Identity-Based Distributed Data Provable Data Possession In Multi Cloud Storage Using Blow Fish Algorithm

Aishwarya.G [1], Dr V.Saravanan [2]
Department of Information Technology
[1] PG Student Hindusthan College of Arts and Science, Coimbatore, India
[2] HOD & Associate Professor, Hindusthan College of Arts and Science, Coimbatore, India

Abstract- *The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie- Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.*

We give the formal definition, system model and security model. Then, a concrete ID-PUIC protocol is designed by using the bilinear pairings. The proposed ID-PUIC protocol is provably secure based on the hardness of CDH (computational Diffie-Hellman) problem. Our ID-PUIC protocol is also efficient and flexible. Based on the original client's authorization, the proposed ID-PUIC protocol can realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking.The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

The concrete ID-DPDP construction mainly comes from the signature, provable data possession and distributed computing. The signature relates the client's identity with his private key. Distributed computing is used to store the client's data on multi-cloud servers. At the same time, distributed computing is also used to combine the multi-cloud servers' responses to respond the verifier's challenge. Based on the provable data possession protocol, the ID-DPDP protocol is constructed by making use of the signature and distributed computing. Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use.

Keywords- Security,Public Cloud Server,Proxy,Integrity Checking,Uploading,Bilinear Pairing,Coherent

I. INTRODUCTION

A protocol (ID-DPDP- Identity - based distributed provable data possession) is proposed to store data in multi cloud ID-DPDP protocol eliminate the certificate management. In this system, the client's data is distributed to multi cloud servers based on type of the data and size of the data.

Private Key generator generates the private key for the client, it contains the client unique id. Client's data is transferred to combiner; the combiner distributes the data according to the size and type of data. Verifier sends the challenges to the Combiner, the combiner transfer the challenge to the respected cloud. Afterwards, combiner aggregates the result and check whether it is valid or not. If it is valid, allow clients to store the data in multi cloud. In the phase Extract, PKG creates the private key for the client. The client creates the block-tag pair and uploads it to combiner.

The combiner distributes the block-tag pairs to the different cloud servers according to the storage metadata. The verifier sends the challenge to combiner and the combiner distributes the challenge query to the corresponding cloud servers according to the storage metadata. The cloud servers respond the challenge and the combiner aggregates these responses from the cloud servers. The combiner sends the aggregated response to the verifier. Finally, the verifier checks whether the aggregated response is valid.

The concrete ID-DPDP construction mainly comes from the signature, provable data possession and distributed computing. The signature relates the client's identity with his private key. Distributed computing is used to store the client's data on multi-cloud servers. At the same time, distributed computing is also used to combine the multi-cloud servers' responses to respond the verifier's challenge. Based on the provable data possession protocol, the ID-DPDP protocol is constructed by making use of the signature and distributed computing.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

The foundations of cloud computing lie in the outsourcing of computing tasks to the third party. It entails the security risks in terms of confidentiality, integrity and availability of data and service. the distributed storage and integrity checking are indispensable. On the other hand, the integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on distributed computation, we will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi-cloud storage.

PROPOSED SYSTEM

In identity-based public key cryptography, this paper focuses on distributed provable data possession in multi-cloud storage. The protocol can be made efficient by eliminating the certificate management. We propose the new remote data integrity checking model: ID-DPDP. The system model and security model are formally proposed. Then, based on the bilinear pairings, the concrete ID-DPDP protocol is designed. In the random oracle model, our ID-DPDP protocol is provably secure. On the other hand, our protocol is more flexible besides the high efficiency. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

III. MODULE DESCRIPTION

a) 1. Cloud Module

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious.

b) 2. Register Module

In this module, we have to create users to allocate files by block tag pairs to combiner. The work of registered users are to create a valid file then to store it in a cloud server. User also called as Client.*Client*: an entity, which has massive data to be stored on the multi-cloud for maintenance and computation, can be either individual consumer or corporation.

c) 3. Client Key Segregation Module

In this module, we will allocate a random key which will be accessible only by the client.PKG(Private Key Generator): an entity, when receiving the identity, it outputs the corresponding private key. While registering a client it will automatically send through secure channel.

d) 4. Combiner Module

In this module, combiner cannot upload the data sent by the user or client. After the conformation from a verifier it will be uploaded without prior notice user or combiner cannot upload files to cloud server. *Combiner*: an entity, which receives the storage request and distributes the block-tag pairs to the corresponding cloud servers.

e) 5. Verifier Module

The verifier sends the challenge to combiner and the combiner distributes the challenge query to the corresponding cloud servers according to the storage metadata.

V. SYSTEM IMPLEMENTATION

In public cloud, this paper focuses on the identity-based proxy-oriented information uploading and remote information integrity checking. By victimization identity-based public key discipline, our planned ID-PUIC protocol is economical since the certificate management is eliminated. ID-PUIC is also a unique proxy-oriented information uploading and remote information integrity checking model in public cloud. we tend to tend to supply the formal system model and security model for ID-PUIC protocol. Then, supported the linear pairings, we tend to tend to designed the first concrete ID-PUIC protocol. inside the random oracle model, our designed ID-PUIC protocol is demonstrably secure.

A. Concrete ID-PUIC Protocol

Concrete ID-PUIC protocol contains four procedures: Setup, Extract, Proxy-key generation, TagGen, and Proof. So as to imply the intuition of our construction, the concrete protocol's style is delineated in Figure one. First, Setup is performed and additionally the system parameters unit generated. Supported the generated system parameters, the opposite procedures unit performed as Figure one. It's delineated below: (1) inside the half Extract, once the entity's identity is input, KGC generates the entity's private key. Especially, it'll generate the private keys for the patron and additionally the proxy. (2) inside the half Proxy -key generation, the primary shopper creates the warrant and helps the proxy generate the proxy key. (3) inside

the half TagGen, once the information block is input, the proxy generates the block's tag and transfer block-tag pairs to PCS..

