Security of Confidential Data

Safiya Tehreem[1], Soundarya K P[1], Prajakta M[2]

[1]*Dept. of ISE, The National Institute of Engineering, Mysuru*
[2]*Asst. Professor, Dept. of ISE, The National Institute of Engineering, Mysuru*

Abstract – *Protection of the confidential data plays a very important role in India's economy. With the digitization of traditional records, general and government entities encounter serious problems, like general and government storage and access. Authenticity and reliability are the problems for record management submitted by the general public.*

This paper introduces a research content which uses ciphertext-based encryption to make sure the confidentiality and access control of data. To keep data secure and to accomplish access control, the content publisher encrypts the stored information. This uses AES Rijndael algorithm for encryption and Shamir's algorithm for splitting up the key. Thus, ensuring the safety of the information and enabling privacy.

***Key Words*: Ciphertext-based encryption, Authenticity, Reliability, AES Rijndael algorithm, Shamir's algorithm, Confidentiality.**

1. INTRODUCTION

Cryptography is a technique to exchange messages between one user with another user or to secure communication between them, by encrypting the message to be safe from a third party because it is issued with a key that is not owned by the third party.

Encryption is a process of converting plain text into cipher text. Generally, encryption is classified into two types, namely symmetric encryption where the key is the same for both encryption and decryption, and asymmetric encryption where the key is different for both encryption and decryption.

.NET is a platform which is employed for developing different types of applications like Web applications, Mobile applications, Desktop applications. .NET framework consists of various APIs, Languages and Libraries which helps in developing different types of applications.

.NET Remoting makes a citation of a remotable object accessible to a client application, which then observes and uses this object as if it were an area object. However, the execution of actual code happens at the server side. Activation URLs identify an object and are detected by a connection to the URL. When the server registers the channel, Remoting runtime creates a listener for the object.

A proxy that stands-in as a pseudo-instantiation of the object is formed by infrastructure at the client side. As such, the general public interface of the object must be known by remoting infrastructure in advance. Any method calls made against the object including the parameters passed, identity of the method is serialized to a byte stream and transferred over a communication protocol-dependent channel to a recipient proxy object by writing to the channel's transport sink at the server side.

2. LITERATURE SURVEY

For general cryptographic use, Key allocation schemes aim to attenuate the expense in storing and managing secret keys.

2.1 Access Control in Publish/Subscribe Systems

There are two methods developed to realize scalability. Namely, role-based control of access and policy-driven control of access. From many publishers to the numerous subscribers it achieves delivering data and loose coupling of devices. So that the publisher need not to understand the identity of the subscriber and subscriber need not to understand who that publisher is and from where the data has been taken. There is no direct communication between the publisher and the subscriber. But there is some highly protected data and it must have both the main points of publisher and subscriber. It should contain knowledge about who has published the information and who has accessed that specific information due to privacy issues.

For instance, large database systems like transport, police, healthcare and environmental monitoring concerns about data security. It explains about the protection in publisher and subscriber systems. It provides security while providing the data and also provides access control over the service API.

2.2 Ciphertext-Policy Attribute-Based Encryption

During this tactic the trusted server is developed to keep track and control the providing information. However, confidentiality will be an issue if the duplication of the information is encountered. Thus, deals with large-scale data after encryption. This method secures the data from different kinds of attacks. For instance, collusion attacks, active attacks or passive attacks etc. While during this method entity details are used to support the subscriber's credentials and encryption/decryption of secured data.

Table -1: Summary of literature survey

Referred Paper	Description	Conclusion
Dynamic and Efficient Key Management for Access Hierarchies.	During this defines a key allocation mechanism that implements such an access graph, that is, an assignment of keys to objects and users where a user encompasses a key for that object.	The count of keys increases with the count of branches. It is unlikely to come back up with a hierarchy that may save the total count of keys to be granted.
Practical Leakage Resilient Identity Based Encryption from Simple Assumptions.	Identity-based encryption (IBE) is a kind of public-key encryption during which the public-key of a user will be set as an identity-string of the user (e.g., an email address).	Different secret keys must be generated for the similar identities, and as a result it is tougher to use leakage resilient techniques.
Improving Security and Privacy in Multi-Authority Attribute-Based Encryption.	During this scheme multiple attribute authorities monitor different sets of attributes and issue corresponding decryption keys to the user and	The key dimensions often increase with the amount of attributes and the ciphertext
	encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message.	size is not constant.

