ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Method to Share and Protect the Confidential Information between Users in the Cloud

S. Aswini
M.Tech Student
Vignana Bharathi Institute of Technology.

N.Srinivas
Associate Professor & HoD,
Vignana Bharathi Institute of Technology.

ABSTRACT

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services),[1][2] which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers[3] that may be located far from the user. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

In the cloud, for achieving accesses management and keeping information confidential, house owners might adopt attribute-based encoding to encode the keep data. Users with restricted computing power are but a lot of possible to delegate the mask of the decoding task to the cloud servers to cut back the computing value. As a result, attribute-based encoding with delegation emerges. Still, there are caveats and queries remaining within the previous relevant works. as an example, throughout the delegation, the cloud servers might tamper or replace the delegated ciphertext and respond a cast computing result with malicious intent. They will additionally cheat the eligible users by responding them that they're ineligible for the aim of value saving. What is more, throughout the encoding, the access policies might not be versatile enough likewise. Since policy for general circuits allows realizing the strongest variety of access management, a construction for realizing circuit ciphertext-policy attribute-based hybrid encoding with verifiable delegation has been thought of in our work. In such a system, combined with verifiable computation and encrypt -then-mac mechanism, the information confidentiality, the fine-grained access management and also the correctness of the delegated computing results are well bonded at identical time. Besides, our theme achieves security against chosen- plaintext attacks beneath the k -multilinear Decisional Diffie-Hellman assumption. Moreover, an intensive simulation campaign confirms the practicability and potency ofthe projected answer.

Keywords *— Ciphertext-policy attribute-based encryption, Circuits, Verifiable delegation, Multilinear map, Hybrid encryption.*

Existing System

Attribute-based encryption proposed the notion of attribute-based encryption (ABE). They focused on policies across multiple authorities and the issue of what expressions they could achieve. Up until recently, raised a construction for realizing KPABE for general circuits. Prior to this method, the strongest form of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

expression is boolean formulas in ABE systems, which is still a far cry from being able to express access control in the form of any program or circuit. Actually, there still remain two problems. The first one is their have no construction for realizing CPABE for general circuits, which is conceptually closer to traditional access control. The other is related to the efficiency, since the exiting circuit ABE scheme is just a bit encryption one. Thus, it is apparently still remains a pivotal open problem to design an efficient circuit CP-ABE scheme.

Hybrid encryption.

Existing system proposed the generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, a one-time MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. Such improved model has the advantage of achieving higher security requirements. ABE with Verifiable Delegation. Since the introduction of ABE, there have been advances in multiple directions. The application of outsourcing computation is one of an important direction. It designed the first ABE with outsourced decryption scheme to reduce the computation cost during decryption. However, since the data owner generates a commitment without any secret value about his identity, the untrusted server can then forge a commitment for a message he chooses. Thus the ciphertext relating to the message is at risk of being tampered. Furthermore, just modify the commitments for the ciphertext relating to the message is not enough. The cloud server can deceive the user with proper permissions by responding the terminator $\perp$ to cheat that he/she is not allowed to access to the data.

Disadvantages

There are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well.

Proposed System

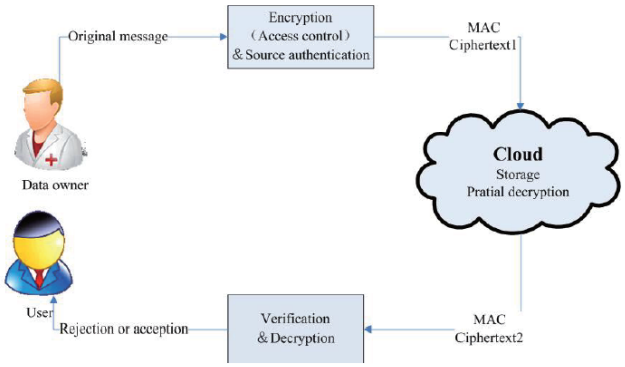
This project proposes a concrete circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme based on the multilinear maps and the verifiable computing technology under cloud environment.

Advantages

This project achieves security against chosen-plaintext attacks under the k-multi linear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

An extensive simulation campaign confirms the feasibility and efficiency.

