Enhancing Cloud Data Security by using Rijndael Encryption Algorithm

Ms. Komal S. Landge
Computer Science and Engineering,
Rashtrasant Tukadoji Maharaj Nagpur University Nagpur,
Maharashtra, India

Ms. Ranjana Shende
Assistant Professor Computer Science and Engineering,
Rashtrasant Tukadoji Maharaj Nagpur University Nagpur,
Maharashtra, India

Abstract— **In recent years, with the rapid development occurring in cloud computing and services we used an cloud for large scale data storage. The most important issues is how to control and prevent unauthorized access to data in the cloud. Security is the main intention of our technique through which unauthorised intruder cannot access your file or data in cloud. For this we use an one well known technique is Rijndael Encryption Algorithm (REA) with the help of this algorithm we can stored encrypted data in public cloud and user also decrypt it. We present a hybrid secure cloud storage architecture that allows an organisation to store data securely in a public cloud and maintain information related to organisation in private cloud. In this architecture users who wish to share or access the data only interact with public cloud, there is no access for public users to access the private cloud. Here explores the security of data at rest as well as security of data while moving.**

Index Terms— **architecture, data storage, cloud computing, Rijndael Encryption Algorithm (REA)**

I. INTRODUCTION

With the rapid developments occurring in cloud computing and services, there has been a growing trend to use the cloud for large-scale data storage. This has raised the important security problem of how to control and prevent unauthorized access to data stored in cloud. Security is the main intention of technique through which unauthorized intruder cannot access your file or data in cloud [1]. One well known access control model which is provides flexible controls and management by having two mappings, users to roles and roles to privileges on data objects. In this paper, we will propose a role-based Rijndael encryption scheme that integrates the cryptographic techniques [2]. Our scheme allows this policies to be enforced for the encrypted data stored in public clouds. Based on the proposed scheme, we present a secure -based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud.[3] Cloud data storage can be particularly attractive for users (individuals or enterprises) with unpredictable storage demands, requiring an inexpensive storage tier or a low-cost, long-term archive. By outsourcing users data to the Cloud, service providers can focus more on the design of functions to improve user experience of their services without worrying about resources to store the growing amount of data. Cloud can also provide on demand resources for storage which can help service providers to reduce their maintenance costs. Furthermore, cloud storage can provide a flexible and convenient way for users to access their data from anywhere on any device. In this paper, we address the issues of secure data storage in the public cloud. Public cloud is formed by one or more data centres often distributed geographically in different locations[6].

II. RELATED WORK

A. *Role-based Access Control Method:*

A Role-based access control (RBAC), cloud storage system model is proposes [1]. where the access control policies are enforced by a new role-based encryption (RBE) . The role-based encryption (RBE) scheme with efficient user revocation that combines RBAC policies with encryption to secure large scale data storage in a public cloud. The proposed RBE scheme has potential to be suitable candidate for developing practical commercial cloud data storage system. It takes maximum time to key setup. It is not an flexible algorithm. Its key size is constant.

B. *Rijndael Encryption Algorithm:*

Rijndael Encryption Algorithm technique is proposes [2] new Encryption technique for encryption and decryption purposed. It is an advanced AES algorithm. It is an standard symmetric key encryption algorithm to be used to encrypt sensitive information. It is an iterated block cipher, the encryption and decryption block of data is accomplished by the iteration of a specific transformation. As, Rijndael accepts input one-dimensional 8-bit byte arrays that create data blocks. The Rijndael can be easily implemented and it is

ISSN: 2278 – 7798

one of the most secure algorithm in the world. Its implementation is very flexible. Its security and efficiency is very high.[2]

C. *Cloud Computing Services:*

Cloud computing is the delivery of computing as a service rather than a product. Cloud storage can provide a flexible and convenient way for users to access their data from anywhere on any device .The survey about what is cloud computing and how it is useful for users ,view of cloud computing and Obstacles of cloud computing**.** The survey clearly shows the main drivers of cloud computing to be cost savings, improved flexibility and better scalability. 88% potential consumers are worried about the privacy of their data, security is often cited as the top obstacle for cloud adoption. So we avoid this problem.[3]