Figure 1. Login form

B. Personal Checking, Delegated Checking And Public Checking

Our planned ID-PUIC protocol satisfies the personal checking, delegated checking and public checking. Within the remote data integrity checking procedure, R1, Ro, Rp protocol can only be performed by the primary shopper. Thus, it's personal checking. On some cases, the first shopper has no ability to envision its remote data integrity, such as, he is taking a vacation or in jail or in battle field, etc. Thus, it's going to delegate the third party to perform the ID-PUIC protocol. it should be the third auditor or the proxy or various entities. the primary shopper sends R1, Ro, and Rp to the delegated third party. The delegated third party has the pliability to perform the ID-PUIC protocol. Thus, it is the property of delegated checking.

Figure 2. Registration form
Client page

Figure 3. Upload file successfullyio

The client is already registered by using his details and then he will login in to the cloud using username and password and then he upload the file.

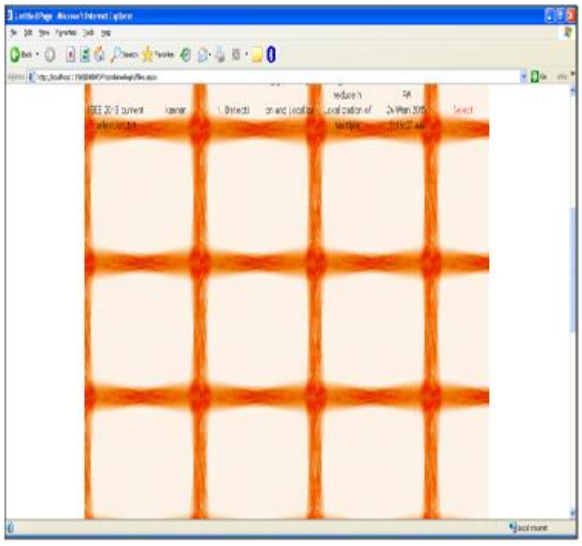

Figure 4. Combining paired data

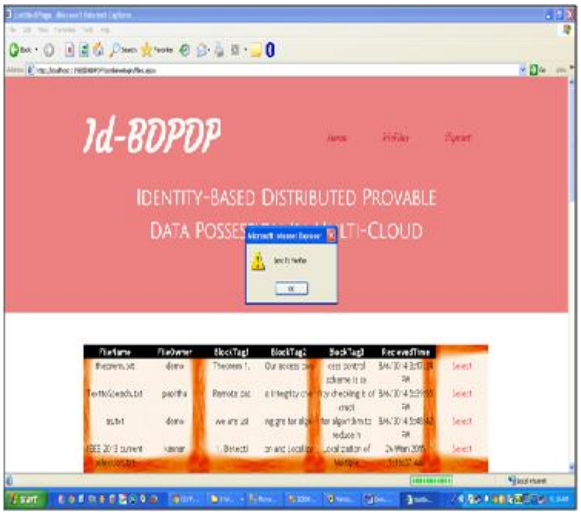

Fig 5. File sent to verifier

IV. CONCLUSION

In multi-cloud storage, this paper formalizes the ID-DPDP system model and security model. At the same time, we propose the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

The system has been designed, developed and implemented after tedious testing and debugging the goals of the system have reached in such a manner that the system is flexible for any change in the near future. The coding has been done cautiously so that any developer can follow the program easily with the knowledge of the convections followed hence it is easy to be maintained. Testing has been completed and a third person, with little knowledge of coding, tested the system for user friendliness and simplicity. This idea is developed with ASP.NET as front-end and SQL Server back-end.

This contains the different types of flats with different area of Square feet's, their registration, Cancellation. Registration Form like information is related to the user or client**.** This is similar to be an application form to be given to the client to be filled by the user**.** The request data will be in the form of name, address, phone, annual income, comments from the customer**.** It is just like to get clients personnel details.

FUTURE ENHANCEMENT

It is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such an issue to provide the support of variable-length block verification. In multi-cloud storage, this paper formalizes the ID-DPDP system model and security model. At the same time, we propose the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

In multi-cloud storage,the ID-DPDP system model and security model. At the same time, it proposes the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

REFERENCES

[1] Birget, J.C., D. Hong, and N. Memon, 'Graphical Passwords Based on Robust Discretization', IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[2] Blonder, Chiasson, S. R. Biddle, and P.C. van Oorschot, 'A Second Look at the Usability of Click-based Graphical Passwords', ACM SOUPS, 2007.

[3] Cranor. L.F, S. Garfinkel, 'Security and Usability', O'Reilly Media, 2005.

[4] Davis.D. F. Monrose, and M.K. Reiter, 'On User Choice in Graphical Password Schemes', 13th USENIX Security Symposium, 2004.

[5] Jiang He, Tong Gao, Wei Hao, I-Ling Yen and Farokh Bastani, 'A Flexible Content Adaptation System using a Rule-based approach', IEEE Transactions on Knowledge and Data Engineering, VOL 19, NO. 1, 2007.

Websites:

1. http://www.vbdotnetheaven.com/
2. http://www.sysimp.com
3. http://en.wikipedia.org/wiki/winsock server
4. http://www.testinggeek.com/testingtype.aspw
5. http://www.sei.cmu.edu./domain-engineering/usecasediagram.html
6. http://en.wikipedia.org/wiki/windows-XP
7. http://www.sys-design.com