Identity Based Encryption With Outsourced Revocation In Cloud Computing

Pooja Dnyaneshwar Mali[1], Rupali Rambhau Mole[2], Bharti Vijay Chandanshiv[3], Prajakta Pralhad Ingle[4], Prof. Y. B Jadhao[5], Prof. A. S. Solanke[6]

[1, 2, 3, 4] Dept of Computer Science & Engineering

[5, 6] Assistant Prof., Dept of Computer Science & Engineering

[1, 2, 3, 4, 5, 6] *Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*

Abstract- *Advancements in cloud computing are leading to a promising future for collaborative cloud computing (CCC), where globally-scattered distributed cloud resources belonging to different organizations or individuals (i.e., entities) are collectively used in a cooperative manner to provide services. Due to the autonomous features of entities in CCC, the issues sof resource management and Reputation management must be jointly addressed in order to ensure the successful deployment of CCC. However, these two issues have typically been addressed separately in previous research efforts, and simply combining the two systems generates double overhead. Also, previous resource and reputation management methods are not sufficiently efficient or effective. By providing a single reputation value for each node, the methods cannot reflect the reputation of a node in providing individual types of resources. By always selecting the highest-reputed nodes, the methods fail to exploit node reputation in resource selection to fully and fairly utilize resources in the system and to meet users' diverse QoS demands. We propose a CCC platform, called Harmony, which integrates resource management and reputation management in a harmonious manner. Harmony incorporates three key innovations: integrated multi-faceted resource/reputation management, multi-QoS-oriented resource selection, and price-assisted resource/reputation control. The trace data we collected from an online trading platform implies the importance of multi-faceted reputation and the drawbacks of highest-reputed node selection. Simulations and trace-driven experiments on the real-world Planet Lab test bed show that Harmony outperforms existing resource management and reputation management systems in terms of QoS, efficiency and effectiveness*

Keywords- Cloud Computing,Node, QoS, Simulations, Planet Lab Test.

I. INTRODUCTION

Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys. Therefore, its possible to decrypt the message directly with user identity. Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such cipher text. Though IBE allows an arbitrary string as the public key which is considered as an appealing advantage over PKI, it demands an efficient revocation mechanism. Specifically, if the private keys of some users get compromised, we must provide a mean to revoke such users from system. In PKI setting, revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques. Nevertheless, the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. But this mechanism would result in an overhead load at PKG. In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows.

In 2008, Boldyreva, Goyal and Kumar presented a revocable IBE scheme. Their scheme is built on the idea of fuzzy IBE primitive but utilizing a binary tree data structure to record users' identities at leaf nodes. Therefore, key-update efficiency at PKG is able to be significantly reduced from linear to the height of such binary tree (i.e. logarithmic in the number of users). [1]

II. SYSTEM DISCUSSED

2.1 Existing System

Cloud resource orchestration (i.e., resource provision, configuration, utilization and decommission across a distributed set of physical resources in clouds) has been

studied in recent years, these two issues have typically been addressed separately. Simply building and combining individual resMgt and repMgt systems in CCC will generate doubled, prohibitively high overhead. Moreover, most previous resMgt and repMgt approaches are not sufficiently efficient or effective in the large-scale and dynamic environment of CCC. Previous repMgt systems neglect resource heterogeneity by assigning each node one reputation value for providing all of its resources. In existing system claim that node reputation is multi-faceted and should be differentiated across multiple resources (e.g., CPU, bandwidth, and memory). For example, a person trusts a doctor for giving advice on medical issues but not on financial issues. Similarly, a node that performs well for computing services does not necessarily perform well for storage services. Thus, previous repMgt systems are not effective enough to provide correct guidance for trustworthy individual resource selection.

2.2 Proposed System

We propose a comprehensive solution for storing and maintaining log records in a server operating in a cloud-based environment. We address security and integrity issues not only just during the log generation phase, but also during other stages in the log management process, including log collection, transmission, storage, and retrieval. The major contributions of this paper are as follows. We propose architecture for the various components of the system and develop cryptographic protocols to address integrity and confidentiality issues with storing, maintaining, and querying log records at the honest but curious cloud provider and in transit. In this project, we introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key-update, leaving only a constant number of simple operations for PKG and eligible users to perform locally. In our scheme, as with the suggestion in , we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update Digital Object Indentifier and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decryptability, unrevoked users needs to periodically request on key-update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP). Compared with the previous work [4], our scheme does not have to re-issue the whole private keys, but just need to update a lightweight component of it at a specialized entity KU-CSP. [2]
We also specify that

1) with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP.
2) No secure channel or user authentication is required during key-update between user and KU-CSP. Furthermore, we consider to realize revocable IBE with a semihonest KU-CSP.

To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model.

Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.[3][4]

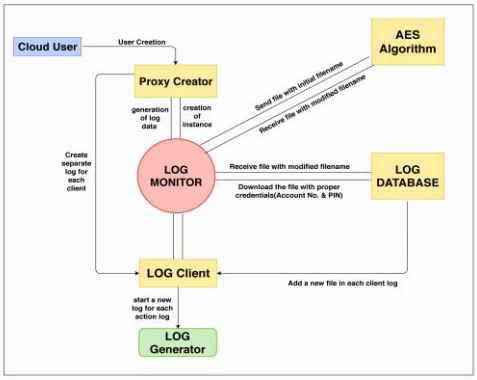

Fig.1 Proposed Architecture

III. ALGORITHM

D-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.ID-based encryption was proposed by Adi Shamir in 1984. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII

string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as *master key*).[4]

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data?the data to be encrypted. This array we call the state array.

You take the following aes steps of encryption for a 128-bit block:

Derive the set of round keys from the cipher key.

1. Initialize the state array with the block data (plaintext).
2. Add the initial round key to the starting state array.
3. Perform nine rounds of state manipulation.
4. Perform the tenth and final round of state manipulation.
5. Copy the final state array out as the encrypted data (ciphertext).[5][6]

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.
The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D0 [9]

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- SubBytes
- ShiftRows

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,” in Advances in Cryptology – CRYPTO’98. Springer, 1998.
[2] V. Goyal, “Certificate revocation using fine grained certificate space partitioning,” in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.
[3] F. Elwailly, C. Gentry, and Z. Ramzan, “Quasimodo: Efficient certificate validation and revocation,” in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.
[4] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.
[5] Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS ’08. New York, NY, USA: ACM, 2008, pp. 417–426.
[6] Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557–557.
[7] R. Canetti, B. Riva, and G. N. Rothblum, “Two 1-round protocols for delegation of computation,” Cryptology ePrint Archive, Report 2011/518, 2011.
[8] U. Feige and J. Kilian, “Making games short (extended abstract),” in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC ’97. New York, NY, USA: ACM, 1997, pp. 506–516.
[9] http://etutorials.org/Networking/802.11+security.+wi-fi+ protected+ access+ and+ 802.11i/Appendixes Appendix+ A.+ Overview of+the+ AES+ Block+ Cipher/Steps+ in+the+ AES+ Encryption+Process/