D. *View of cloud computing:*

It is an different types of infrastructures associated with a cloud and services provided by cloud. Here introduces an different types of services A public cloud is a cloud which is made available to the general public, and resources are allocated in a pay- as-you-go manner. A private cloud is an internal cloud that is built has full operated by a single organization. The organization has full control of the private cloud, and the private cloud cannot be accessed by external parties. Hence private cloud is often considered to be more secure and trusted. so from this paper we taken an information about private and public cloud infrastructures.[4]

E. *Identity-based broadcast encryption (IBBE):*

The new Identity-based broadcast encryption (IBBE) technique is proposes an system with constant size ciphertexts and private keys that is secure under a more assumption, or which achieves a stronger security , equivalent to full security in IBE schemes. we used an IBBE algorithm with help of this it is impossible to attacker identify an user id.In IBBE scheme one public key can be used to encrypt a message to any possible group of identities. [5]

III. PROPOSED WORK

One of the most secure technique we have designed that is an Rijndael Encryption algorithm with help of this algorithm we can stored encrypted data in a public cloud and user also decrypt it. We present a hybrid secure storage cloud architecture that allows an organization to store data securely in a public cloud and maintain information related to organization in private cloud. In this architecture, the user who wish to share or access data only interact with public cloud, there is no access for public users to access the private cloud. The public cloud is used to stored large amount of data. The encryption of data performed by data owner and decryption of data performed by cloud users. This architecture not only dispels the organisation's concerns about risks of leaking sensitive structure information, but also takes full advantage of public cloud's power to securely store large volume of data. Another significant benefit of this architecture is that it overcomes collusion attacks such as the public cloud colluding with a revoked user, thereby allowing this user to decrypt data that has been encrypted to a role of which the user was a member previously.

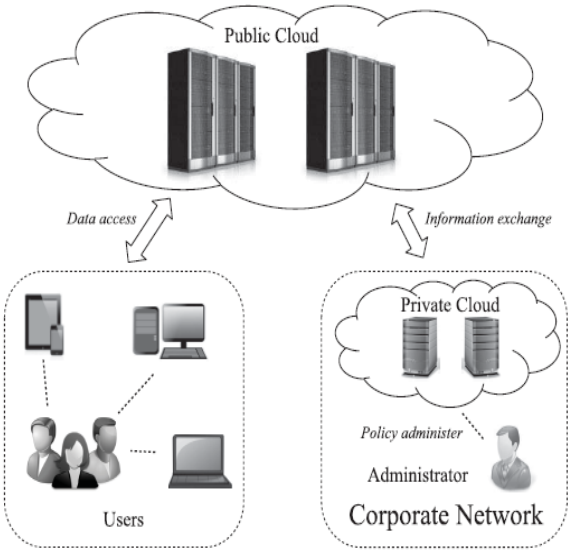

Figure. 1 Hybrid storage cloud

Rijndael Encryption Algorithm(REA)

Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive information. Rijndael is an iterated block cipher algorithm so the encryption or decryption of a block of data is accomplished by the iteration of a specific transformation. Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped in to state . The cipher key output is also a one-dimensional 8-bit byte array. A primary feature of Rijndael is its ability to work on varying sizes of keys and data blocks. It provides extra flexibility in to both the key size as well as block size may be 128, 192, or 256 bits. Since Rijndael specifies three key sizes. Size of data blocks to be encrypted with rijndael is always 128 bits. Initial round of Rijndael is AddRoundKey, this is followed by four iterative round including subBytes, shiftRows, mixColumns and add round key. Rijndael with 128 bit key length has 10 round, 192 bit has 12 rounds and 256 bit has 14 round. Each round consists of the following steps.

1. Initial AddRoundKey
2. SubBytes () Transformation
3. Substitutional Box Created For Subbytes
4. MixColumns () Transformation
5. AddRoundKey () transformation

The SubBytes Step:

The SubByte step is a non-linear byte substitution that operates on each of the 'state' bytes independently, where a state is an intermediate cipher result. Here each byte in the state matrix is replaced with a SubByte using an 8-bit substitution box, the Rijndael S-box.

The ShiftRows step:

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth

ISSN: 2278 – 7798

rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes.

