SECURE DATA SHARING IN CLOUDS USING REVERSIBLE IDENTITY-BASED DOUBLE ENCRYPTION WITH TIME STAMP

[1]M.Geetha, [2]A.Imrana, [3]M.Navina
[1]Associate Professor, MCA Department, Paavai Engineering College, Namakkal, Tamil Nadu
[2,3]II MCA, Paavai Engineering College, Namakkal, Tamil Nadu

Abstract :Cloud computing has gained widespread adoption due to its ability to store massive amounts of data and provide extensive computing power. However, ensuring secure data sharing is crucial for cloud applications. To address this issue, identity-based broadcast proxy re-encryption schemes have been proposed, but they require cloud users to participate in the group shared key renewal process, which can compromise cloud security. To overcome this limitation, a new security notion called revocable identity-based double-encryption with timestamp has been introduced. This scheme enables a user to revoke a set of delegates designated by the delegator from the double-encryption key, which is created and time-stamped for a brief time period during which the delegate can view or download the requested file. This ensures maximum security and privacy. Performance evaluation indicates that the proposed scheme is highly efficient and practical.

keywords :Business to Customer., Cloud Sharing, Encryption, Document Transfer

I. INTRODUCTION

Cloud computing provides users with on-demand access to computer resources, such as data storage and computing power, without requiring active management. However, security and privacy challenges remain a concern. Encryption, particularly Identity-based encryption, is a promising solution to ensure data confidentiality. In some scenarios, such as medical research involving genome data, data owners may want to share encrypted data with specific recipients. Proxy re-encryption can be used to enable complex re-encryption computations in the cloud, allowing for secure data sharing. To address these challenges, we propose a three-layer storage framework based on fog computing that takes advantage of cloud storage while protecting data privacy. Our framework uses the Hash-Solomon code algorithm to divide data into parts, with a small part stored locally and in fog servers to enhance privacy. Using computational intelligence, our algorithm determines the proportion of data stored in the cloud, fog, and local machine. We have validated the feasibility of our approach through theoretical safety analysis and experimental evaluation, making it a powerful supplement to existing cloud storage schemes.

Web server applications have changed over the past few years from static to dynamic applications. Some flaws in earlier web site design made this progression inevitable. For instance, traditional web site design technologies are not sufficient to move more business activities online, whether in business-to-consumer (B2C) or business-to-business (B2B) industries. Every developer encounters the following main problems when creating web applications:

Scalability: A popular website will attract more visitors, and since this number is growing quickly, web applications must be scalable in order to keep up.

Integration of data and business logic - Since the web is just another means of conducting business, the middle-tier and data-access programmes should be compatible.

Manageability - As websites continue to grow in size, we need a workable management system to control the interaction of the expanding content with business systems.

Personalization — giving the website a

personalised touch becomes crucial to retaining our customers. In order to provide feedback and involvement from what would otherwise be a very one-sided dialogue, it is crucial to understand their preferences, to let them customise the information they view, to remember their past transactions, or to remember their frequent search terms.

Aside from these basic requirements for a business-focused website, it has become clear that new technologies are required to build reliable, dynamic, and small server-side web apps. The following are the primary traits of dynamic web server programmes today: Provide data streams and HTML and XML to the web client. Presentation, logic, and data interfaces to databases, other Java applications, CORBA, directory, and mail services are all separate from one another.

II. LITERATURE REVIEW

PRE permits an intermediary to change over a ciphertext under one client's (delegator's) public key into one more ciphertext which can be unscrambled with another client's (delegatee's) confidential key, without revealing the basic plaintext and secret key data. Since Burst et al. [4] proposed the main PRE conspire, countless PRE plans with various attributes have been introduced. In [4], Nuñez et al. surveyed, thought about, and dissected the primary PRE investigates. Their review included PKI-based intermediary reencryption [5-6], character based intermediary reencryption (IBPRE) [7, 8], quality based intermediary reencryption (ABPRE) [9, 10], and grid based intermediary reencryption (LBPRE) [14]. Among these examinations, the IBPRE plot is introduced to be a significant exploration heading. It joins character based encryption (IBE) [11, 12] and PRE [4], where the client's personality is utilized as the public key for encryption, staying away from the complicated public-key authentication the board which is helpful in a few situations.

Green and Ateniese [8] set forward the primary IBPRE conspire, in which two noncollusion safe methodologies were presented, and a few promising uses of IBPRE were referenced. Accordingly, numerous enhancements and applications were proposed to address different issues and deficiencies of past arrangements. Wang et al. [15] proposed two IBPRE plans that could oppose plot assaults. The first has no ciphertext development, while the subsequent one accomplishes CCA security. Wang et al. [6] gave an improved multiuse IBPRE conspire, which accomplishes CCA2 security in the irregular prophet model. Their answer offers a confirmable response to the open issue referenced in [8]. Shao and Cao [17] presented the principal CCA-secure and plot safe IBPRE conspire in the standard model. Xu et al. [21] introduced a contingent personality based broadcast PRE conspire and applied it to cloud email. Zhou et al. [13] proposed an IBPRE conspire with variant 2, which gives a ciphertext change from convoluted personality based broadcast encryption (IBBE) to straightforward IBE. Ge et al. [18] introduced a safe fine-grained character based broadcast PRE conspire for encoded microvideo sharing. The plans referenced above broke down the effectiveness, security, and access control of the calculations exhaustively yet didn't think about the elements of authorization repudiation and ciphertext advancement.

