ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

DYNAMIC IDENTITY BASED APPROACH TO CHECK DATA POSSESSION IN PUBLIC CLOUD SERVICE

[1]KALA.M, [2]ARIVUSELVI.P, [3]RAMYA.R[1,2,3]

Master of Engineering in Computer Science and Engineering

srikalai6632@gmail.com

[4]Ms.MAHALAKSHMI.C, M.E., *Assistant Professor*[4], *Department of Computer Science and Engineering*

Bharathiyar Institute of Engineering for Women

Tamil Nadu, India

ABSTRACT

The clients would like to store their data to public cloud servers along with the rapid development of cloud computing. There is lot of security problems in the cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. When the user is confidential to admittance PCS, he will delegate its proxy to process his data and upload them. Remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data are kept intact without downloading the whole data. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. Generate two key to secure the file, one at the user site and one at the server site and the keys get distributed in the cloud by getting the authentication of the user. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis. The proposed ID-PUIC protocol can also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the original client's authorization.

Index Terms—Cloud computing, Identity-based cryptography, Proxy public key cryptography, Remote data integrity checking.

INTRODUCTION

Along with the rapid development of computing and com-munication technique, a great deal of data are generated. These massive data needs more strong computation resource and greater storage space. Over the last years, cloud computing satisfies the application requirements and grows very quickly. Essentially, it takes the data processing as a service, such as storage space, compute, information safety measures, *etc*. By using the public cloud platform, the clients are relieved of the burden for storage space management, common information contact with independent environmental location. Thus, more and more clients would like to store and process their data by using the remote cloud computing system. In public

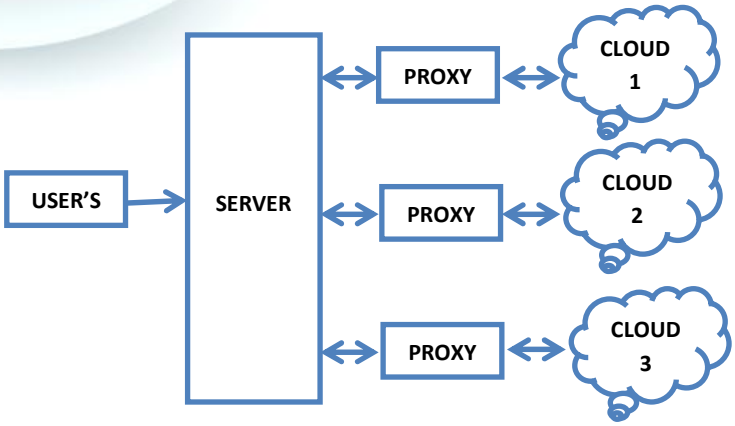
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

cloud computing, the clients store their massive data in the remote public cloud servers. Since the stored data is outside of the control of the clients, it entails the security risks in terms of confidentiality, integrity and availability of information and examine. Inaccessible information integrity examination is a primitive which can be used to convince the cloud clients that their data are kept intact. In some special cases, the data owner may be restricted to access the public cloud server, the data owner will delegate the task of data processing and uploading to the third party, for example the proxy. On the other side, the remote data

integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on identity-based public cryptography and proxy public key cryptography, we will study ID-PUIC protocol .

SYSTEM ARCHITECTURE

By means of identity-based open key cryptology, our future ID-PUIC procedure is well-organized while the credential administration is eliminated. ID-PUIC is a narrative proxy-oriented information uploading and isolated information reliability examination model in public cloud. We give the ceremonial system form and security form used for ID-PUIC protocol. After that, base on the bilinear pairings, we intended the first concrete ID-PUIC protocol. During the casual vision model, our designed ID-PUIC protocol is provably protected. Based on the original client's approval, our protocol can realize private checking, delegated checking and public checking. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and competence examination. Scheduled the additional tender, the proposed ID-PUIC protocol can also understand private remote information reliability inspection, delegated remote information reliability examination and public remote information reliability examination based on the original client's authorization. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity. In PKI, the considerable overheads come from the heavy certificate verification, certificate invention, release, revocation, renewal. In public cloud computing, the end devices may have low computation capacity, such as mobile phone. Identity-based public key cryptography can eliminate the complicated certificate management. In order to increase the efficiency, identity based proxy-oriented data uploading and remote data integrity checking is more attractive. Based on the original client's authorization, our protocol can realize private checking, delegated checking and public checking. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

