International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Safe Outsourced Attribute-Based Signatures

M. Manjusha
(M.Tech student) Deportment of Computer science and Engineering Aurora's Technological and Research Institute
Email id:mmunagala7@gmail.com
Mrs. T. Padmaja
(Associate Professor) Deportment of CSE and IT Aurora's Technological and Research Institute

Abstract:
Attribute-based signature (ABS) is a useful variant of digital signature, which enables users to sign messages over attributes without revealing any information other than the fact that they have attested to the messages. However, heavy computational cost is required during signing in existing work of ABS, which grows linearly with the size of the predicate formula. As a result, this presents a significant challenge for resource-limited users (such as mobile devices) to perform such heavy computation independently. Aiming at tackling the challenge above, we propose and formalize a new paradigm called OABS, in which the computational overhead at user side is greatly reduced through outsourcing such intensive computation to an un trusted signing-cloud service provider (S-CSP). Furthermore, we apply this novel paradigm to existing ABS to reduce complexity and present two schemes, i) in the first OABS scheme, the number of exponentiations involving in signing is reduced from O(d) to O(1) (nearly three), where d is the upper bound of threshold value defined in the predicate; ii) our second scheme is built on Herranz et al's construction with constant-size signatures. The number of exponentiations in signing is reduced from O(d2) to O(d) and the communication overhead is O(1). Security analysis demonstrates that both OABS schemes are secure in terms of the unforgeability and attribute- signer privacy definitions specified in the proposed security model. Finally, to allow for high efficiency and exibility, we discuss extensions of OABS and show how to achieve accountability and outsourced verification as well.

I INTRODUCTION

As a novel cryptographic primitive, attribute-based signature (ABS) enables a party to sign a message with fine-grained access control over identifying information. Specifically, in an ABS system, users obtain their attribute private keys from an attribute authority, with which they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that whether the signer's attributes satisfy the signing predicate while remaining completely ignorant of the identity of signer. ABS is much useful in a wide range of applications including private access control, anonymous credentials, trust negotiations, distributed access control for ad hoc networks, attribute-based messaging, etc. However, one of the main eficiency drawbacks of ABS is that the time required to sign grows with the complexity of predicate formula. More precisely, the generation of signature requires a large number of module exponentiations, which commonly grows linearly with the size of the predicate formula. Although the traditional desktop computers should be able to quite easily handle IEEE Transactions on Parallel and Distributed Systems,(Volume:PP , Issue: 99) Year:2014 such task for typical formula size, this presents a significant challenge for users that manage and view private data on mobile devices where processors are often one to two orders of magnitude slower than their desktop counterparts. The recently emerged next-generation computing paradigm, named cloud computing, provides the feasibility to reduce the computation overhead at user side by outsourcing the computation of signing to a signing-cloud service provider (S-CSP). Though promising as it is, this paradigm also brings forth new challenge when users intend to outsource ABS on untrusted cloud server. Specifically, by the reason that some private information is involved in the outsourced signing operation, it demands a way to prevent the untrusted S-CSP from learning any private information about signer. Moreover, since the cloud service is typically required to be paid in the commercial setting, it also demands a way for signer to guarantee the accountability on cloud

service provider once the signature is not generated correctly.

II SYSTEM ANALYSIS

Existing System:
Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorize users.

These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

DisAdvantages Of Exixting System:
Software update/patches- could change security settings, assigning privilegestoo low, or even more alarmingly too high allowing access to your data by other parties.

Security concerns- Experts claim that their clouds are 100% secure - but it willnot be their head on the block when things go awry. It's often stated that cloudcomputing security is better than most enterprises. Also, how do you decidewhich data to handle in the cloud and which to keep to internal systems once decided keeping it secure could well be a full-time task?

Control- Control of your data/system by third-party. Data - once in the cloudalways in the cloud! Can you be sure that once you delete data from your cloudaccount will it not exist any more... ...or will traces remain in the cloud

Proposed System :
This proposed system addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.

