World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 3.419

A SECURE DELEGATION PROCESS USING CIRCUIT CIPHER-TEXT POLICY IN CLOUD COMPUTING

Mrs.Divya K.S[1], Ranjitha.V,[2]* Mehak Showkat[2] and Likhitha V.N.[3]

[1]Associate Professor, M.S. Engineering College, Bangalore, Karnataka India.

[2]M.S. Engineering College, Bangalore, Karnataka India.

[3]8th Sem. Students, M.S. Engineering College, Bangalore, Karnataka India.

Article Received on 24/04/2016 Article Revised on 14/05/2016 Article Accepted on 03/06/2016

***Corresponding Author**
Ranjitha V.
M.S Engineering College, Bangalore, Karnataka India.

ABSTRACT

Cloud Computing is a new technology that is widely being used and was introduced in the original ARPANET by 1977. The word cloud Computing does not have any clear well defined meaning. Though cloud computing has uncountable advantages, it still lacks behind in the areas concerning security and privacy. For such purposes, we make use of certain technologies which help overcome these shortcomings. Technologies such as Encryption and cipher-text circuit policy are being implemented for privacy and security. Cloud computing ensures that there is increasing trust dependency on remote servers and the services they provide. Data owner encrypt their data before sending it to the cloud for privacy. Delegation is a process which is used by the end-users who have less computing power. The decryption process is delegated by the data owner to the cloud to reduce the computation cost. Sometimes the cloud server may tamper the given cipher text and send the modified one to the data user for attack. The access control is implemented effectively using a circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation method. Also there is proper use of the k-multi linear Decisional Diffie-Hellman algorithm to improve the security of encrypted data.

KEYWORDS: Cloud computing, Circuit Cipher-text policy, Encryption.

I. INTRODUCTION

Cloud computing defines a mode of computer services, familiar to the method in which

electricity supply is used. End-Users can simply make proper utilization of it. Users do not need to bother about where the electricity is coming from, how it is made, or transferred. The users pay for what they consume, every month. The cloud computing idea resembles this: The user can simply use the storing capacity, computing power, without having to bother about how they work internally. Security and privacy pose major threats in the cloud which are used for data storage. By the use of encryption, we can overcome these limitations. Though encryption provides confidentiality of the data in the cloud, the conventional encryption approach is not efficient for the use of access control policies.

Approach such as attribute-based access control, provide access control which is important for security and privacy of data. Encryption methodologies have been developed for access control over the data that is encrypted. Such approaches collect and distribute data items based on access control policies and then each group formed are encrypted with a different symmetric keys. These keys are given only to those users who are authorized, for those data items which have been allotted the access.

II. MODULES USED

i. Attribute Based Encryption

The idea of attribute based encryption was offered by Amit Sahai and Brent Waters. Attribute based encryption is a sort of public key encryption in which there is a secret key of a user and the cipher-text which are dependent upon properties. In such a system, the decryption of a cipher-text is possible only if the group of properties of the user key matches the properties of the cipher-text. An important safety point of view of Attribute-Based Encryption is resistant to collusion**.**

ii. Hybrid Encryption

Hybrid encryption is a form that goes into together two or more encryption systems. It mixes one time message authentication code with symmetric encryption to form key encryption mechanism. They are used mostly to ensure safety in a system.

iii. Verifiable Delegation

Verifiable delegation is used to put forward arguments approved by users without being tricked throughout the delegation. The facts that the owner encrypts the data he wants to upload to the cloud and it provides a proper mechanism to transfer the data effectively. The below figure.1 shows the two layer encryption approach.

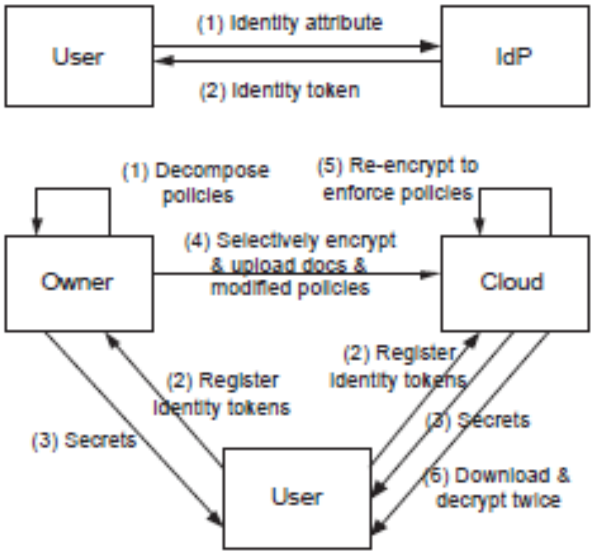

Figure 1: The Two Layer Encryption Approach

III IMPLEMENTATION

We use a two layer encryption approach to secure the data from being tampered or misplaced or misused from the intruders.