3. PROPOSED SYSTEM

We propose a system to develop a windows application which will help to secure the confidential data record in both general and government sectors. The research department collects the research content and stores it in the database. Each research content is encrypted by using the AES Rijndael algorithm and is stored in the database. Random key is generated for encryption and splitted using Shamir's algorithm. In order to view the research content, the Access key is sent to the respective staff/user email for verification. Once Access Key verify, decrypt data using a random key. This enables privacy and security and thus, prevents third party access.

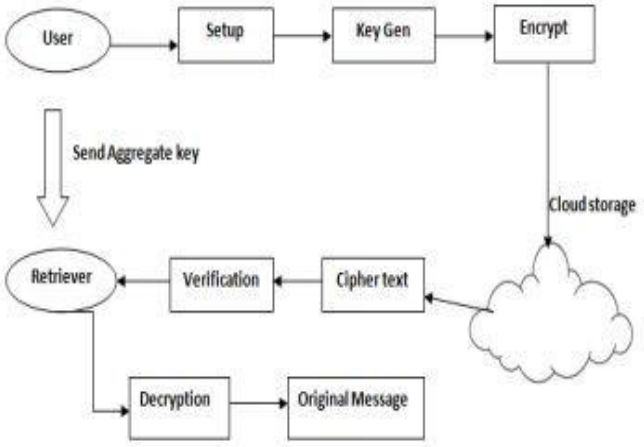

Fig -1: System Architecture

3.1 Advantages of the Proposed System

- It overcomes the disadvantages of existing systems.
- Supports publishers to predict whether the user is trusted or not.
- Reduces the number of keys generated.
- Error free data can be obtained.
- Maintains the confidentiality of information
- Information can be sent to any number of subscribers.
- The information will be secured, and it will reach the subscriber within the fraction of seconds.

4. IMPLEMENTATION

Following are the actors considered in our implementation:

- Admin
- Government staff and General user

1. Admin

Admin have the option to login application by default. Also, the admin Id and password is added to the database by default. Before adding the department, the application will check whether the department is added or not. Departments such as water, electrical, telecommunication etc. Once the department is added, the admin now adds the basic details of government staff based on department using random class in C#. Thus, the staff Id and password will be generated and sent to staff email id using SMTP protocol. and the same procedure is followed for adding the general staff.

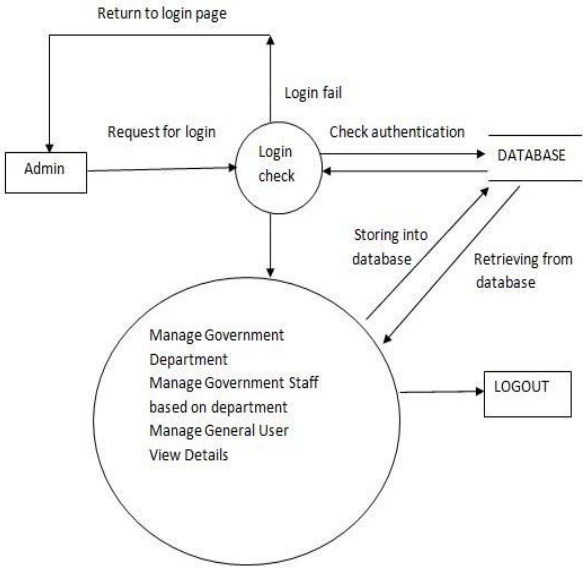

Fig -2: DFD of Admin

2. Staff and General user

Application user login using the data sent by admin and publish a content based on the department by inputting record name and record content. Published content will be encrypted using AES Rijndael algorithm and key will be generated using random class in C#. Key will be splitted into parts in order to be secure and stored in the database along with the encrypted data using Shamir's algorithm.