We propose a hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extends the ciphertext-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

Advantages Of Proposed System :
- Low initial capital investment
- Shorter start-up time for new services
- Lower maintenance and operation costs
- Higher utilization through virtualization
- Easier disaster recovery

More specifically, we associate each data file with a set of attributes, and assign each user an expressive access structure whichis defined over these attributes. To enforce this kind of access control, we utilize KP-ABE to escort data encryption keys of data files. Such construction enables us to immediately enjoy fine-grainedness of access control. However, this construction, if deployed alone, would introduce heavy computation overhead and cumbersome onlineburden towards the data owner, as he is in charge of all the operations of data/user management. Specifically, such an issue is mainly caused by the operation of user revocation, which inevitably requires the data owner to re-encrypt all the data files accessible to the leaving user, oreven needs the data owner to stay online to update secret keys for users. To resolve this challenging issue and make the construction suitable for cloud computing, we uniquely combine PRE with KP-ABEand enable the data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents. Such a construction allows the data owner to control access of his data files with a minimal overhead in terms of computation effort and online time, and thus fits well into the cloud environment. Data confidentiality is also achieved since Cloud Serversare not able to learn the plaintext of any data file in our construction. For further reducing the computation overhead on Cloud Servers andthus saving the data owner's investment, we take advantage of thelazy re-encryption technique and allow Cloud Servers to "aggregate "computation tasks of multiple system operations. As we will discuss in section V-B, the computation complexity on Cloud Servers is eitherproportional to the number of system attributes, or linear to the size of the user access structure/tree, which is independent to the number of users in the system. Scalability is thus achieved. In addition, our construction also protects user access privilege information againstCloud Servers. Accountability of user secret key can also be achieved by using an enhanced scheme of KP-ABE.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

III LITERATURE SURVEY

About the Domain

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture. In the last several years, cloud computing has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive attention from both academia and industry. Cloud computing holds the promise of providing computing as the fifth utility after the other four utilities (water, gas, electricity, and telephone). The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on. Different service-oriented cloud computing models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Numerous commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2, Amazon's S3, and IBM's Blue Cloud are IaaS systems, while Google App Engine and Yahoo Pig are representative PaaS systems, and Google's App and Salesforce's Customer Relation Management (CRM) System belong to SaaS systems. With these cloud computing systems, on one hand, enterprise users no longer need to invest in hardware/software systems or hire IT professionals to maintain these IT systems, thus they save cost on IT infrastructure and human resources; on the other hand, computing utilities provided by cloud computing are being offered at a relatively low price in a pay-as-you-use style.

Literature Survey

1) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility

With the significant advances in Information and Communications Technology (ICT) over the last half century, there is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). This computing utility, like all other four existing utilities, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community. To deliver this vision, a number of computing paradigms have been proposed, of which the latest one is known as Cloud computing. Hence, in this paper, we define Cloud computing and provide the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs). We also provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation. In addition, we reveal our early thoughts on interconnecting Clouds for dynamically creating global Cloud exchanges and markets. Then, we present some representative Cloud platforms, especially those developed in industries, along with our current work towards realizing market-oriented resource allocation of Clouds as realized in Aneka enterprise Cloud technology. Furthermore, we highlight the difference between High Performance Computing (HPC) workload and Internet-based services workload. We also describe a meta-negotiation infrastructure to establish global Cloud exchanges and markets, and illustrate a case study of harnessing 'Storage Clouds' for high performance content delivery. Finally, we conclude with the need for convergence of competing IT paradigms to deliver our 21st century vision.