The MixColumns step:
During this operation, each column is multiplied by the known matrix that for the 128-bit key is
:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

The multiplication operation is defined as: multiplication by 1 means no change, multiplication by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing xor with the initial unshifted value. After shifting, a conditional xor with 0x11B should be performed if the shifted value is larger than 0xFF. In more general sense, each column is treated as a polynomial over **GF**(*28*) and is then multiplied modulo x4+1 with a fixed polynomial c(x) = 0x03 · x3 + x2 + x + 0x02

The AddRoundKey step
In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.[3]

IV. EXPERIMENTAL RESULTS

The experimental simulation is conducted by using the Dot Net software package . We create an GUI of an Home page, Registration form, Login form for user to create an his account and providing an different role to users and authenticate them.

Figure 2(a): Home page

Figure.2(b): Registration page

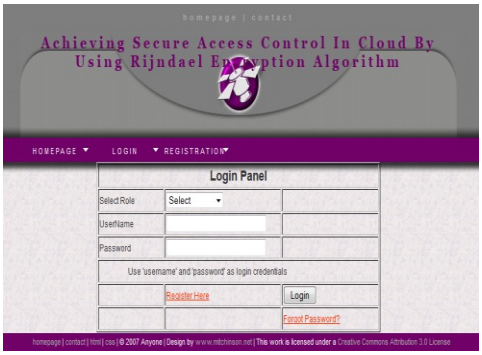

Figure 2(c): Login page

V. CONCLUSION

we will proposed a new scheme that achieves efficient user revocation. Then in future present a secure access control based cloud storage architecture which allows an organization to store data securely in a public cloud and maintaining the sensitive information related to the organization's structure in a private cloud. Both encryption and decryption computations are efficient on the client side, and decryption time at the cloud can be reduced by having multiple processors, which is common in a cloud environment. The proposed system has the potential to be useful in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these access policies.

REFERENCES

[1] Lan Zhou, Vijay Varadharajan, and Michael Hitchens "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage" IEEE transactions on Information Forensics And Security vol. 8, no. 12, December 2013.

[2] Sanjoli Singla, Jasmeet Singh "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013

[3] (2010). From Hype to Future: KPMG's 2010 Cloud Computing Survey [Online]. Available: http:// www.kpmg.com/ES/es/ActualidayNovedades/ ArticulosyPu blicaciones/Documents/2010-Cloud-Computing-Survey.pdf

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

ISSN: 2278 – 7798

[5]C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *ASIACRYPT* (Lecture Notes in Computer Science), vol. 4833. New York, NY, USA: Springer-Verlag, 2007, pp 200– 215..

[6]F. R. Institute. (2010). *Personal Data in the Cloud: A Global Survey of Consumer Attitudes* [Online]. Available: http://www.fujitsu.com/downloads /SOL/fai/reports fujitsu_personal-data-in-the-cloud.pdf.

[7] (2011). Global Survey: Has Cloud Computing Matured? [Online]. Available: http://www.avanade.com /Documents/Research%20 and %20 Insights . Global_Survey_Slide_Has_Cloud_Matured. Pdf

[8]Sanjoli Singla, Jasmeet Singh, "Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm", Global Journal of Computer Science and Technology (GJCST), Vol. 13, Issue 5, 2013.

[9] P. Samarati and S. D. C. di Vimercati, "Data protection in outsourcing scenarios: Issues and directions," in *Proc. ASIACCS*, Apr. 2010 pp. 1–14.

First Author: Ms. KOMAL S. LANDGE

Department of Computer Science and Engineering,

G. H. Raisoni Institute Of Engineering And

Technology

For Women,

Nagpur, Maharashtra, India

Mobile No.-8412965346

Education Details-B.E (CSE) from GWCET, Nagpur

Pursuing M.Tech (CSE) From G. H. Raisoni Institute Of Engineering And Technology For Women,Nagpur

Second Author: Ms. RANJANA SHENDE

Department of Computer Science and Engineering,

G. H. Raisoni Institute And Technology For Women,

Nagpur, Maharashtra, India

Mobile No.-9766969604

Education Details: B.E.(CSE) from K.D.K. college Nagpur,

M.Tech (CSE) from G.H. Raisoni College Of Engineering, Nagpur

Publications: IJERT, IJCST

Membership: CSI member

ISSN: 2278 – 7798