the cloud server to confine the get admission to to the ones clients with a comparable association of traits while saving customer safety, i.E., the cloud server simply realizes that the purchaser satisfies the specified predicate, yet has no clue on the proper character of the consumer. At lengthy final, we moreover do a reenactment to show the practicability of our proposed 2FA framework.

Keywords:- Fine-grained, two-factor, access control, Web services.

I. INTRODUCTION

In this paper, we present any other high-quality-grained -aspect authentication (2FA) get to control framework for electronic distributed computing administrations. In specific, in our proposed 2FA get to control framework, a assets based totally get to manipulate gadget is performed with the need of both a customer thriller key and a light-weight security system. As a consumer can not get to the framework inside the occasion that they don't keep both, the tool can improve the security of the framework, specifically in those situations where numerous clients have a similar PC for digital cloud administrations. Likewise, assets primarily based manage within the framework moreover empowers the cloud server to restriction the doorway to the ones customers with a comparable arrangement of traits at the same time as safeguarding customer security, i.E., the cloud server just realizes that the client satisfies the required predicate, but has no clue on the precise character of the customer. At lengthy closing, we likewise do a reproduction to expose the practicability of our proposed 2FA framework.

II. LITERATURE REVIEW

Joseph K. Liu and Duncan S. Wong [2] The key presentation difficulty in ring mark mainly the suggest the first forward comfortable ring

mark plot and the major key-included ring mark conspire. Forward comfy ring marks created inside the beyond is still included. In the other manner the alternate off of up to all mystery keys does now not permit any enemy to create a full-size key-covered ring mark for the rest of the eras. Patrick P. Tsang, Man Ho Au, Joseph K. Liu [4] Ring mark that offers unavoidable endorser secrecy and unconstrained amassing association. As of late IDbased ring mark plans were proposed and every one among them rely on bilinear pairings advocate the frst IDbased restriction "linkable" ring mark conspire. We underline that the namelessness of the genuine endorsers is kept up even against the private key generator (PKG) of the IDbased framework. At long ultimate we demonstrate to add persona escrow to the 2 plans. Due to the dierent degrees of endorser obscurity. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen [7] Cloud interfaces to abusing the cloud administrations for attacks on different systems.The fundamental problem that the allotted computing worldview verifiably contains is that of comfy outsourcing of sensitive and also businessbasic statistics and techniques. At the point when considering using a cloud management the customer have to realize approximately the manner that every one statistics given to the cloud dealer depart the claim manipulate and security circle. Much greater if sending statistics preparing packages to the cloud (with the aid of IaaS or PaaS). A cloud supplier increases complete control on those strategies Hence a strong accept as true with dating between the cloud supplier and the cloud consumer is viewed as a fashionable essential in dispensed computing.

Ming Li Member, IEEE, Shucheng Yu [8] A excessive stage of patient security is ensured at the equal time through misusing multi-electricity ABE conspire moreover empowers dynamic adjustment of get to strategies or report characteristics bolsters effective on-demand patron/assets renouncement and wreck-glass get entry to underneath disaster situations. Broad logical and test comes about.

Mihir Bellare and Sara K. Miner[9] Forward security is to make certain some components of mark protection against the risk of introduction of the thriller marking key yet basically particularly without requiring dissemination or ensured stockpiling gadgets and without increasing key administration fees. Forward security" is but that a qualification can be made between the security of files regarding (which means dated in) the past (the time previous key presentation) and people referring to the duration after key advent.

