Attribute Based Encryption For Health Care Data

Mohammad Moinuddin Ansari
Dept. Computer Science and Technology
Dayanand Sagar University
Bangalore ,India
mohdmoinuddin711@gmail.com

Dr.M Shahina Parveen
Dept.Computer science and Technology
Dayananda Sagar University
Bangalore, India
chairman-ct@dsu.edu.in

Abstract

With this effort, we hope to improve attribute-based encryption's (ABE) suitability for access control to cloud-stored data. In order to do this, we focus on granting the encrypted complete control over the access privileges, enabling workable key management even in the presence of many independent authorities, and supporting workable user revocation, which is crucial in real-world applications. Our main accomplishment is an identity-based user revocation component added to the decentralised CP-ABE scheme. By removing the computational load of a revocation event from the service provider, our revocation system is made practical at the cost of some ongoing, but tolerable overhead of the encryption and decryption techniques used by the users. Consequently, a potentially large number of users bear the burden of the computing overhead.

1:INTRODUCTION

A user should only be permitted access to data in some distributed systems if they possess a specific set of credentials or qualities. Currently, using a trusted server to store the data and handle access control is the only way to enforce such regulations. The confidentiality of the data will, however, be jeopardised if any server hosting the data is compromised. In this research, we introduce Cipher text-Policy Attribute-Based Encryption, a system for implementing complicated access control on encrypted data. Even if the storage server is unreliable, encrypted data may be kept private using our approaches since they are secure against collusion assaults.

2:Objective

Primary Objective

- Implementing attribute based Dual key encryption for 32 bit alpha numeric key.
- Actors can be created by the admin. Admin can provide data access control to the users.
- Key updating will be done in a cyclic process.
- Implementing this technology in a hospital domain which suits best

Secondary Objective

- Admin can able to customize the rights provided to the actors.
-

- Due to centralizing the data, recepients can take advantage of being treated at any time as these procedures implemented in a cloud server.
- Each and every in the database has been encrypted dual times using dual key encryption method
- All readings will be displayed in graphs and charts
- Actors will be provided with a separate with a private login to view their login zone.

Goal:

To create Enhanced attribute based encryption in centralized way.. Implementing it in two key encryption. Admin can control data with customisation. The motive of implementing these technologies is to make better relationship between doctors and patients.

4:EXISTING SYSTEM

This theory holds that the current system is attribute-based encryption, which will operate via quantum cryptography, which deals with both mining and architectural design. It is possible to use networking and data mining together in this situation. Data engineering methodology will be the name given to this technique. Quantum Key Distribution Protocols (QKDPs) are used in quantum cryptography to distribute session keys and check for eavesdroppers and to confirm the accuracy of session keys. Here, data configuration won't be possible. Public debates, however, cost valuable energy and necessitate extra communication loops between the sender and receiver. Contrarily, traditional cryptography only offers practical methods for reliable key verification and user authentication.

Sharing secret session keys is facilitated via KEY distribution techniques.

- **Manual efforts**

  More number of persons is required to maintaining the transactions, as the data are maintained in various departments. Also, persons are required for testing the transactions.

- **Slower Transactions**

  The transactions are carried out slowly, because of more manual efforts. More time is needed for preparing data-sheets, entering the data into the data-sheets, verifying and testing the entered data, etc.

- **Low Reliability**

  Although experienced accountants would be processing the transactions, it cannot be said that there would no errors in calculations, because of computational complexities. Also, more time would be needed to regenerate the reports, in case of errors.

- **Slower Reports**

  Considerable amount of time would be wasted in generating and finalizing the reports. The reports generated would not be so attractive as that generated with the computers. If they are prepared with typewriters, then more time would be wasted to generate the reports manually and then through typewriters.

- **Low Data-security and backup**

  Data-security is lower than that with computers. Also, it is difficult to take back up of the data in the reports.

5:PROPOSED SYSTEM

All the information that is now maintained manually is computerised in our suggested system. The data entered are extremely safe thanks to computerization and cannot be accessed or altered by dishonest people. The proposed structure benefits all departments the most. This initiative started with the hiring of qualified personnel that the company required. It speaks to their regularity and work output. It is entirely user-friendly and menu-driven, making it possible for someone to use a project accurately and easily. Any time, it is simple to update the record. The suggested system has the following benefits:

Dual Key Cryptography

It is important to assume that the attacker already has access to the specifics of the cryptographic algorithm when developing security measures.

Reduced manual efforts

The number of persons involved in maintaining the transactions is reduced, so that the processes can be carried out quickly, as the reports are not transferred to any persons for testing, etc.

Faster Transactions

The transactions can be carried out quickly, than the manual efforts. The time taken for transactions would be the time taken for feeding the data into the computer only; there would be no time needed for calculations or generation of reports.

Increased Reliability

The computational complexity is reduced, so that the error-rates are also reduced. Unlike manual efforts, any changes can be reprogrammed in the software, quickly.

