International Journal of Research and Engineering
ISSN: 2348-7860 (O) | 2348-7852 (P) | Vol. 04 No. 05 | May 2017 | PP. 156-160
http://digital.ijre.org/index.php/int_j_res_eng/article/view/282

Secure data control: Privacy and security based on abe for access control over cloud

Author(s): Narayan R.[1] , Pramod N.[2] , Rahul A.B.[3] , Ranjan H.R.[4], Chandrakala B.M.[5]
Affiliation:[1,2,3,4]Student, [5]Associate Professor, Dept. of Information Science and Engineering,
Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

Abstract— In today's world, there is a strong requirement for sharing information over cloud. However, privacy and security remains a setback especially when working with bulk amounts of data in the Cloud. Data is abundantly stored outside the control of the data owner's machine with lack of his knowledge to the data owner, how the data being used and where the data are being stored. So, there is a necessity for the data owner to have a more control over their data, similar to the level of control they possess when the data are being stored on their own machine. For example, when a data owner shares an important file with his colleague, he cannot trust what his colleague will do with his data. In this paper, we try to address this problem by monitoring and preventing unauthorized operations by the data consumer. We present a solution called Secure-Data, which bundles the data owner's data and specified policy, based on XACML, in an object called Secure-Data object. Secure-Data enforces the policies set out by the data owner by communicating with the cloud based applications to disable certain operations and/or run a background process for monitoring the data. We define a software based protocol that will enable to secure the data in the cloud and will support the use of the android app for authentication purposes.

Keywords— Access Control; cloud; privacy; security; policy; monitoring.

I.INTRODUCTION

In recent times, there has been a massive growth in data sharing and collaboration by both social users and enterprise users. The growth of data sharing in recent times has provided an abundance of information and resources for every types of users such as education, research , medicine and entertainment to name a few. This has improved the quality of life. This level of access to data and information was not an imaginable task a decade ago.

With the growing demand for sharing massive amount of data using a variety of trending technologies, the privacy and security needs of the data owners will become prominent in future generation. When privacy and security of data is in the hands of dishonest recipients, data owners lose faith in sharing their information . This can have negative businesses when a trade secret is leaked. While there are many literature on securing data in the Cloud , little work has focused on giving the data owner an even greater level of control to their data. One concern of a data owner is the data access control problem. Once the data owner has provided accessibility to a data consumer to access data, he can no longer ensure that the data consumer will protect the data to the expectancy level of the data owner. The data consumer can share the data further to their peers and colleagues without the knowledge of the data owner. There needs to be a method for data owner's to have full control over their data. The data owner should have the ability to specify operations and usability of data by specific data consumers. If the user performs operations beyond the policy, it would be treated as unauthorized and the permissions would be revoked.

Moreover sharing the data in the cloud based environment is a burden on the cloud server as well as data owner. One such problem is key management. When a data owner wants to revoke a particular data consumer from access to their data, the data owner would to re-encrypt and re-distribute new keys to the remaining users. Bring Your Own Device (BYOD) is a trending technology which encourages data consumers to get their own devices such as smart phones, tablets and laptops to access sensitive information. BYOD can help address the key management problem as each user has a unique key tied up to the device. But BYOD has certain drawbacks such as security and privacy attacks.

Furthermore, a corrupt database administrator may access the sensitive data and disclose the data of data owner. Cloud Service Providers (CSPs) may also sell data to third parties in order to gain profit.

A.Our Contribution

In this paper, we mainly address two problems:

- Key management problem: In the existing system the encryption of the data was based on asymmetric encryption where in once an access is granted to a particular user the revoking of permissions was complex which requires the re-encryption of the data and redistribution of keys to maintain confidentiality. In our proposed system we use symmetric key encryption where an authorized user can access the data only after attribute verification.
- Data owner access problem :To provide data owner the stronger control over his data we introduced secure data object which binds data contents and the owner's policy by using open source language XACML
- .Double authentication: In our work we provide higher level of security by double authentication ie by using Android application during login and another based on Attribute verification.