We also use the DES/RNS algorithm for the identity key and secret key generation whenever required.

Input: uploaded file.

Output: Decrypted file will be downloaded to the user's system.

Step 1: First admin logins with the username and password. Checks the domain, subdomain, and data owner and cloud server details.

Step 2: Data Owner logins with his/her username and password. Then he/she uploads a file to the cloud server with the circuit policy attributes (domain, subdomain).

Step 3: A new user will register with the basic information such as user id, username, email id and also he/she has to specify the domain, subdomain details.

Step 4: Once the user is registered, identity token key will be sent to his/her mail. Now the user can login with his/her valid user id and password. This identity token key will be uploaded for user verification.

Step 5: User will request for the secret key for downloading the particular file.

Step 6: Data Owner will check for the file request and sends the secret key file to the particular user's mail.

Step 7: for downloading the requested file, User uploads the secret key file for verification. The requested file will be decrypted and get downloaded in the user's system.

IV RESULTS

Screenshot 1: First we enter the login page for the Admin module successfully.

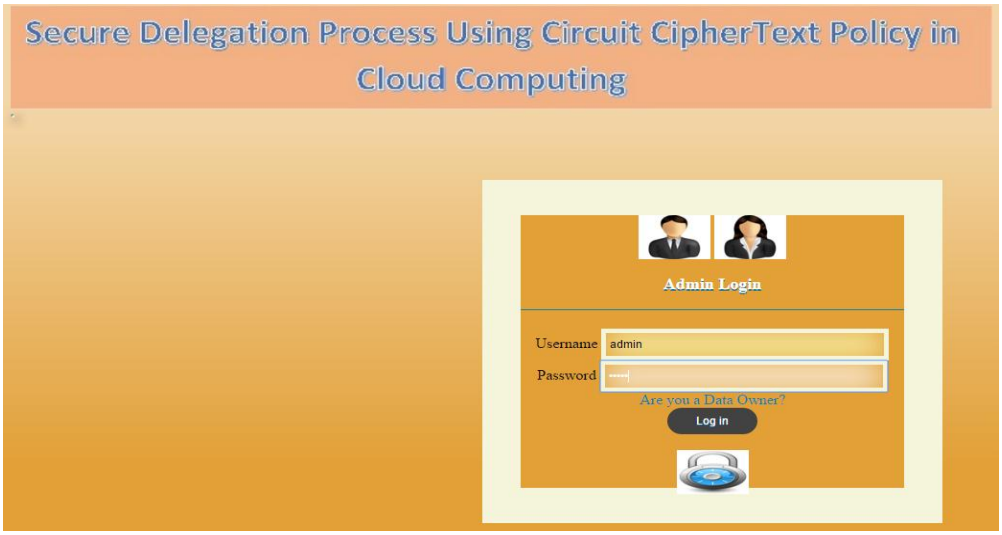

Figure.2: Admin Login Page

We start the Tomcat server & login with user id, password. We select the workspace under which we need to work. Then we get the above Figure 2 admin login page. We can view various details about the admin profile and edit them too. Also we can view the data owner details that have been registered with the Data Admin.

We can view the domain and the sub-domain details that are to be used to subject the circuit cipher text policy for privacy.

Snapshot 2: Next we upload other details for the data owner and then upload any particular file by specifying access control policies with it.