2) Methods and limitations of security policy reconciliation

A security policy is a means by which participant session requirements are specified. However, existing frameworks provide limited facilities for the automated reconciliation of participant policies. This paper considers the limits and methods of reconciliation in a general-purpose policy model. We identify an algorithm for efficient two-policy reconciliation, and show that, in the worst-case, reconciliation of three or more policies is intractable. Further, we suggest efficient heuristics for the detection and resolution of intractable reconciliation. Based upon the policy model, we describe the design and implementation of the Ismene policy language. The expressiveness of Ismene, and indirectly of our model, is demonstrated through the representation and exposition of policies supported by existing policy languages. We conclude with brief notes on the integration and enforcement of Ismene policy within the Antigone communication system.

3) A unified scheme for resource protection in automated trust negotiation

Automated trust negotiation is an approach to establishing trust between strangers through iterative disclosure of digital credentials. In automated trust negotiation, access control policies play a key role in protecting resources from unauthorized access. Unlike in traditional trust management systems, the access control policy for a resource is usually unknown to the party requesting access to the resource, when trust negotiation starts. The negotiating parties can rely on policy disclosures to learn each other's access control requirements. However a policy itself may also contain sensitive information. Disclosing policies' contents unconditionally may leak valuable business information or jeopardize individuals' privacy. In this paper we propose UniPro, a unified scheme to model protection of resources, including policies, in trust negotiation. UniPro improves on previous work by modeling policies as first-class resources, protecting them in the same way as other resources, providing fine-grained control over policy disclosure, and clearly distinguishing between policy disclosure and policy satisfaction, which gives users more flexibility in expressing their authorization requirements. We also show that UniPro can be used with practical negotiation strategies without jeopardizing autonomy in the choice of strategy, and present criteria under which negotiations using UniPro are guaranteed to succeed in establishing trust.

4) Ciphertext-policy attributebased encryption

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

5) Fuzzy identity based encryption

We introduce a new type of Identity Based Encryption (IBE) scheme that we call Fuzzy Identity Based Encryption. A Fuzzy IBE scheme allows for a private key for an identity id to decrypt a ciphertext encrypted with another identity id # if and only if the identities id and id # are close to each other as measured by some metric (e.g. Hamming distance). A Fuzzy IBE scheme can be applied to enable encryption using biometric measurements as identities. The error-tolerance of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently contain some amount of noise during each measurement.

IV MODULE IMPLEMENTATION

Number of Modules

After careful analysis the system has been identified to have the following modules:

1. Cloud Computing Module.
2. Attribute Based Signature Module.
3. OutsourceABS Computation Module.
4. OABS With Outsource Verification Module.

1. Cloud Computing Module:

Cloud computing, provides the feasibility to reduce the computation overhead at user side by outsourcing the computation of signing to a signing-cloud service provider (S-CSP). This presents a significant challenge for users that manage and view private data on mobile devices where processors are often one to two orders of magnitude slower than their desktop counterparts. We employ a hybrid private key by introducing a default attribute for all the users in the system. The private key component for user's attributes (denoted as outsourcing key OK in this paper) which is to be utilized by S-CSP to compute the outsourced signature; ii) the private key component for the default attribute which is to be utilized by signer to generate a normal ABS signature from the outsourced signature returned from S-CSP.

2. Attribute Based Signature Module:

Attribute-based signature (ABS) enables a party to sign a message with fine-grained access control over

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

identifying information. Specifically, in an ABS system, users obtain their attribute private keys from an attribute authority, with which they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that whether the signer's attributes satisfy the signing predicate while remaining completely ignorant of the identity of

signer. ABS is much useful in a wide range of applications including private access control, anonymous credentials, trust negotiations, distributed access control for ad hoc networks, attribute-based messaging.

3. Outsource ABS Computation Module:

Outsourced attribute-based signature scheme OABS consists of five probabilistic polynomial-time algorithms below:

Setup: It takes as input the security parameter _, attribute universe U and an auxiliary information d. It outputs the public key PK and the master key MK.

Key Gen (MK; Ω) : For each user's private key request on attribute set Ω, the private key generation algorithm takes as input the master key MK and the attribute set Ω. It outputs the user's private key SK and the outsourcing key OK.