Application users have the option to request the published content. These requests will be logged into the database. Once the request is approved, the access key will be generated and sent to requested application users' email-id. If the access key is verified, the requested content(encrypted) and splitted parts of key is fetched from the database. The splitted parts of the key will be reconstructed into the original key by Shamir's algorithm. Encrypted data will be decrypted with the original key using AES Rijndael algorithm enabling access to requested data. If the access key is invalid, then invalid access key message will be displayed.

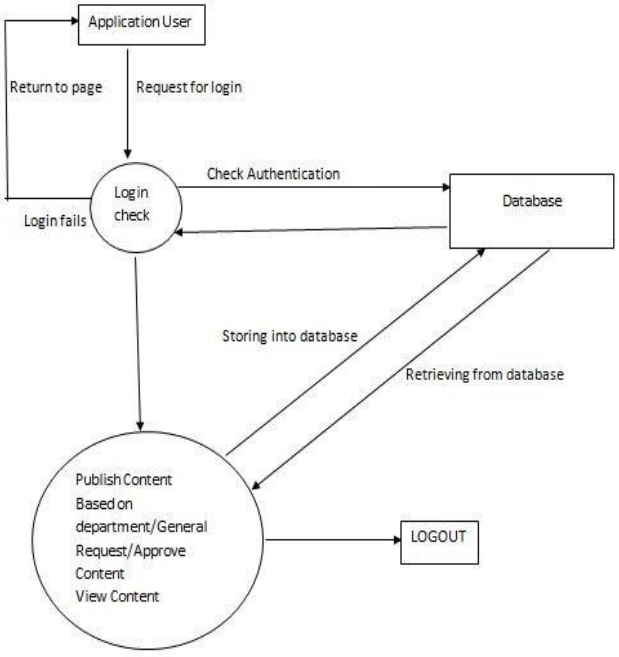

Fig -3: DFD of Application User

4.1 Algorithms

Following are the algorithms used for implementation:

- AES Rijndael algorithm
- Shamir's algorithm

4.1.1 AES Rijndael algorithm

AES is an iterated symmetric block cipher that works by repeating the identical defined steps multiple times. AES encryption algorithm is reversible so that almost the identical steps are performed to complete both encryption and decryption in reverse order. It operates on a fixed number of bytes and it is a secret key encryption algorithm which makes it simpler to explain and implement.

Rijndael algorithm was submitted for Advanced Encryption Standard (AES) for electronic data. Rijndael is an iterative block cipher with a variable length and a variable key length. It is based on some very simple operations like Exclusive OR, permutations of the columns and bits shifts. In each round of algorithm, the original form contains four transformations namely, Byte Substitution, Shift Row, Mix Columns, Add XOR Round Key. The combination column transformation is not used in the last round. The modification involves a mathematical process that is easy to implement at software level by using MATLAB programming because of the matrix-based structure of the algorithm.

This algorithm involves four steps. These steps perform particular transformations consisting of 10, 12 or 14 rounds in the input plaintext.

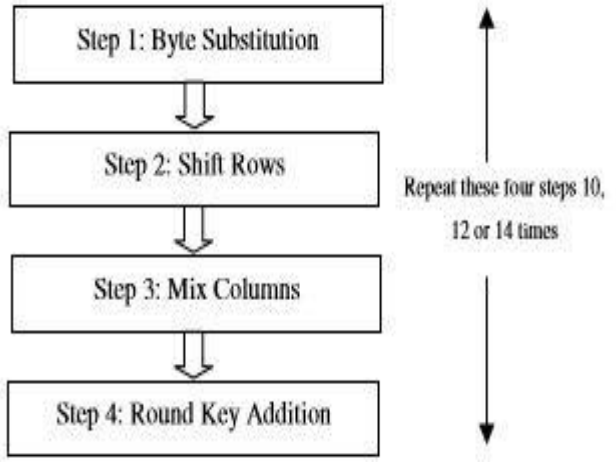

Fig -4: Steps in Rijndael algorithm

Step1: Byte Substitution

During this transformation, a secret S-box is applied to each byte separately. The inverse table has the inverse of the byte substitution that has a mapping of the inverses at the corresponding locations in the S-box.