Organization of the paper

The paper will be organized as follows, In section II , we are discussing about the related works. In section III we are comparing the existing system with our proposed system. In section VI we describe implementation details of our work. In section V we briefly describe the different phases involved in our system. In section VI, we listed various steps involved in the methodology.In section VII we discussed about the performance evaluation. We finally conclude our work in section VIII.

II.RELATED WORK

In this section, we review over the existing system related to data access control in the Cloud.

Yang et al.[6]proposed extended proxy assisted approach. This approach weakens the trust required by the cloud server. In this work we are using partial key for decryption. The cloud server will be having a private key for decryption. This is based on all-or-nothing principle.As we are using partial key from both the side collusion problem arises and there is no solution for this problem in this work.In our work we are avoiding a revoked consumer from getting the completely decrypted data even if collusion occurs.

Chen et al. [8] proposed the system where they are using access control policy to bundle the data and called as Data safe architecture. To authorize users and applications data bundle is distributed among them.Hardware tags are formed using the specified policies with parts of data associated with it such as electronic health record etc.It provides monitoring services to control some of the operations like print,save,copy etc.The proposed scheme is applicable only to special hardware compliant machines.In our work, we similarly bind encrypted data and keys inside a data object called Secure-Data. Our scheme is generic.

Squicciarini et al. [7] the idea of self controlling objects were introduced where in SCO's control's how data is used. The SCO's are encoded with data policies user created policies and jurisdictions policies similar to chen et al.SCO's are maintained by SCO network which updates each replica of SCO with the latest change to address the cloud storing multiple copies of data.This scheme uses CP-ABE for policies, the retrieval of plaintext data doesn't occur if the user is unauthorized.

Kayem [10] this solution prevents authorised users from unauthorised data exchange. The solution uses a hash of the encrypted data and key which is invisible digital water mark. Kirkpatrick and Kerr [11]formed a solution which provides accessibilities only to known trusted devices.This prevents the data leakage of data to an unauthorized user and recognizes the user immediately after connection. The drawback of the system is many users never stick to one machine which lacks in portability.This solution disrupts the flexibility of cloud service.

Zic and Nepal [17] and Nepal et al. [16] proposed a technology called the Trusted Extension Device.To enable mobile and portable trust in distributed systems it uses TPM based cryptographic controller. The advantage of this solution is that the keys are encapsulated within the TED device which are never exposed. The cryptographic operations are carried out in TED via API calls. We make use of android applications instead of TED device which is the most economic solution.

Danan Thilakanathan[13] proposed a security model that enable data sharing in a remote telecare environment. The patients connects sensor to their body and measures ECG. They run an app on their smart phone which connects to the sensors using Bluetooth. This app reads all the ECG data and stores it to the cloud server after encryption. Doctors who are authorized uses their partial key to decrypt the data. This solution is asymmetric encryption, as key partition is done here. This work doesn't handle collusion attack between user and cloud.

In this solutions which are studied data access control in distributed environment do not provide full data access control to data owner and focuses only on protecting data from the cloud. Goel et al[15] proposed fine grained attribute encryption .Where a user can decrypt the data only if his given attributes matches with the access policy formed by the data owner.

Boldyreva et al[18] proposed a system where user identity is used to form a key to access the data. This system is called as identity based encryption.

Sahai and Seyalioglu[17] described worry free encryption. In this key a user can send his data to other users without worrying whether they have right to access the data. The scheme works based on functional encryption with public key.

In all of the above solutions, the authorized user is assumed to conform the operations allowed by data owner. However once the data is decrypted and downloaded on to data consumers machine the data owner loses control of his data and the decrypter can utilize the data as he wishes without being caught. In our solution we are introducing trust barrier to the consumer and consider all the authorized data consumers are curious.

In this paper, we combine our previous works [14], [1], [13] when sharing data in the cloud we are providing stronger privacy and security.