System Architecture



MODULES

- USER
- Authentication
- Import User Report

- ADMIN
- Authentication
- Authority
- Upload report in cloud

- DOCTOR
- Authentication

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- View User Message
- View User Report

MODULE DESCRIPTION

USER

AUTHENTICATION

Authentication

The user have to be coerced to go in actual username and countersign that is given inside the registration, if login accomplishment suggests that it'll seize up to main page else it'll stay inside the login page itself. If it's a brand new user next it'll move to the registration page.

Import User Report

In this module, User will transfer their report in data server. that report consented to admin. If user selects one sort report, user will transfer data in server.

ADMIN

Authentication

Admin has became to proposal precise username and word that was endowed at the period of registration, if login accomplishment suggests that it'll seize up to main page else it'll stay inside the login page it self.

Authority

In this module, Power will produce attribute chiefly established key and dispatch to vision proprietor and user. Power upheld Generated key and utilized for protect vision in cloud server.

Upload report in cloud

In this module, vision proprietor will transfer Encrypted vision and rework to user. If vision proprietor transfer and rework vision to user, vision are protective in cloud.

View User Request

In this module, Admin elucidate user request. If valid user appeal dispatch to admin, next admin consented their appeal and confirm valid user or not.

View Doctor Request

In this module, admin can think doctor request. If admin consented doctor appealand user report dispatch to doctor, data will be protecting in cloud.

DOCTOR

Authentication

Admin has becameto proposalactual username and hidden that was endowed at the period of registration, if login accomplishment way that it'll seize up to main page else it'll stay inside the login page itself.

View User Message

In this module, Doctor sights user message. If valid user dispatch memo to doctor, next doctor consented user memo from user and reply their memo for communication.

View User Report

In this module, Doctor sights user report. Doctor will accord report from admin and gaze at user report. Then, if doctor notify their report upheld user erect, doctor dispatch user notified report back to user directly.

CONCLUSION

In the cloud, for accomplished admission association and keeping vision confidential, {the knowledge|theinfo|the information} homeowners could accept attribute-based cryptography to encipher the grasp on data. decoding task to the cloud servers to cut back the computing value. Our ciphertext strategy attribute-based hybrid cryptography, we incline to could representative the verifiable partial decoding to the cloud server.

References

[1] Wen, Q. , Li, W. , Jin, Z., Xu, J. “CIRCUIT CIPHER TEXT-POLICY ATTRIBUTE-BASED HYBRID ENCRYPTION WITH VERIFIABLE DELEGATION IN CLOUD COMPUTING” Parallel and Distributed Systems, IEEE Transactions on (Volume:PP , Issue: 99) January 2015.

[2] M. Green, S. Hohenberger and B. Waters, ” Outsourcing the Decryption of ABE Cipherte xts,” in Proc. USENIX SecuritySymp., San Francisco, CA, USA, 2011.

[3] J. Lai, R. H. Deng, C. Guan and J. Weng, ”Attribute-Based Encryption with Verifiable Outsourced Decryption,” in Proc. IEEE Transactions on information forensics and security, vol.8, NO. 8, pp.1343-1354, 2013.

[4] A. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[5] B. Waters,”Cipherte xt-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization,” in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[6] B. Parno, M. Raykova and V. Va ikuntanathan, ”How to Delegate and Verify in Public: verifiable computation from attribute-based encryption,” in Proc. TCC, pp.422-439, Springer-Verlag Berlin, Heidelberg, 2012.

[7] S. Yamada, N. Attrapadung and B. Santoso,”Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication,” in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.

[8] J. Han, W. Susilo, Y. Mu and J. Yan, ”Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption,” in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.

[9] S. Ga rg, C. Gentry, S. Halevi, A. Sahai and B. Waters, ”Attribute-Based Encryption for Circuits from Multilinear Maps,” in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin, Heidelberg, 2013.

[10] S. Go rbunov, V. Vaikuntanathan and H. Wee, ”Attribute-Based Encryption for Circuits,” in Proc. STOC, pp.545-554, ACM New York, NY, USA, 2013.