Attractive Reports

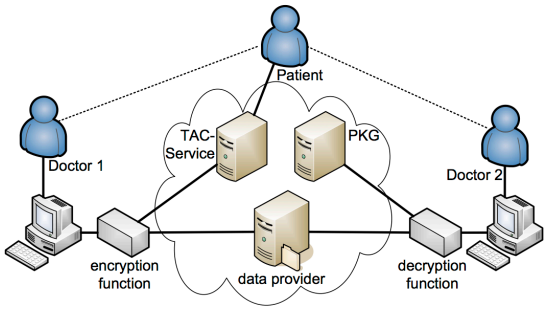
The reports can be generated quickly anytime when they are needed. The reports generated would be neat and attractive and can be changed to any required form.

Secured Data and Backup

Unscrupulous persons cannot access the data stored through the software, as there are passwords for every entry. The large amount of data can be taken backup, so that loss of data is greatly reduced.

6:Attribute Based Encryption - Methodology

Considered recently, attribute-based encryption (ABE) reexamines the idea of public-key cryptography. A message is encrypted for a specific receiver using the receiver's public key in traditional public-key cryptography. By allowing the public-key to be any arbitrary string, such as the recipient's email address, identity-based cryptography, and in particular identity-based encryption (IBE), revolutionised the way that public-key cryptography was previously understood. Roles, for example, and messages can be encrypted with regard to subsets of attributes (key-policy ABE - KP-ABE) or policies defined across a collection of attributes are just a few examples of how ABE goes one step further and defines the identity not as an atomic but as a set of attributes (ciphertext-policy ABE - CP-ABE). The crucial point is that a ciphertext should only be decrypted by someone who possesses a key.



7:IMPLEMENTATION

- The project's implementation phase is when the theoretical design is transformed into a functional system. The achievement of a successful new system and providing the user with assurance that the new system will operate successfully and efficiently in the implementation state are the two most important stages.
- The setup includes

- using straightforward data to test the built programme.
- Error detection and correction.
- Whether or not the system satisfies user requirements.
- checking the system's viability.
- making any adjustments required by the user.
- employee user training.I
- IMPLEMENTATION PROCEDURE: Compared to system design, implementation procedures lack creativity. A system project may be abandoned at any point before implementation, albeit doing so gets more challenging once it enters the design stage.
- Procedural flowcharts, record layouts, report layouts, and a practical plan for converting the candidate system design into an operational one are all included in the final report to the implementation phase. One element of implementation is conversion.
- The implementation plan's conversion section has been completed and authorised.
- Data is transformed.
- On a unique form, parallel processing between the old and new systems is recorded.
- Parallel processing is stopped, presuming there are no issues. Results of implementation are recorded for future use.c.

8:RESULT AND DISCUSSION

The attribute permission for the actors accessible in this application is represented by this result. At first, the chart will include all the actors who are currently available. Additionally, the actor availability will be displayed actor-wise utilising grouping techniques. The number of actors in the arch group is displayed below.

For displaying the permissions, an attribute-wise chart has also been built. The graphic also shows the attribute that users are allowed to use the most. This improves data clarity so that you can see the situation as it is. In order to display each user's attribute permissions actor-wise, the actors are also ungrouped.