[1] uses TED which is a hardware based TPM module to enable secure sharing of data. The device uses a certifying authority for verifying the credentials and decrypts the data if verified.

[13]In this work the data and the policy are bundled to a Safe protect object (SPO).Only if the user adhere to the policy then only he can get the data.

[14] proposes a system which also bundles data and policy similar to the safe protect object. It also monitors the consumer actions on the decrypted data using a background monitoring process. Actions, such as copying or printing, are restricted and periodically neglected and notifications are sent to the data owner if any unauthorised operation are carried out.

In our work we are also using an Android app for the authentication process where the IMEI of the user will be used to verify the user before each login.This will provide an even greater level of security and prevents unauthorized access of the data curious users.In our work we are using Android app for authentication as it is easily available and is cost effective.

III.EXISTING SYSTEMS AND PROPOSED SYSTEM

A.Existing System

There exist Safe Protect where policy of the owner and the data are binded using XACML. The data owner's policy will be used to provide the data about the data to the data owner.

There exists TED (trust extension device) which is used for the authentication of the user during login. This approach can be easily achieved. Nevertheless, there exists security risk. If the adversary (who has stolen the security device) can also break into the computer where the other part of secret key is stored, then it can decrypt all cipher text corresponding to the victim user. It is neither economical to use such devices.

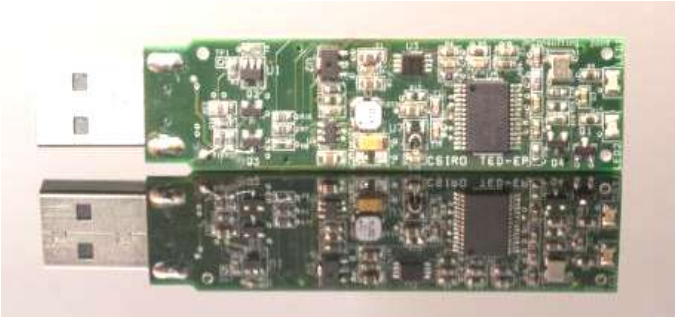

Fig.1 Trust extension device.

Disadvantages of Existing System**:**

- In initial systems there are no solutions for collusion problem and require special hardware compliant machines which limits portability.
- Previous systems didn't had a feasible solution for key management.
- Usage of TED devices is not economical and it isn't easily available.

B. Proposed System

This paper describes an enhanced privacy and security using ABE for data storage in the cloud environment. This mechanism provides the following features:

1. The system is an ABE (Attribute-based encryption) - based mechanism. That is, the data owner will generate certain attributes for his/her data and such data will be accessible only by those users who possess the same attributes.
2. The system provides authentication using android where in the IMEI of the device will be fetched during the registration and the same will be stored in the server and used for further logins.
3. A Privacy Certifying Authority that is responsible for verifying that the data user is valid and authentic. We use the Android device in our work to authenticate and validate all data consumers personnel.
4. The monitoring service keeps track of operations like save, print, copy that are operated on data owner's data and it also provide a feature which detects the unauthorized operations by a curious data consumer.
5. The decryption of cipher text is not a function of the cloud server.

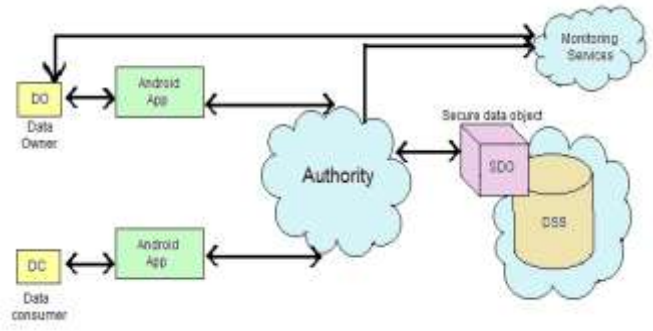

Fig.2 Architecture diagram.