Sign out (OK; Ω; _): The outsourced signing algorithm takes as input the outsourcing key OK, the corresponding attribute set Ω and the predicate _. It outputs the partial signature _part.

Sign (SK;M; _part; _) : The signing algorithm takes as input the private key SK, the message M, the partial signature _part and the corresponding predicate _. It outputs the signature _ of message M with the predicate _.

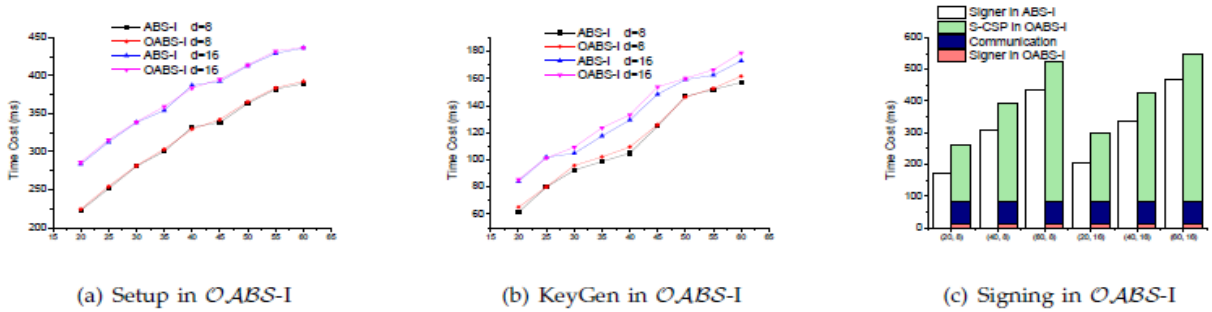
Verify (M; _; _; PK) : The verifying algorithm takes as input a message M, the signature _,the predicate _ and public key PK. It outputs 1 if the original signature is deemed valid and 0 otherwise.

5. OABS With Outsource Verification Module:

This technique can only guarantee the correctness of outsourced computation with accountability, it cannot check the correctness and detect the misbehaves of S-CSP on spot. To solve this problem, we provide another solution to verify the outsourced signature with low computational cost by introducing another independent entity called verifying-cloud service provider (V-CSP). We also introduce an assumption that the S-CSP and V-CSP will not collude. Actually, such assumption has also appeared to deal with the problem of secure outsourcing computation as well. Accordingly, an outsourced verification protocol, including the transformation algorithm for outsourced verification Transfer, the outsourced verifying algorithm Verifyout and the verifying algorithm Verify, replaces the original verifying algorithm in OABS definition.

Experimental Results for OABS-I

In Fig. 1(a), we show the efficiency comparison for the setup phase between OABS-I and ABS-I. In this evaluation, we fix the threshold d = 8 and 16 respectively, and vary the number of attributes in the universe from 60 to 100. Theoretically, the proposed scheme OABS-I requires a little more time than the original one ABS-I. More specifically, compared with the original scheme ABS-I, our construction requires an additional initialization for a default attribute θ for facilitating outsourcing. However, we have to point out that the additional time is negligible in the case of a large universe. Though the figure, we can deduce that the schemes OABS-I and ABS-I have the same computational complexity in the Setup phase (note that the two curves almost overlap with each other).



(a) Setup in $\mathcal{OABS}$-I (b) KeyGen in $\mathcal{OABS}$-I (c) Signing in $\mathcal{OABS}$-I

Fig. 1. Efficiency Comparison for Setup, KeyGen and Signing between OABS-I and ABS-I

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Fig. 1(b) illustrates the efficiency comparison in the KeyGen phase between two schemes . It is not surprising to see that OABS-I also requires (very) little more time than ABS-I. This is because the attribute authority has to additionally issue private keys for the new introduced default attribute θ, involving nearly two exponentiations. Similarly, the additional time is negligible in the case of a large universe. Therefore, the two schemes have almost the same computational complexity in the KeyGen phase.

