Double Encryption Using Rijndael Algorithm for Data Security in Cloud Computing

D.Gayathri
Lecturer, MCA Dept, Andhra Loyola PG College, Vijayawada, India.

Manjula.A
Lecturer, MCA Dept, Andhra Loyola PG College, Vijayawada, India.

Abstract – Cloud Computing is a new computing paradigm that attracted many computer users, business and government agencies. Cloud computing brought a lot of advantages where everyone can access computer services through internet, thus avoiding physical hardware or servers .In this case Data security becomes more important while storing data to cloud. Cloud computing provides a way to share distributed resources and services that belong to different organizations or sites. The resources shared with the cloud are accessed via a network in an open environment can make a security threat (passive or active threats) to our data.

In this paper the authors implemented Rijndael and explain the security lies in it when stored data in encrypted form. Besides the security provided by the cloud storage provider, storing data in double encrypted format using Rijndael provides confidentiality.

Here to encrypt a file we are using Rijndael algorithm. After encrypting (the process of converting plain text to cipher text using substitutions and transpositions) the data is un-intelligible and confidential; we can decrypt (the process of converting cipher text to plain text) the file to get the plain text. Hence the personal data remains secure thus avoiding security breach in cloud.

Index Terms – Cloud computing, AES, Security.

1. INTRODUCTION

Cloud computing is a new computing approach where in computer processing is being performed though internet by a standard browser. Cloud computing based services and applications offers some benefits such as cost savings, scalability, reliability, maintenance, and mobile accessible.

Deployment Models:

The four development models differ in specific characteristics that supports needs of services and users of the cloud in particular ways.

Private Cloud: The cloud infrastructure has been deployed, and is maintained and operated for a specific organization.

Community Cloud: The cloud infrastructure is shared among number of organizations with similar interests and requirements.

Public cloud: The cloud infrastructure is available to the public on a commercial basis by a cloud service provider.

Hybrid Cloud: The cloud infrastructure consists of number of clouds of any type, but the clouds have the ability through their interfaces to allow data/applications to be moved from one cloud to another.

Challenges: One of the main challenge of cloud computing is security and privacy. Using cryptographic encryption system we can maintain, authenticity, confidentiality, data integrity to our files.

While deploying data to any model, if we store the file to the cloud by double encrypting it with Rijndael algorithm provides more security.

2. PROPOSED WORK

Implementing Rijndael algorithm in VB.net for providing data security. Rijndael was named after the two Belgian cryptographers (Dr.Joan Daemen & Dr.Vincent Rijmen) who developed and submitted it. On November 2001, AES (which is standardized version of Rijndael) became a FIPS standard (FIPS 197).

Like DES, AES is a symmetric block cipher; however AES is quite different from DES in number of ways.

The algorithm allows for a variety of block and key sizes .The AES states that the algorithm can only accept a block size of 128 bits and a choice of three keys-128,192,256 bits.

3. IMPLEMENTATION & RESULTS

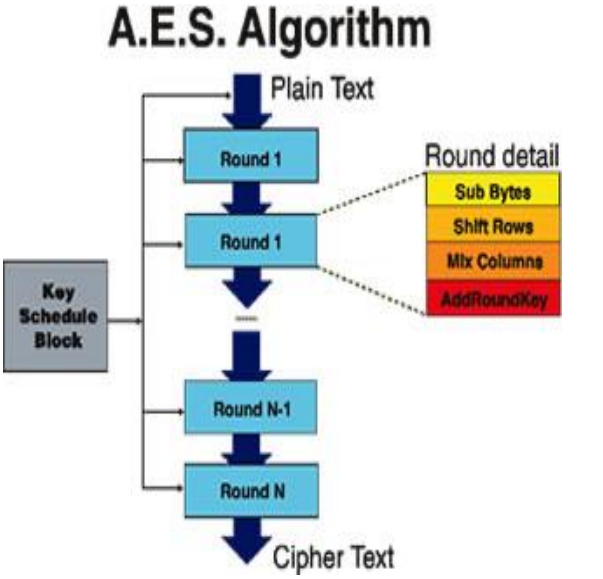
The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

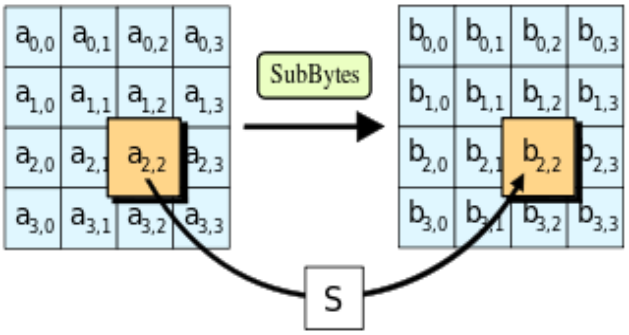
You take the following Rijndael steps of encryption for a 128-bit block:

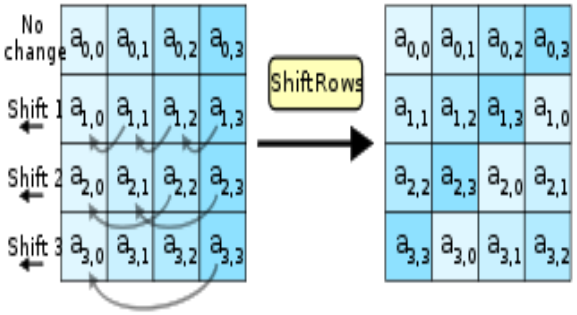
1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).