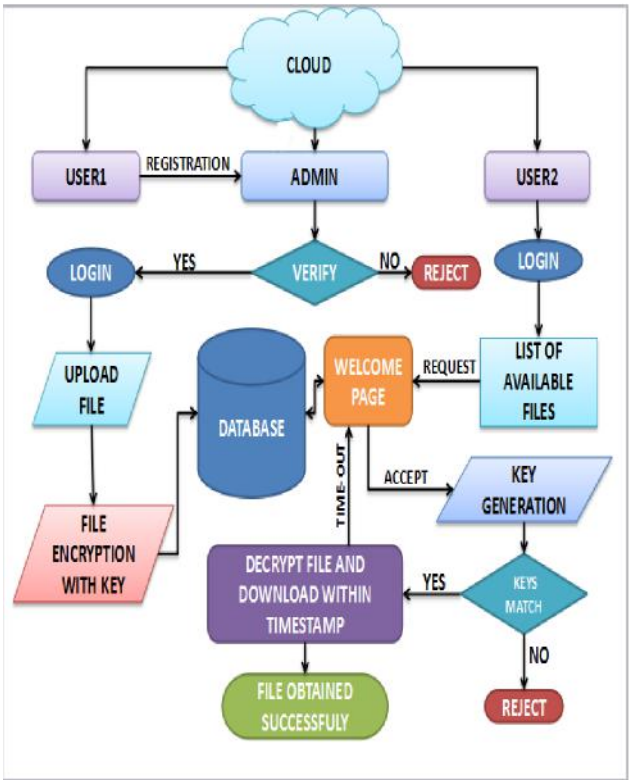
Liang et al. [2] proposed an effective cloud-based revocable IBPRE conspire for occasional key and ciphertext refreshes by refreshing time tokens, in which the length of ciphertext increments straightly with the hours of reencryption. Sun et al. [19] proposed a CCA-secure revocable IBE with ciphertext development for information partaking in distributed storage, which stresses that the size of the ciphertext in the cloud stays in consistent size paying little heed to developments. In any case, their methodology did not depend on PRE. The ciphertext put away in the cloud is scrambled by the information proprietor utilizing the character of the requester rather than his own personality, and that intends that there are various ciphertexts put away on the cloud relating to various requesters, rather than only one ciphertext in the PRE framework. Shafagh et al. [20] understood an undertaking that incorporates elements of approval, repudiation, key update, and ciphertext update in PKI-based engineering, which needs complex endorsement the executives.

Enlivened by the work introduced in [20], we propose a better IBPRE conspire, which incorporates the capabilities above for a solid individual information cloud sharing application. This better methodology has the attributes of noninteractivity, unidirectionality, agreement wellbeing, ciphertext streamlining,

and multiuse and nontransferability in the irregular prophet model. In addition, the ciphertext update (reencryption) activities can be executed on different occasions, and the ciphertext length continues as before. The ciphertext reencrypted (designated) to the agent, be that as it may, can't be reencrypted (reauthorized). The enhancements depend on Green and Ateniese [18] and intend to acknowledge secure client information sharing on cloud servers by joining fundamental qualities of information sharing, ciphertext refreshing, and trait based admittance consent giving and renouncement. Moreover, the plan likewise features the properties of multiuse and conspiracy safe and the streamlining of reencryption execution (that abbreviates reencryption time; guarantee proficiency when numerous clients access information, or much ciphertext refreshed simultaneously).

III. PROPOSED SYSTEM

We investigate how to accomplish keyword search over fascinating encoded cloud data using symmetric-key based affirmation in the proposed framework and provide a logical plot in this paper. We provide a revolutionary Accumulative Authentication Label based on symmetric-key cryptography to provide an affirmation tag for each catchphrase in order to aid in the effective verification of dynamic data.Multiple data sources can be used with separate secret keys thanks to multi-key creation. without losing any data during the transfer.



System Block Diagram

IV. IMPLEMENTATION

i. User point of interaction plan
ii. File transfer
iii. Double encryption process
iv. Request to administrator
v. Response from administrator
vi. Download the record

4.1.1 UI Plan

i. This is the main module of our venture.
ii. The significant job for the client is to move login window to client window.
iii. This module has made for the security reason.
iv. In this login page we need to enter login client id and secret word.
v. It will check username and secret word is match or not (substantial client id and legitimate secret word).
vi. If we enter any invalid username or secret key we can't go into login window to client window it will shows mistake

message.

vii. So we are keeping from unapproved client going into the login window to client window. It will give a decent security to our undertaking.

viii. So server contain client id and secret word server likewise really take a look at the confirmation of the client.

ix. It well works on the security and keeping from unapproved client goes into the organization.

x. In our task we are involving JSP for making plan.

xi. Here we approve the login client and server verification.