Step 2: Shift Rows

During this transformation, the rows of blocks are cyclically shifted. The number of bytes shifted in row 0 is zero and the number of bytes shifted in row 1 is one and so on. Inverse of this transformation is in the reverse direction of a simple cyclic shift.

Step 3: Mix Column

During this transformation, a fixed polynomial is multiplied with every column. Inverse of this transformation is again a mix column where multiplication is done with the multiplicative inverse.

Step 4: Round Key Addition

During this transformation, a round key derived using some operations on the cipher key is XORed with the entire block state obtained till the Mix Column transformation. The same round key is the inverse of it and can be XORed during the decryption round.

4.1.2 Shamir's algorithm

Shamir's algorithm is a form of secret key sharing, where a secret key is splitted into parts giving each participant its own unique part. To reconstruct the original secret key, a minimum number of parts(k) are required but the number must be less than the total number of splitted parts. The secret key is divided into multiple parts called shares. These shares are used to reconstruct the original secret key. To unlock the secret key through Shamir's secret key sharing, a minimum number of shares are required.

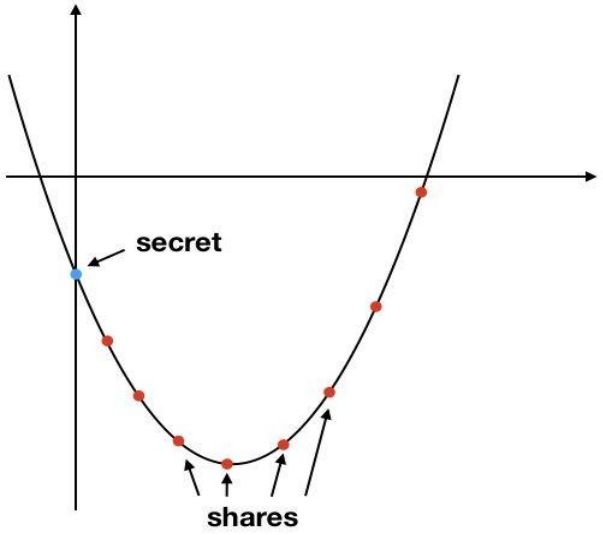

Chart -1: Shamir's secret key sharing

Some of the useful properties of Shamir's secret key sharing:

- **Minimal:** The size of each splitted key should not exceed the size of the original key.
- **Extensible:** When k is kept fixed, k-1 parts can be randomly added or deleted.
- **Secure:** Security of conceptual information.
- **Dynamic:** Security can be easily amplified without changing the secret key, but by changing the polynomial often and constructing new shares.

5. CONCLUSION

This paper has described a new way in providing authentication and confidentiality while the information is delivered from one government staff department to another government staff department without using the intermediate network. The system is able to verify a staff as authenticated to view confidential content or not. If the general user requests government staff to view the content the user may not get the service Thus, achieves security and confidentiality of information.

REFERENCES

[1] Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing. Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin.

[2] A Literature Survey on Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem.Prof. B. M. Kore #1, Archana Jadhav*2, Prof. V. V. Pottigar #3 # Computer Science And Engineering Department, Solapur University, SKN Sinhgad College of Engineering, Korti, Pandharpur, India.

[3] Attribute-Based Encryption Along with Data Performance and Security on Cloud Storage.Ms. Snehal Rathod Department of Computer Engineering Zeal College of Engineering and Research.

[4] FIPS 197, "Advanced Encryption Standard" Advanced Encryption Standard (AES) http://www.ratchkov.com/vpn/aes/aes.html RIJNDAEL http://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html The Laws of Cryptography http://www.cs.utsa.edu/~wagner/laws/

[5] https://cryptography.fandom.com/wiki/Shamir%27s_Secret_Sharing