III. SYSTEM ARCHITECTURE

A naive wondering to attain our purpose is to use a ordinary ABS and genuinely split the consumer mystery key into elements. One component is kept by the consumer (saved inside the pc)even as another element is initialized into the security device. Special care ought to be taken in the process because normal ABS does not assure that the leakage of part of the secret key does no longer have an effect on the safety of the scheme at the same time as in 2FA, the attacker could have compromised one of the factors. Besides, the splitting ought to be finished in the sort of way that most of the computation load must be with the users pc because the protection tool is not imagined to be powerful. If get right of entry to manipulate given to any unique user , We cannot take again this Access authority from that person and also malicious activity offers to block

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

unique user ,we can't revocate it. Our device consists of the subsequent entities:

- Trustee: It is chargeable for generating all gadget parameters and initialized the security tool.
- Attribute-issuing Authority: It is responsible to generate user secret key for every user in step with their attributes.
- User: It is the player that makes authentication with the cloud server. Each consumer has a mystery key issued through the characteristic-issuing authority and a safety tool initialized via the trustee.
- Cloud Service Provider: It presents services to nameless legal customers. It interacts with the consumer throughout the authentication system.

(a) User Key Generation Process

(b) Access Authentication Process

Fig 1: Proposed System Architecture:

A. Our Contribution

In this paper, we propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.

With this device, our protocol provides a 2FA security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through USB) in order to authenticate the user for accessing the cloud. The user can be granted access only if he has both items. Furthermore, the user cannot use his secret key with another device belonging to others for the access.

Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same

time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user.

To show the practicality of our system, we simulate the prototype of the protocol. In the next section, we will review some related works that are related to our concept.

IV. RELATED WORKS

We review some related works including attribute-based cryptosystems and access control with security device in this section.

A. Attribute-Based Cryptosystem

Attribute-based encryption (ABE) [20], [39] is the cornerstone of attribute-based cryptosystem. ABE enables fine-grained access control over encrypted data using access policies and associates attributes with private keys and ciphertexts. Within this context, ciphertext-policy ABE (CP-ABE) [6] allows a scalable way of data encryption such that the encryptor defines the access policy that the decryptor (and his/her attributes set) needs to satisfy to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data with respect to the pre-defined policy.

This can eliminate the trust on the storage server to prevent unauthorised data access. Besides dealing with authenticated access on encrypted data in cloud storage service [21], [23], [24], [27]–[29], [36], [42], [43], ABE can also be used for access control to cloud computing service, in a similar way as an encryption scheme can be used for authentication purpose: The cloud server may encrypt a random message using the access policy and ask the user to decrypt. If the user can successfully decrypt the ciphertext (which means the user's attributes set satisfies the prescribed policy), then it is allowed to access the cloud computing service.

In addition to ABE, another cryptographic primitive in attribute-based cryptosystem is attribute-based signature (ABS) [35], [38], [41]. An ABS scheme enables a user to sign a message with fine-grained control over identifying information. Specifically, in an ABS scheme, users obtain their attribute private keys from an attribute authority. Then they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that the signer's attributes satisfy the signing predicate if the signature is valid. At the same time, the identity of signer remains hidden. Thus it can achieve anonymous attribute based access control efficiently. Recently, Yuen *et al.* [47] proposed an attribute-based access control mechanism which can be regarded as the interactive form of ABS.

B. Access Control With Security Device

1) Security Mediated Cryptosystem: Mediated cryptography was first introduced in [8] as a method to allow immediate revocation of public keys. The basic idea of mediated cryptography is to use an on-line mediator for every transaction. This on-line mediator is referred to a SEM (Security Mediator) since it provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer. Recently, an attribute-based version of SEM was proposed in [13]. The notion of SEM cryptography was further modified as security mediated certificateless (SMC) cryptography [14], [46]. In a SMC system, a user has a secret key, public key and an identity. In the signing or decryption algorithm, it requires the secret key and the SEM together. In the signature

verification or encryption algorithm, it requires the user public key and the corresponding identity. Since the SEM is controlled by an authority which is used to handle user revocation, the authority refuses to provide any cooperation for any revoked user. Thus revoked users cannot generate signature or decrypt ciphertext. Note that SMC is different from our concept. The main purpose of SMC is to solve the revocation problem. Thus the SME is controlled by the authority. In other words, the authority needs to be *online* for every signature signing and ciphertext decryption. The user is not anonymous in SMC. While in our system, the security device is controlled by the user. Anonymity is also preserved.