Figure 1 System Architecture

RELATED WORK

Scalable and Efficient Provable Data Possession :

Storage outsourcing is a rising trend which prompts a number of interesting protection issue, numerous of which contain be at length investigate in the history. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The major issue is how to commonly, professionally and strongly authenticate that a storage space server is authentically storing its client's (potentially very large) outsourced data.

A review on dissimilar Encryption scheme and protection challenge in Cloud storage space structure :

Security of storing data in cloud is challenging Availability and irretrievability of the data to the authenticated ones is done with different levels of security pass. When compared to all the previous methods and security measures, the newly proposed threshold proxy re-encryption scheme and erasure codes over exponents improved security in this paper. The threshold proxy re-encryption scheme supports encoding and data forwarding, and partial decryption operations over encoded data in a distributed way.

A Proxy Re-Encryption Scheme with the Enforceability of Re-Encryption Keys against Collusion Attacks:

Proxy re-encryption (PRE) schemes are cryptosystems which allow a proxy who has a re-encryption key to convert a cipher text originally encrypted for one party into a cipher text which can be decrypted by another party. Wished-for the new security notion for PRE called enforceability of re-encryption keys against involvement attack," UFR key-CA for tiny. They planned the PRE scheme and claim that their schemes meet UFR key-CA.

Mutual Verifiable Provable Data Auditing in Public Cloud Storage:

Cloud storage space is at the present a searing investigate subject in sequence expertise. In cloud storage, information protection property such as information discretion, reliability and accessibility become more and more vital in many saleable applications. Freshly, many verifiable information possession schemes are proposed to care for information reliability.

Compact Proofs of Retrievability.

In a proof-of-irretrievability association, a information storage space hub convince a verifier that he is really store all of a client's data. The essential face up to construct systems that are together capable and provably protected – to facilitate is, it ought to be promising to extract the client's information from any proved that passes a confirmation prove.

Syntax of Proxy Signature Schemes:

A proxy mark scheme occupy a digital signature scheme for representative signing, a protocol

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

that users sprint in organize for one of them to assign the other as a proxy signer, assign algorithm to be use by substitute signers and a equivalent confirmation algorithm for substitute signature. Furthermore, the brawny identifiability assets noted in the opening suggests that in attendance be an algorithm that removes the individuality of the substitute signer on or after a substitute signature. This individuality is the usual figure identifying the user. We reminder that identities of a unique signer and its substitute can correspond in holder of self-delegation. The explanation we give uses communication space descriptors to identify the liberty of letters for which substitute signers are permitted to construct signatures.

A belief of safety for substitute cross scheme:

The opposition might fraudulent users and gain knowledge of their clandestine keys. The opponent can also insert fresh users and record public keys for them. These keys do not have be scattered according to the sharing distinct by the key-generation algorithm and, in standard, they can depend on, the public keys of straightforward users.

Proxy Re-Encryption Scheme

Proxy re-encryption (PRE) allows a proxy to transform an encryption of m under Alice's pub-lic key into another encryption of the same message under Bob's public key. The proxy, however, cannot learn the underlying message m, and thus both parties' privacy can be maintained. This primitive have various applications ranging from encrypted email forwarding securing distributed file systems , to Digital Rights Management (DRM) systems .In addition application-driven purposes, various works have shown connections between re-encryption (and its variants) with other crypto-graphic primitives, such as program obfuscation Thus studies along this line are both important and interesting for theory and practice.