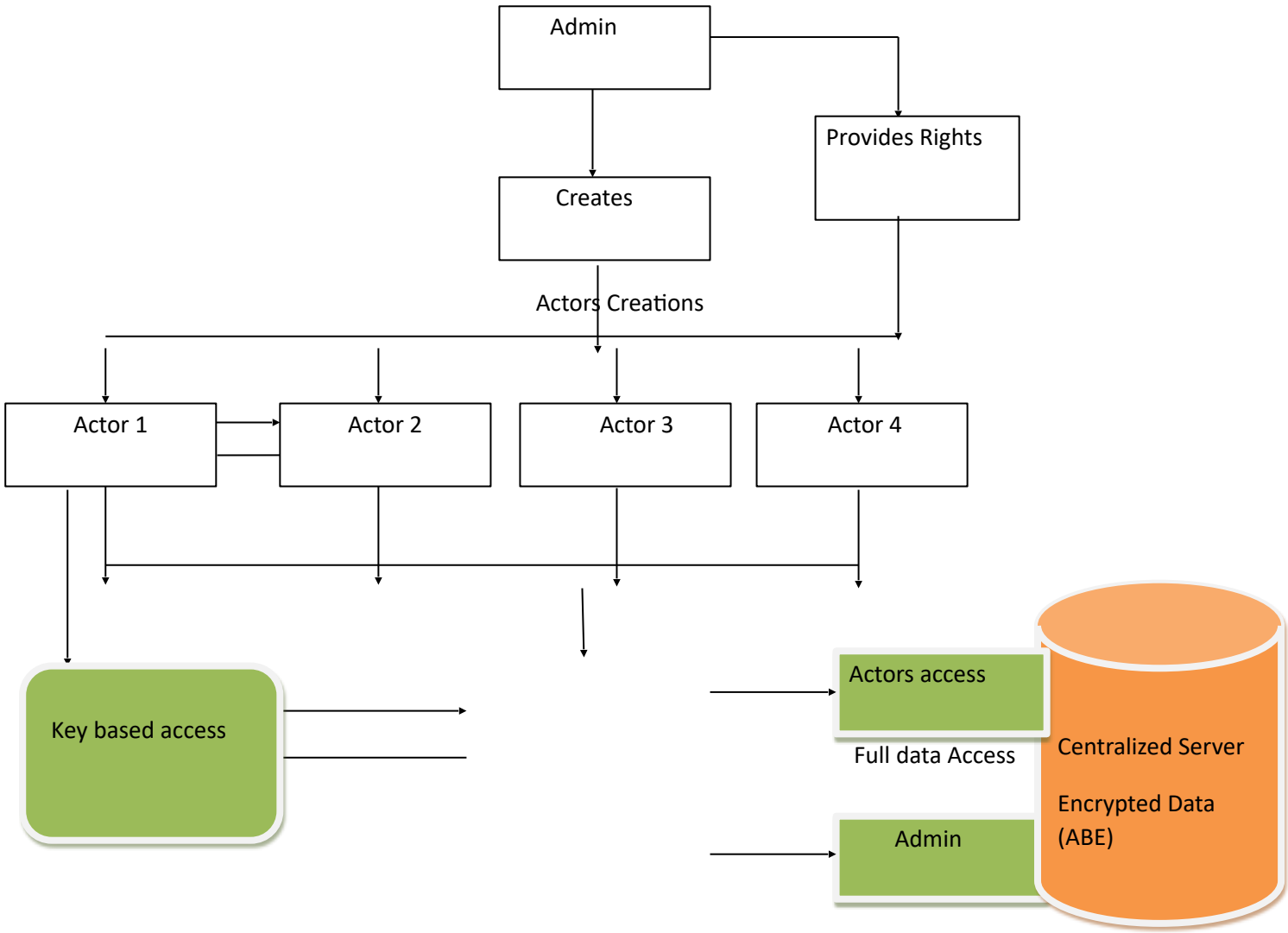
As a result, the suggested system is superior because it performs and is implemented well. Overall system performance has been improved over that of the current system.

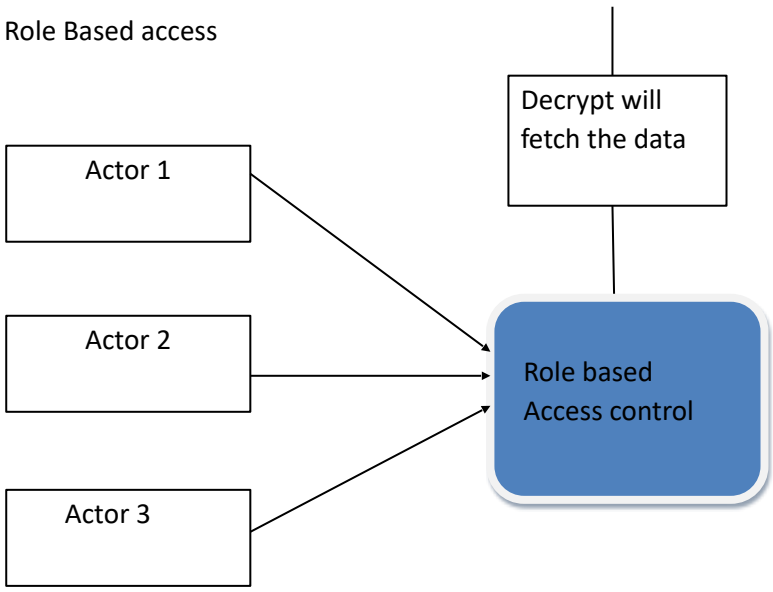
9:CONCLUSION

The system has performed better than expected in terms of efficiency. Before providing the formal proof, we emphasise that our construction is at least as secure as the one by from the perspective of a user whose attributes have never satisfied the access structure defined in the cypher text because the computation is equivalent to the decryption computation provided there in this thesis.

The system resembles a decision support system and offers administrative decision makers useful transformation. Making judgments regarding the allocation of frequently accessed data in the server is aided by this information. Faster implementation of the client's requested system based on their input.

10ARCHITECTURE DIAGRAM





13: References

A. Beimel. Secure Methods for Secret Distribution and Key Sharing. 1996 PhD dissertation, Technion, Israel Institute of Technology, Haifa.
[2] P. Rogaway and M. Bellare. Practical random oracles: A model for creating effective protocols. Pages 62–73 of 1993's ACM Conference on Computer and Communications Security (ACM CCS).
[3] Generalized Secret Sharing with Monotone Functions by J. Benaloh and L. J. Volume 403 of LNCS, Advances in Cryptology - CRYPTO, pages 27–36. 1988 Springer.
[4] B. Waters, A. Sahai, and J. Bethencourt. the toolkit for cpabe. http://acsc.csl.sri.com/cpabe