Advantages of Proposed System:

- Giving the data owner an even greater level of control to their data.
- Attribute Verification for security purpose.
- Prevents a revoked consumer from revealing the fully decrypted data in the case of collusion.
- High portability is achieved as we make use of android device for authentication.

IV.IMPLEMENTATION

We developed a prototype for a system using the JAVA programming language.The DSS,CDS and PROXY servers were developed using JAVA programming language,apache TOMCAT and apache axis2.We also made use of Mysql server for data storage.

We are using ABE (Attribute based encryption)for the authentication process where attributes of the users are matched with the owner's policy and allowed to access the data only if the attributes are verified.We are using JAVA pairing – Based cryptography library(jPBC library)for coding purpose.To develop the secure data object,we made use of executable Jar files.

In our work we incorporate XACML policy language.XACML is an open source , attribute based access control policy language built on XML.In our scheme we are binding the dataowner's data and his policies using XACML.We developed Graphical user interface based tool which helps the user to easily specify a wide range of policies over their data.

A simple Android application has been developed for authentication purpose using automated IMEI verification where IMEI of the user is checked everytime before login so as to prevent the unauthorized users from accessing the data.

V. MODULE DESCRIPTION

In this implementation we have 5 Modules,

- Initialization phase.
- The data owner storage and setup phase
- The data share phase
- The data access phase.
- The data consumer revocation phase

Module 1: *Initialization phase*.

The Data Owner and the User must register himself before making any changes to the cloud storage. Android authentication is done before the login to verify the user using IMEI.

Module 2: *The data owner storage and setup phase*.

In this phase the Data Owner securely stores his data in the cloud storage and configures the data for data sharing. The Data Owner sends the data and policy to create the encrypted data contents and policy to a Secure data object . Later sends these details to the cloud storage.

Module 3: *The data share phase*.

In this phase the User requests access to the Data Owner's data to the authority. Authority checks if the
User is authorized to access the data by comparing his attributes with the policy. If a valid user the Authority shares the key with the User.

Module 4: *The data access phase*.

In this phase a User accesses the DO's data after Android authentication and attribute checking. The User gains the encrypted data contents. By using the key shared by Authority, we decrypt the symmetric key and subsequently, the data. Once the data is displayed, the background monitoring operation begins and logs every operation of the User. The owner gets alert notification regarding the same.

Module 5*: The data consumer revocation phase*.
In our protocol user revocation can be achieved without re-encrypting the data each time. The data consumers credentials associated with the data is simply removed from the data base. This way if the revoked data consumer attempt to re-access the data he will never be able to decrypt it.

