Review on An Approach of Attribute Based Encryption Method With Verifying Outsourced Decryption In Mobile Cloud Computing

Ashwini D. Pradhan[1], Prof. K. B. Bijwe[2], Prof. V. B. Gadicha[3]
[1, 2, 3] Dept of Computer Science & Engineering
[1, 2, 3] P. R. Pote (Patil) college of Engineering & Management, Amravati

Abstract- *With the increasing number of mobile applications and the popularity of cloud computing, the combination of these two techniques that named mobile cloud computing (MCC) to bring rich computational resources to mobile users, network operators.*

There is focus on combining the MCC and ABE method. In existing method which is Ciphertext Policy Attribute Based(CP-ABE) method is based on attributes which is used to describe a user's credentials for generate a combine public key from that attributes, then providing public key to clusters and party encrypting data determine a policy for who can decrypt. For all that process, the computational overhead of encryption decryption grows with complexity of the access policy. To lower that computational overhead in this method generate the public key from that attributes of that user only who is requesting the data, with applying verifiable outsourced decryption in this scheme can verify the correctness of the transformed message.

Keywords- CP- ABE, Mobile Cloud Computing Outsourced Decryption, Verifiable.

I. INTRODUCTION

In this modern life increasing the development of mobile cloud computing, growing data is being centralized into the cloud for sharing. To keep the data secure for data owners, the sharing data needs to be encrypted before being uploaded and fine-grained access control is required. So introduced attribute based encryption, this is a promising technique for fine-grained access control of encrypted data in a cloud storage, however, decryption involved in the ABEs is usually too expensive for resource-constrained front-end users, which greatly hinders its practical popularity. However, one of the drawbacks of ABE is that the computational overhead of encryption and decryption grows with the complexity of the access policy. To reduce the decryption computational overhead on data, some researchers consider that decrypt the ciphertexts by outsourced decryption cloud servers. What's more, these semi-trusted servers learn nothing about the messages and DRs can verify the correctness of the transformed ciphertexts. But the encryption overhead is not taken into account. To solve the problem, we propose an efficient encryption scheme based on CP-ABE, which can dramatically enhance data encryption efficiency without loss of data security and data privacy, which can lower the overhead on data owners. To further reduce the decryption overhead on data receivers, so here additionally propose a verifiable outsourced decryption scheme. By security analysis and performance evaluation, the proposed scheme will prove to be secure as well as efficient.

II. LITERATURE REVIEW

A Sahai, B Waters in 2005 has proposed that Fuzzy identity-based encryption technique allows for a sender to encrypt a message to an identity without access to a public key certificate [1].

Sahai and Waters, V Goyal, O Pandey in 2006 introduced attribute-based encryption (ABE) as a new means for encrypted access control. In an attribute-based encryption system ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography. Instead both users' private keys and ciphertexts will be associated with a set of attributes or a policy over attributes [2].

J. Bethencourt in 2007 introduced Ciphertext- Policy Attribute Based Encryption (CP-ABE), and used the attributes to describe a user's credentials. The data owners specified the access policy. The decryption keys consisted of a set of attributes without any tree structure [3].

M. Green in 2011 proposed scheme that allow users to outsource their ciphertexts to cloud, and the cloud servers could translate them into a (constant-size) El Gamal-style ciphertext, without disclosing any information about the user's

messages. However, it couldn't verify the correctness of outsourced decryption [4].

G. Salodkar, K. Bijwe in 2015 proposed the secure and efficient data sharing for decentralized DTN in this method proposed an efficient and secure data retrival method using CPABE for decentralized DTN [6].

A. Ahuja, K. Bijwe in 2015 proposed the scheme of secure and encrypted accessing and sharing of data in distributed virtual cloud in this technique implemented an efficient data storage security in cloud where splitting of data in less time and efficient manner [7].

G. Kishor Kumar, Dr. Gobi in 2017 introduced "Survey on Mobile Cloud Computing and its Security and Future Challenges there is talks about survey on mobile cloud and mostly which challenges arises on future [12].

Dejan Kovachjev, Ralf Klamma in 2012 Framework for Computation Offloading in Mobile Cloud Computing about a Survey on various framework Mechanisms and about offloading in Mobile Cloud Computing and also the problems persist in the existing mechanisms [15].