The performance of signing phase in both OABS-I and ABS-I is shown in Fig. 1(c). Note that in this experiment, we assume that signer has been assigned with the attribute private key for all the attributes in the universe U of size 100, and randomly pick $|\Omega^*|$ attributes from U to prove that he/she has at least d attributes of Ω^* (i.e., the signing predicate is Υ_{d,Ω^*}), where d is the threshold value. The efficiency in Fig 1(c) is evaluated in several cases for $|\Omega^*|$ = 20, 40, 60 and d = 8, 16, respectively. It is clear that OABS- I is overall slightly expensive regarding to computation and communication complexity because we consider the issue of secure outsourcing. Specifically, compared with ABS-I, our scheme supports private delegation, which sacrifices slight efficiency (e.g. some computations involving the default attribute θ) for preserving the privacy of signer and his/her signing key. However, concerning on the local computation performed by the signer, our scheme OABS-I achieves much nearly constant performance compared with the linear increasing efficiency of ABS-I. This advantage allows our scheme to be applied for the resourceconstraint devices to complete the task of ABS.

V CONCLUSION

Aiming at eliminating the most computational overhead at signer, we introduce outsourcing computation into ABS and propose two eficient OABS schemes. With the help of C-CSP, our first scheme requires only three exponentiations for signing a single message at signer side. Our second scheme is built on Herranz et al.'s work [21], but reduces the number of exponentiations from O(d2) to O(d), where d is the upper bound of the threshold value. Furthermore, the communication overhead between the signer and S-CSP is very low which requires only three group elements. We discuss the extensions for OABS including accountability and outsourced verification and show practical solutions as well.

REFERENCES

[1] Atallah, M.J., Frikken, K.B.: Securely outsourcing linear algebra computations. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. pp. 48{59. ASIACCS'10, ACM, New York, NY, USA (2010)

[2] Atallah, M.J., Li, J.: Secure outsourcing of sequence comparisons. International Journal of Information Security 4, 277{287 (2005)

[3] Atallah, M.J., Pantazopoulos, K., Rice, J.R., Spa_ord, E.E.: Secure outsourcing of scienti_c computations. In: Zelkowitz, M.V. (ed.) Trends in Software Engineering, Advances in Computers, vol. 54, pp. 215 { 272. Elsevier (2002)

[4] Benjamin, D., Atallah, M.J.: Private and cheating-free outsourcing of algebraic computations. In: Proceedings of the 2008 Sixth Annual Conference on Privacy, Security and Trust. pp. 240{245. PST'08, IEEE Computer Society, Washington, DC, USA (2008)

[5] Bicakci, K., Baykal, N.: Saots: A new e_cient server assisted signature scheme for pervasive computing. In: Hutter, D., Mller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing, Lecture Notes in Computer Science, vol. 2802, pp. 187{200. Springer Berlin / Heidelberg (2004)

[6] Bicakci, K., Baykal, N.: Server assisted signatures revisited. In: Okamoto, T. (ed.) Topics in Cryptology { CT-RSA 2004, Lecture Notes in Computer Science, vol. 2964, pp. 1991{1992. Springer Berlin / Heidelberg (2004)

[7] Boneh, D., Ding, X., Tsudik, G.: Fine-grained control of security capabilities. ACM Trans. Internet Technol. 4(1), 60{82 (2004)

[8] Boneh, D., Ding, X., Tsudik, G., Wong, C.M.: A method for fast revocation of public key certi_cates and security capabilities. In: USENIX Security Symposium (2001)

[9] Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) Advances in Cryptology { CRYPTO, Lecture Notes in Computer Science, vol. 3621, pp. 258{275. Springer Berlin / Heidelberg (2005)

[10] Canetti, R., Riva, B., Rothblum, G.N.: Two 1-round protocols for delegation of computation. Cryptology ePrint Archive, Report 2011/518 (2011)