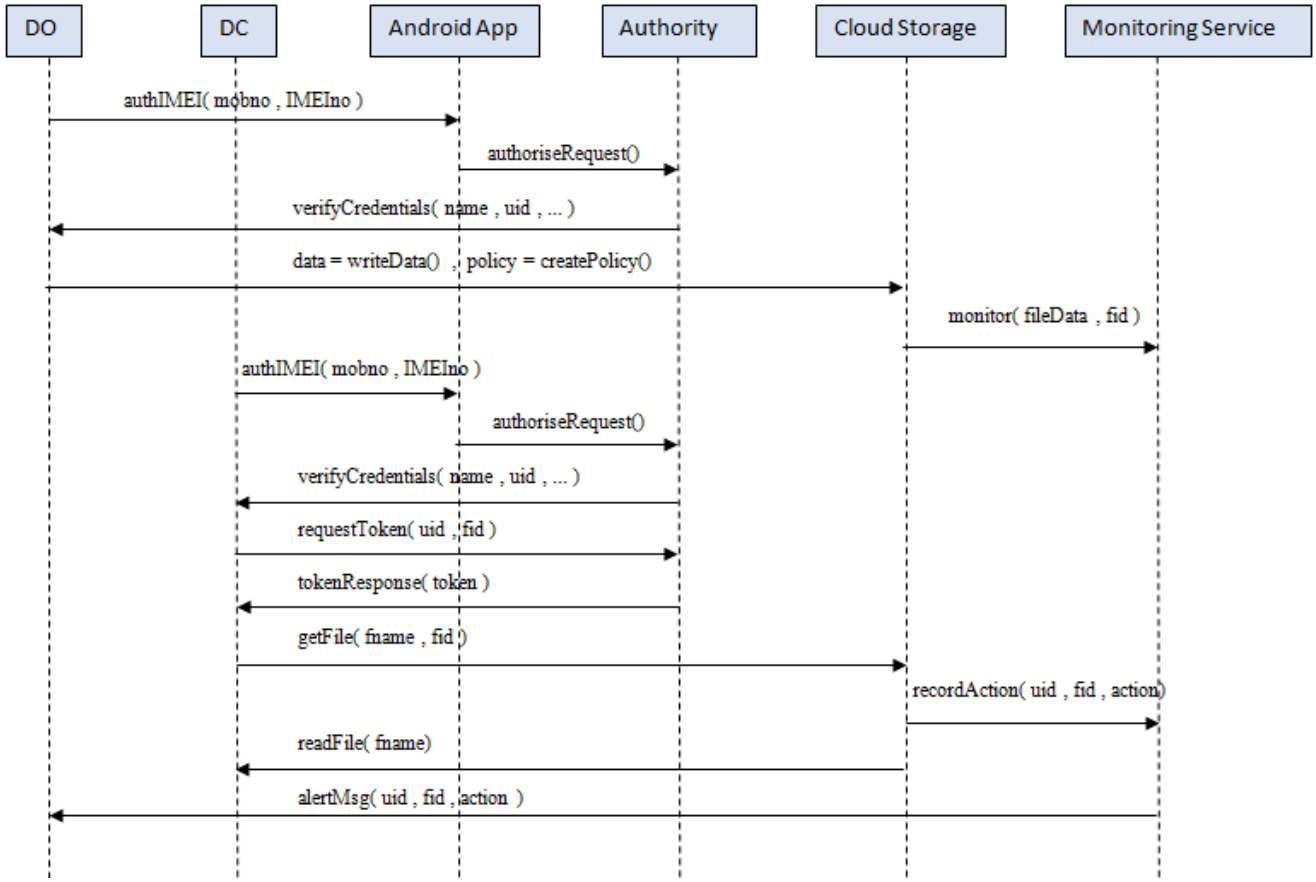

Fig.3 Sequence diagram

VI. METHODOLOGY

The implementation of such a system includes the following steps-

- The Data Owner registers himself by providing his attributes.
- Data Owner creates policy for uploading the file to the cloud storage.
- The data owner uploads the encrypted file to the cloud storage.
- The User who wants to access any of the files in the cloud must login by verifying the credentials with the Database to check the authenticity.
- Once verified through android, the user sends a request for Secret Key to the Authority.
- Authority checks if the user is authorized to access the file requested for, if yes the Secret Key is given to the User.
- Using the Secret Key, user access the files from the cloud Storage.
- User downloads the file from the cloud storage and Decrypts the data.
- An Alert Notification is sent to the Data Owner about the download done by the user.

VII.PERFORMANCE TEST

From the performance test we found that the,the secure data object was comparably slower in encryption process.This is mainly due to the generation of JAR files.Data access time increases exponentially for larger data sizes.However with increased processing power the generation of JAR files optimizes.this will improve access time in near future.

In our solution user may be willing to wait for the process.For instance a business user may be willing to wait longer than a minute to access 35Mb of highly confidential

data.This makes our solution highly reliable and available to users who are more concerned over privacy and availability compared to performance time.

VIII.CONCLUSION

In this paper, we have proposed a model and protocol that will enable private and secure data sharing in the Cloud that provide data owners greater control and ownership over their data using data owner data owner defined policies. We are using ABE for encryption where the attributes of the user needs to be matched with the attributes provided by the owner. Android device is used for the authentication purpose where in the IMEI of the device is used to identify the user.
A monitoring service will be monitoring all the users actions.It disable's all the actions like print,save,etc. and will notify the data owner as soon as any unauthorized actions are performed.An alert notification will be sent to the data owner after each download.