Pratika Singh and Harsh Dev in 2016 introduced security Access Control Mechanism for Outsourced Data in Mobile Cloud Computing Environment in these method talk about how outsourcing data from mobile cloud environment and providing security access control mechanism[16].

III. RELATED WORK

ABE model was proposed by Sahai and Waters in 2005 year. ABE is the mechanism in which users are allowed to encrypt and decrypt data based on user attributes. User attributes are used to decide the secret key of the user and cipher text. If the set of attributes of the user key matches the attributes of the cipher text; then only decryption of a cipher text is possible. ABE enforces access control through public key cryptography. In this system perform pairing operation. The central purpose for these models is to provide access control and security. However, one of the drawbacks of ABE is that the computational overhead of encryption and decryption grows with the complexity of the access policy. To reduce the decryption computational overhead on data, consider that decrypt the ciphertexts by outsourced decryption cloud servers. Another problem with attribute based encryption (ABE) scheme is that data owner needs to use public key of every authorized user to encrypt data. So introduced CPABE based access control schemes have been proposed to overcome this problem.

IV. PROPOSED WORK

In this proposed system introduce the encryption method to generate the key by using the attribute like client MAC and Date from the mobile device. It reduces the clustering requirement for public key in existing system. User required to fetch the data from cloud storage, first key will generated from the MAC and Date of client mobile device and the decryption take place. Following give the flowchart of detail process of this method.

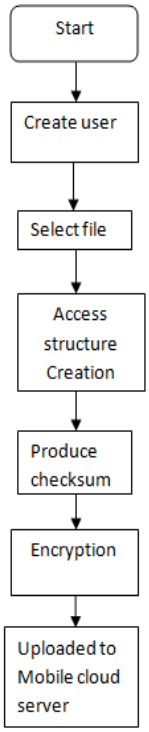

Fig.1 File uploading process

First step is the user creation the user who going to access the file should be registered. Firstly for the registration process, User details are corrected along with the user details are corrected. Finally here the user attribute are corrected along with the user details also corrected. User details are use for the further authentication, the access structure creation here the condition for the file size created, each file having separate access structure. Access structure authentication process, then next step is file encryption here the file are encrypted according to the attribute which are all in the access structure then the user details and encrypted file and access structure are uploaded to the mobile cloud server and the cloud server is connected with the proxy server.

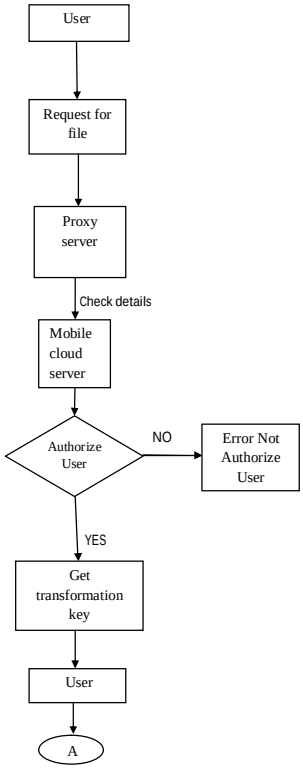

Fig.2 File outsourcing process

User first send the request to the server, the request should contain file name and user attributes the request is send to the proxy server, the proxy server check the user details from the server, if the user is authorize user then the server will outsource the file to the proxy server otherwise it passes a error message. If is an authorize user then server request for the transformation key from the user then transformation key send to the proxy server by the user.

Then transformatiopn key is send to the proxy server by the user then server perform the decryption over the file using the transformation key given by the user and decryption and generate the checksum for verifying the decrypted file.Then next step is the verification process. For the verification then user produced new checksum for the file, the server also will give the file checksum, if the both checksum are same the transformation perform wih proxy server is true otherwise the transformation is wrong and outsourcing the file.