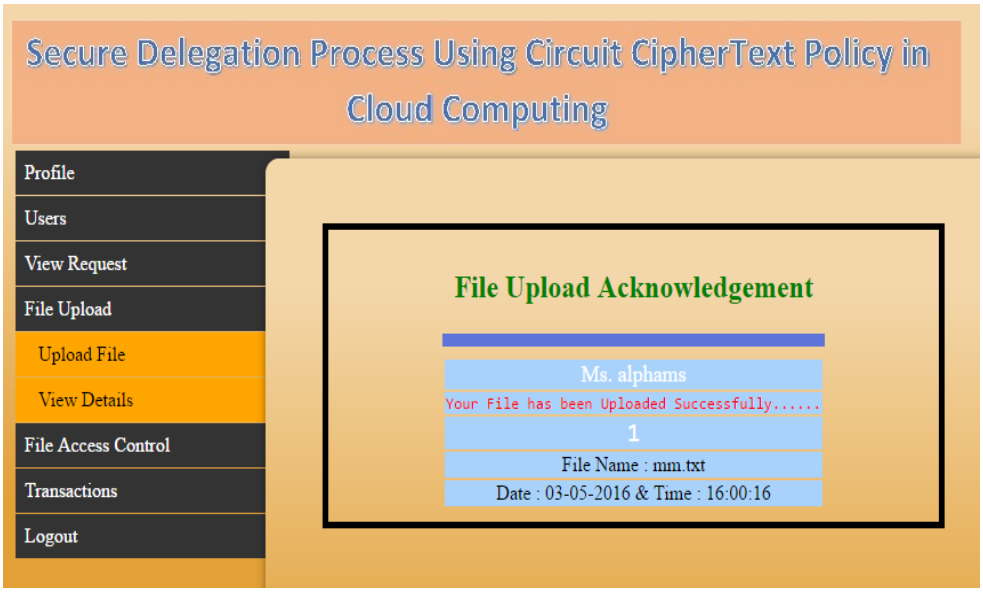

Figure 3: File Upload Acknowledgement.

When the Data owner uploads a file to the cloud, the file will be encrypted and we will get an acknowledgement as file is uploaded to cloud along with some details as shown in Figure 3 file upload acknowledgement. We get the a printed response indicating that the file has been uploaded and encrypted successfully.

We can view and edit various details of the Data Owner in View Data Owner Profile. We can also remove any Data Owner that is not needed by the system.

Snapshot 3: We can edit and view the End user details and also change its password
We perform necessary actions for the End user and then request to download the file needed by the End user.

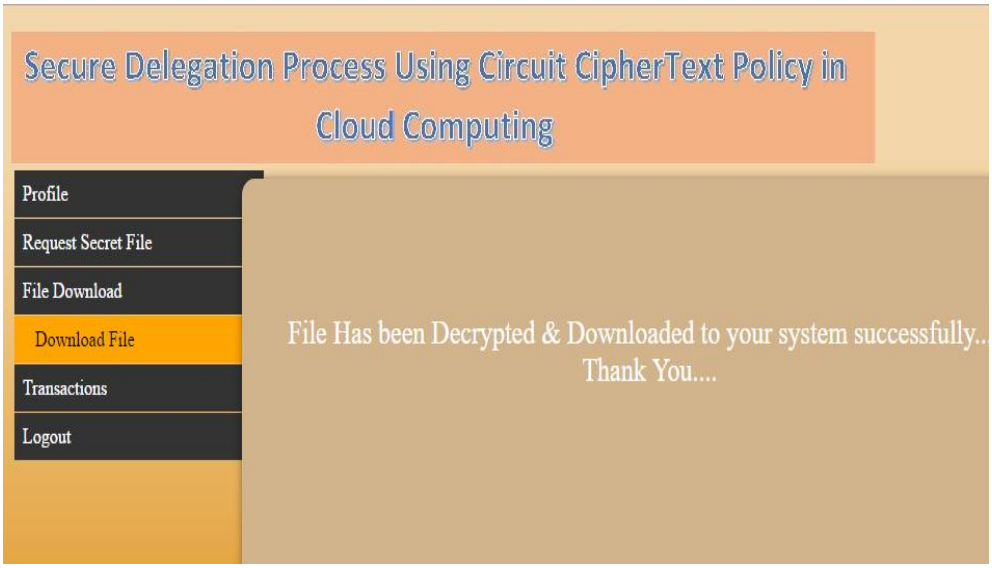

Figure 4: Decrypting & downloading the file.

When the domain and sub-domain remains the same with the file access control, the requested file will be decrypted and downloaded to the user's system as shown in the above Figure 4 Decrypting & downloading the file.

In case there is any error while downloading the file or in decryption it indicates that the data has been altered or the message authentication code doesn't match that of the data owner.
Also chances are it is due to the network failure. We need to have proper access to the network at all times.

CONCLUSION

In general, data transfer to the user from the data owner was not secure and verified. The data may be tampered or misplaced or misused by the intruder when data is transferring. Security

and privacy were main issues in data transfer in cloud computing. So we use two layer encryption approach in order to secure and verify data from intruder. We also implement our scheme over the integers. We use circuit policy attributes for user verifiability. Use of secret key and identity token key ensures the data confidentiality. Any End user can access the data if it is authorized to that particular data. End user can be present anywhere geographically but due to the access to Internet he can request to download the file uploaded by the Data Owner.

REFERENCES

1. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEE International Conference on Information Reuse and Integration (IRI), 2012.
2. E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," ACM Trans. Inf. Syst. Secur., 2002; 5(3): 290–331.
3. G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in VLDB '2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment, 2003; 898–909.
4. N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy-preserving approach to policy-based content dissemination," in ICDE '10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.
5. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing, ser.Collaborate Com., 2011; 11: 172–180.
6. M.Nabeel, N.Shang, and E.Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Transactions on Knowledge and Data Engineering, 2012; 14.
7. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rdInternationalConferenceonVeryLarge Data Bases, ser.VLDB '07. VLDB Endowment, 2007; 123–134.