4.1.2 Document Transfer

In this module, after proprietor login, the proprietor will transfer the record while transferring the document, document content will be scrambled and put away under data set.

Document contents, record size, record type and all subtleties of record will be put away under information base.

4.1.3 Twofold Encryption Cycle

In this module, when the record is being transferred in the back-end there happens the twofold encryption cycle and it will be put away in the data set.

4.1.4 Solicitation to Administrator

In this module, the client will send the document solicitation to the administrator for which records, the client needs the entrance. Without the authorization structure the administrator, the client can't ready to download the document.

4.1.5 Reaction from Administrator

In this module, the administrator will be giving the acknowledgment to the client for which document needs the entrance. After the acknowledgment, the record key will be shipped off the client.

4.1.6 Download the Record

In this module, subsequent to getting the key from the administrator, the client can download the record utilizing the key gave by the administrator.

V. CONCLUSION

In this paper, we defined revocable identity-based broadcast proxy re-encryption, proposed a concrete construction under the definition and proved our scheme is CPA secure in the random oracle model. More importantly, the property and performance comparison reveal that our proposed scheme is efficient and practical. Furthermore, our RIB-DET scheme can nicely support key revocation for a data sensitive system in a cloud environment, for example, a volunteer-based genome research system. While this work has answered the issue of key revocation for data sharing, it drives several intriguing open topics as building RIB-BPRE scheme without random oracles and how to provide more expressive on identities.

REFERENCES

[1]. H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, “Secure sharing of partially homomorphic encrypted IoT data,” in *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, pp. 1–14, ACM, Delft, Netherlands, November 2017.

[2]. C. Ge, W. Susilo, J. Wang, and L. Fang, “Identity-based conditional proxy re-encryption with fine grain policy,” *Computer Standards & Interfaces*, vol. 52, pp. 1–9, 2017.

a. View at: Publisher Site | Google Scholar

[3]. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, “An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing,” in *Proceedings of the European Symposium On Research In Computer Security*, pp. 257–272, Wroclaw, Poland, September 2014.

[4]. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in *Proceedings of the International Conference on the Theory And Applications of Cryptographic Techniques*, pp. 127–144, Espoo, Finland, May 1998.

[5]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 1, pp. 1–30, 2006.

[6]. B. Libert and D. Vergnaud, “Unidirectional chosen-ciphertext secure proxy re-encryption,” *IEEE*

Transactions on Information Theory, vol. 57, no. 3, pp. 1786–1802, 2011.

[7]. C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in *Proceedings of the International Conference On Information Security*, pp. 189–202, Valparaíso, Chile, October 2007.
View at: Google Scholar

[8]. M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 288–306, Zhuhai, China, June 2007.
View at: Google Scholar

[9]. X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pp. 276–286, ACM, Sydney Australia, March 2009.
View at: Google Scholar

[10]. K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proceedings of the 2013 5th International Conference On Intelligent Networking And Collaborative System*, pp. 552–559, IEEE, Xi'an, China, September 2013.
View at: Google Scholar

[11]. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceeedings of the Annual International Cryptology Conference*, vol. 32, no. 3, pp. 586–615, Santa Barbara, California, USA, August 2001.

[12]. B. Waters, "Efficient identity-based encryption without random oracles," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 114–127, Aarhus, Denmark, May 2005.

[13]. Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu, and Y. Ding, "Identity-based proxy re-encryption version 2: making mobile access easy in cloud," *Future Generation Computer Systems*, vol. 62, pp. 128–139, 2016.

[14]. Y. Aono, X. Boyen, L. T. Phong, and L. Wang, "Key-private proxy re-encryption under LWE," in *Proceedings of the International Conference on Cryptology in India*, vol. 8250, pp. 1–18, Lecture Notes in Computer Science, Mumbai, India, December 2013.

[15]. L. Wang, L. Wang, M. Mambo, and E. Okamoto, "New identity-based proxy re-encryption schemes to prevent collusion attacks," in *Proceedings of the International Conference on Pairing-Based Cryptography*, pp. 327–346, Yamanaka Hot Spring, Kaga, Japan, December 2010.
View at: Google Scholar

[16]. H. Wang, Z. Cao, and L. Wang, "Multi-use and unidirectional identity-based proxy re-encryption schemes," *Information Sciences*, vol. 180, no. 20, pp. 4042–4059, 2010.

[17]. J. Shao and Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption," *Information Sciences*, vol. 206, pp. 83–95, 2012.

[18]. X. Zhang, H. Wang, and C. Xu, "Identity-based Key-Exposure Resilient Cloud Storage Public Auditing Scheme from Lattices," *Information Sciences*, pp. 223–234, 2019.

[19]. Y. Sun, W. Susilo, F. Zhang, and A. Fu, "CCA-secure revocable identity-based encryption with ciphertext evolution in the cloud," *IEEE Access*, vol. 6, pp. 56977–56983, 2018.

[20]. H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, "Secure sharing of partially homomorphic encrypted IoT data," in *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, pp. 1–14, ACM, Delft, Netherlands, November 2017.

[21]. P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity-based broadcast proxy re-encryption and its application to cloud email," *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66–79, 2016.