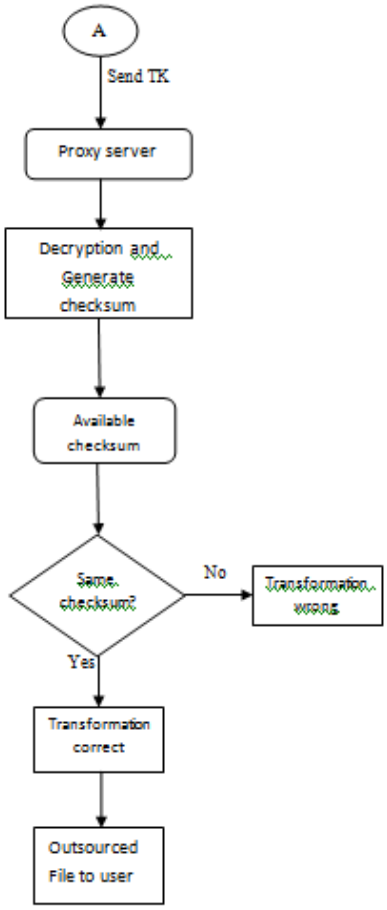

Fig. 3 Decryption and Verification Process

V. CONCLUSION

In this system,we proposed efficient approach of encryption method by using CPABE method in mobile cloud computing for secure and protect data from unauthorised user. These scheme is more efficient than ABE and ABE with outsourced decryption in every aspect like computational cost and complexity.

VI. ACKNOWLEDGMENT

The author would like to present their sincere gratitude towards the, Prof. K. B. Bijwe (Guide) and also special thanks to Prof. Vijay B. Gadicha (Main Guide) for their extreme support to complete this assignment.

REFERENCES

[1] A Sahai, B Waters, “Fuzzy identity-based encryption”, *in proc. EUROCRYP*, 2005, pp. 457-473.
[2] V Goyal, O Pandey, A Sahai, B Waters, “Attribute-based encryption for fine-grained access control of encrypted data”, *in proc. CCS*, 2006, pp. 89-98.

[3] J Bethencourt, A Sahai, B Waters, "Ciphertext-Policy Attribute-Based Encryption", *in proc. IEEE SP*, 2007, pp. 321-334.

[4] Wang, Q Liu, J Wu, "Hierarchical Attribute-Based Encryption for Fine Grained Access Control in Cloud Storage Services", *in proc. CCS*, 2010, pp. 735-737.

[5] M Green, S Hohenberger, B Waters, "Outsourcing the decryption of ABE ciphertexts", *in proc. SEC*, 2011, pp. 34-34.

[6] J Lai, RH Deng, C Guan, J Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption", *IEEE Transactions on Information Forensics & Security*, vol. 8, no.8, pp. 1343-1354, Aug. 2013.

[7] G. Salodkar, K. Bijwe "Secure and Efficient Data Sharing for Decentralized DTN" ,*International Journal of Science and Resarch*, vol.4 Apr 2015 pp.2319-7064.

[8] A. Ahuja, K. Bijwe "Secure and Encrypted Accessing and Sharing of Data in Distributed Virtual Cloud", *IORD Journal of Science of Technology*, vol. 2 May 2015 pp 24-23.

[9] S Lin, R Zhang, H Ma, M Wang, "Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption", *IEEE Transactions on Information Forensics & Security*, vol. 10, no.10, pp. 2119-2130, Oct. 2015.

[10] A. Pandit, A. Lamture, P. Sankpal, "Attribute Based Encryption with verifiable Outsourced Decryption", *International Journal of Technical Research and Applications* e-ISSN: 2320-8163, Issue 41 AVALON March 2016, PP. 57-61.

[11] H Zhang, Z Zhou, X Du, P Li, X Yu, "Practical and Privacy-assured Data Indexes for Outsourced Cloud Data", *in proc. IEEE GLOBECOM*,2013, pp. 671-676.

[12] G. Kishore Kumar, Dr. M. Gobi "Survey on Mobile Cloud Computing [MCC], its Security & Future Research Challenges" *Inernational Research Journal of Engineering and Technology (IRJET)* e-ISSN: 2395 -0056 Volume: 04 Issue: 06 | June -2017 p-ISSN: 2395-0072.

[13] S Yu, C Wang, K Ren, W Lou, "Achieving Secure, Scalable, and Fine grained Data Access Control in Cloud Computing", *in proc. IEEE INFOCOM*, 2010, pp. 1-9.

[14] Dejan Kovachjev, Ralf Klamma, "Framework for Computation Offloading in Mobile Cloud Computing, *in proc IJIMI. 2012*, pp. 11-71.

[15] Pratika Singh, Harsh Dev , " A security Access Control Mechanism for Outsourced Data in Mobile Cloud Computing Environment", "International *Journal of Innovative Research in Advance Engineering"*, e-ISSN: 2349-2763 Issue10|October 2016.