Once the data is downloaded by a data consumer, an alert message is sent to the data owner regarding the same. Thus the data owner will be having a strong knowledge about what is happening to his/her data. This helps us achieving portability and is cost effective.

VIII.REFERENCES

[1] Thilakanathan, S. Chen, S. Nepal, R. A. Calvo (2013): Secure data sharing in the Cloud, Book Chapter on Security, Privacy, and Trust in Cloud Systems, Springer: 45 - 72

[2] Gellin (2012): Facebooks benefits make it worthwhile. Buffalo News (Buffalo NY). Dialog LLC. 2012. Retrieved May 07, 2013 from High-Beam Research: http://www.highbeam.com/doc/1P2-30776177.html

[3] G. Benedis-Grab (2011). Sharing digital data. Science and Children, 48(8), 42-46.

[4] T. Jones and K. Cuthrell. YouTube: Educational potentials and pitfalls. Computers in the Schools 28.1 (2011): 75-85.S.E. Fienberg, and M.E. Martin. Sharing research data. Natl Academy Pr, 1985.Library Hi Tech Newss, Vol. 27 Iss: 4/5: 12 - 14

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. Advances cryptology, 1985: 469 - 472

[6] Y. Yang, J. K. Liu, K. Liang, K. R. Choo, J. Zhou (2015): Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. In Proceedings of 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna, Austria, Lecture Notes in Computer Science, Springer-Verlag [In press]

[7] Squicciarini, G. Petracca, E. Bertino (2013): Adaptive Data Protection in Distributed Systems. Third ACM Conference on Data and Application Security and Privacy (CODASPY), February 2013: 365 - 376

[8] Y. Chen, P. A. Jamkhedkar, R. B. Lee (2012): A Software-Hardware Architecture for Self-Protecting Data. In Proceedings of the 19th ACM Conference on Computer and Communications Security, October 2012: 14 - 27

[9] J. Bethencourt, A. Sahai, B. Waters (2007): Ciphertext-Policy Attribute-Based Encryption. Security and Privacy, IEEE Symposium: 321 - 334

[10] A.V.D.M. Kayem (2010): On monitoring information flow of outsourced data. Information Security for South Africa (ISSA), 2010: 1-8

[11] M.S. Kirkpatrick, S. Kerr (2011): Enforcing physically restricted access control for remote data.ACM conference on Data and application security and privacy (CODASPY '11): 203-212.

[12] Thilakanathan, S. Chen, S. Nepal, R.A. Calvo, L. Alem (2013): A Platform for Secure Monitoring and Sharing of Generic Health Data in the Cloud. Special Issue on Integration of Cloud Computing and Body Sensor Networks, Future Generation Computer Systems.

[13] D. Thilakanathan, S. Chen, S. Nepal, R.A. Calvo: Secure and Controlled Sharing of Data in Distributed Computing. 2nd IEEE International Conference on Big Data Science and Engineering (2013): 825 - 832.

[14] V. Goyal, O. Pandey, A. Sahai, B. Waters (2006): Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on Computer and communications security (CCS'06): 89 - 98

[15] S. Nepal, J. Zic, D. Liu, J. Jang (2011): A mobile and portable trusted computing platform. EURASIP J. Wireless Comm. and Networking 2011: 75.

[16] J. Zic, S. Nepal (2008): Implementing a portable trusted environment. Proceedings of the Future of Trust in Computing Conference: 17-29.

[17] A. Boldyreva, V. Goyal, and V. Kumar, ''Identity-based encryption with efficient revocation,'' in Proc. 15th ACM Conf. Comput. Commun. Secur. (CCS), 2008, pp. 417–426.

[18] A. Sahai and H. Seyalioglu, ''Worry-free encryption: Functional encryption with public keys,'' in Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS), 2010, pp.t46