In addition to ABE, another cryptographic primitive in attribute-based cryptosystem is attribute-based signature (ABS) [35], [38], [41]. An ABS scheme enables a user to sign a message with fine-grained control over identifying information. Specifically, in an ABS scheme, users obtain their attribute private keys from an attribute authority. Then they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that the signer's attributes satisfy the signing predicate if the signature is valid. At the same time, the identity of signer remains hidden. Thus it can achieve anonymous attribute based access control efficiently. Recently, Yuen *et al.* [47]proposed an attribute-based access control mechanism which can be regarded as the interactive form of ABS.

2) Key-Insulated Cryptosystem: The paradigm of key insulated cryptography was introduced in [17]. The general idea of key-insulated security was to store long-term keys in a physically-secure but computationally-limited device.

Short-term secret keys are kept by users on a powerful but insecure device where cryptographic computations take place. Short term secrets are then refreshed at discrete time periods via interaction between the user and the base while the public key remains unchanged throughout the lifetime of the system. At the beginning of each time period, the user obtains a partial secret key from the device. By combining this partial secret key with the secret key for the previous period, the user renews the secret key for the current time period. Different from our concept, key-insulated cryptosystem requires all users to update their keys in every time period. The key update process requires the security device. Once the key has been updated, the signing or decryption algorithm does *not* require the device anymore within the same time period. While our concept *does* require the security device every time the user tries to access the system. Furthermore, there is no key updating required in our system.

V. OVERVIEW

A. Intuition

A naive thinking to achieve our goal is to use a normal ABS and simply split the user secret key into two parts. One part is kept by the user (stored in the computer) while another part is initialized into the security device. Special care must be taken in the process since normal ABS does not guarantee that the leakage of part of the secret key does not affect the security of the scheme while in two 2FA, the attacker could have compromised one of the factors. Besides, the splitting should be done in such a way that most of the computation load should be with the user's computer since the security device is not supposed to be powerful.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

We specifically design our system in another manner. We do not split the secret key into two parts. Instead, we introduce some additional unique information stored in the security device. The authentication process requires this piece of information together with the user secret key. It is guaranteed that missing either part cannot let the authentication pass. There is also a linking relationship between the user's device and the secret key so that the user cannot use another user's device for the authentication. The communication overhead is minimal and the computation required in the device is just some lightweight algorithms such as hashing or exponentiation over group G*T* .2 All the heavy computations such as pairing are done on the computer.

The idea of our system is illustrated in Figure 1.

B. Entities

Our system consists of the following entities:

• Trustee: It is responsible for generating all system parameters and initialise the security device.

• Attribute-issuing Authority: It is responsible to generate user secret key for each user according to their attributes.

• User: It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.

• Cloud Service Provider: It provides services to anonymous authorised users. It interacts with the user during the authentication process.

C. Assumptions

The focus of this paper is on preventing private information leakage at the phase of access authentication. Thus we make some assumptions on system setup and communication channels. We assume each user communicates with he cloud service provider through an anonymous channel [26], [37] or uses IP-hiding technology. We also assume that rustee generates the security parameters according to the algorithm prescribed. Other potential attacks, such as IP hijacking, distributed denial-of-service attack, man-in-the-middle attack, etc., are out of the scope of this paper.

D. Threat Model

In this paper, we consider the following threats:

1) Authentication: The adversary tries to access the system beyond its privileges. For example, a user with attributes {Student, Physics} may try to access the system with policy "Staff" AND "Physics". To do so, he may collude with other users.

2) Access without Security Device: The adversary tries to access the system (within its privileges) without the security device, or using another security device belonging to others.

3) Access without Secret Key: The adversary tries to access the system (within its privileges) without any secret key.

It can have its own security device.