PROPOSED SYSTEM

In public cloud security based on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a narrative proxy-oriented information uploading and remote information reliability examination model in public cloud. We provide the proper system copy and safety representation for ID-PUIC protocol. Then, based on the bilinear pairings, we intended the foremost actual ID-PUIC protocol. In the casual revelation replica, our planned ID-PUIC protocol is provably secure. Based on the unique client's agreement, our protocol can understand private examination, delegate examination and community examination. The real ID-PUIC protocol is provably protected and well-organized by using the formal security evidence and competence examination. On the additional hand, the proposed ID-PUIC protocol can also appreciate private inaccessible information reliability examination, delegated distant information reliability examination and public distant information reliability examination based on the original client's approval. TCP/IP sockets are used to realize consistent, bidirectional, constant, point-to-

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

point, stream-based associations among hosts on the Internet. A hollow can be used to attach Java's I/O system to other programs that may exist in moreover on the confined machine or on any other engine on the Internet. The making of a Socket item completely establishes a relationship among the client and server. There are no methods or constructors that overtly depiction the information of establishes that association. Here are two constructors used to create client sockets. Socket thread hostname, int port create a socket connecting the limited host to the named host and port; can throw an unidentified congregation omission or anIOException.Socket InetAddress ipAddress, int port Creates a socket using a preexisting InetAddress object and a port; can throw an IOException.

CONTRIBUTIONS

In community cloud, this paper focuses on the identity-based proxy-oriented information uploading and isolated information reliability examination. By using identity-based public key cryptology, our future ID-PUIC procedure is well-organized in view of the fact that the official document man-agreement is eliminated. ID-PUIC is a description proxy-oriented information uploading and in the sticks information reliability examination mode in public cloud. We grant the ceremonial system model and protection model for ID-PUIC protocol. Then, based on the bilinear pairings, we intended the initial tangible ID-PUIC protocol. In the accidental revelation model, our intended ID-PUIC protocol is provably protected. Based on the inventive client's approval, our protocol can apprehend personal examination, delegated examination and public examination.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

CONCLUSION

Aggravated via the submission needs, this paper proposes the novel protection concept of ID-PUIC in public cloud. The paper formalizes ID-PUIC's system model and protection model. Then, the first existing ID-PUIC protocol is planned by by means of the bilinear pairings practice. The existing ID-PUIC etiquette is provably protected and capable by using the proper protection confirmation and effectiveness investigation. On the other hand over, the proposed ID-PUIC protocol can also become conscious private isolated information reliability examination, delegated remote information reliability examination and public remote information reliability examination based on the innovative client's agreement.

REFERENCES

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, "Provable data possession at untrusted stores",*CCS'07*, pp.598-609, 2007.
2. G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and efficient provable data possession", *SecureComm 2008*, 20
3. C. C. Erway, A. K ¨upc¸ ¨u, C. Papamanthou, R. Tamassia, "Dynamic provable data possession", *CCS'09*, pp. 213-222, 2009.
4. E. Esiner, A. K ¨upc¸ ¨u, O Ozkasap, "Analysis and optimization on FlexDPDP: a practical solution for dynamic provable data possession", *Intelligent Cloud Computing*, LNCS 8993, pp. 65-83, 2014.
5. H. Guo, Z. Zhang, J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys", *Cryptology and Network Security*, LNCS 8813, pp. 20-33, 2014.
6. X. Liu, J. Ma, J. Xiong, T. Zhang, Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing", *Internet and Distributed Computing Systems*, LNCS 8223, pp. 238-251, 2013.
7. M. Mambo, K. Usuda, E. Okamoto, "Proxy signature for delegating signing operation", *CCS 1996*, pp. 48C57, 1996.
8. S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, K. Matsuura, "Re-encryption verifiability: how to detect malicious activities of a proxy in proxy re-encryption", *CT-RSA 2015*, LNCS 9048, pp. 410-428, 2015.
9. Y. Ren, J. Shen, J. Wang, J. Han, S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317-323, 2015.
10. E. Yoon, Y. Choi, C. Kim, "New ID-based proxy signature scheme with message recovery", *Grid and Pervasive Computing*, LNCS 7861, pp. 945-951, 2013.