4) Privacy: The adversary acts as the role of the cloud server and tries to find out the identity of the user it is interacting with.

VI. OUR PROPOSED SYSTEM

A. Specification of the Security Device

We assume the security device employed in our system satisfies the following requirements.

1) *Tamper-resistance.* The content stored inside the security device is not accessible nor modifiable once it is initialized. In addition, it will always follow the algorithm specification.

2) *Capability.* It is capable of evaluation of a hash function. In addition, it can generate

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

random numbers and compute exponentiations of a cyclic group defined over a finite field.

B. Efficiency Analysis

We analyze the efficiency of our protocol in two parts. In the first part, we identify the major operations for the authentication protocol. The symbols *P*, *E*1, *ET* represent. We consider three different platforms, namely, a computer, a smart phone and a smart card. For the time cost on a smartcard, we use the benchmark result from [40]. The configuration of our test platforms, namely, Computer and Smartphone, The time and space cost on the three platforms are listed. Details of the experiment settings are discussed below. We use Miracl library version 5.2. The base field is a prime field *Fq*, where *q* is a 512-bit prime whose value is:

8*BA*2*A*5229*BD*9*C*57*CFC*8*ACEC*76*DFDBF*3*E*
3*E*1952*C*6*B*3193*ECF*5*C*571*FB*502*FC*5*DF*4
10*F*9267*E*9*F*2*A*605*BB*0*F*76*F*52*A*79*E*8043
*BF*4*AF*0*EF*2*E*9*FA*78*B*0*F*1*E*2*CDFC*4*E*8549*B*

The elliptic curve is defined by the equation $y2 = x3 + 1 \bmod q$. The group G (as well as G*T*) is of order $p =$ 800000000000000000000000000000000000020001, where *p* is a 160-bit prime. The pairing is Tate pairing. Listed the number of operations and communication for an authentication transaction. Recall that *n* is the size of the attribute universe, _ and *m* are the length and width of the span program representing the access policy.

1) Simulation: Assume the total number of attributes in the system is 100. In other words, the attribute universe

A = {1, . . . , 100}. In the following we estimate the efficiency

of our system using policy of the following format:

$$\bigvee_{i=1}^{a}\left(\bigwedge_{j=1}^{b}(\text{attr}_{i,j})\right),$$

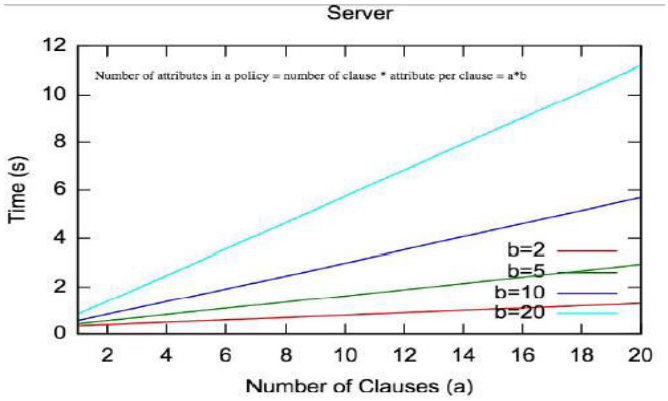

Fig. 2. Running time of the Auth protocol

VII. CONCLUSION

In this venture, we've supplied a new 2FA (including each consumer mystery key and a lightweight security device) get admission to manage machine for internet-primarily based cloud computing offerings. Based on the characteristic-primarily based get entry to control mechanism, the proposed 2FA get right of entry to control device has been identified to no longer only allow the cloud server to restrict the get right of entry to to the ones users with the identical set of attributes however also keep user privacy. Detailed protection analysis shows that the proposed 2FA get right of entry to control device achieves the favored security requirements. Through overall performance evaluation, we validated that the development is viable. We depart as future work to further improve the efficiency even as keeping all first-class functions of the system.

VIII. 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 *k*-TAA," 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, "Ciphertextpolicy 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.