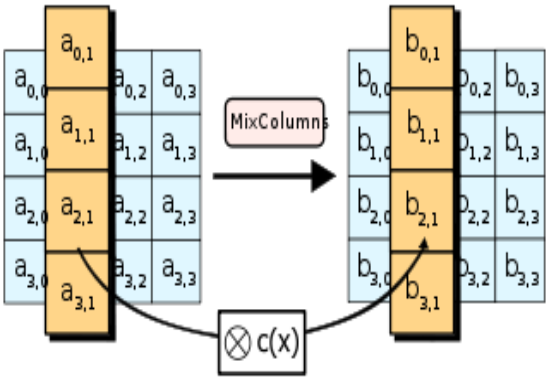
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

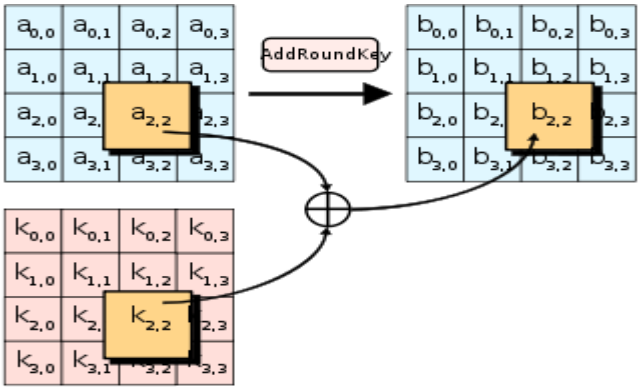
The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.







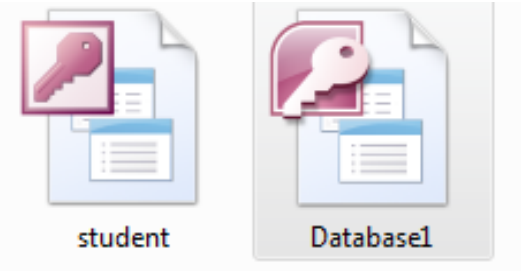




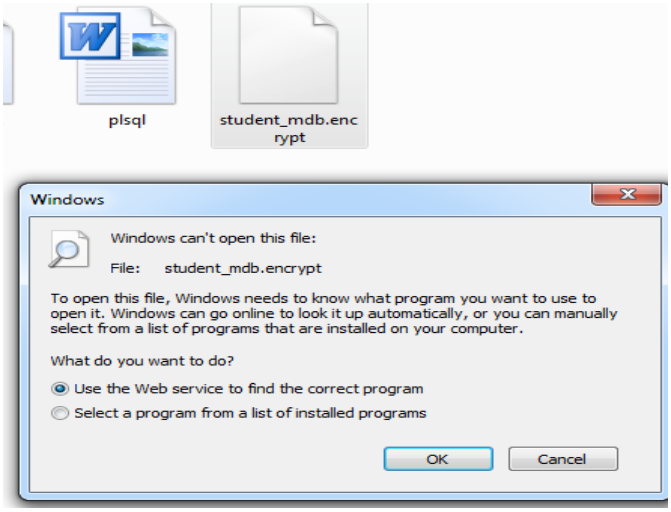
The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- Sub Bytes
- Shift Rows
- Mix columns
- Add round key

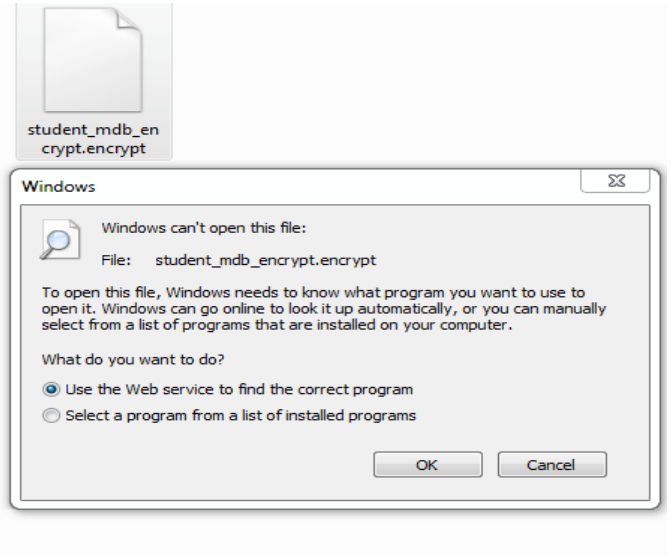
Before Encryption



After Single Encryption



After Double Encryption



4. CONCLUSION

With the rapid increase in the adoption of cloud computing by many organizations security issues arise. In this implementation after single encryption we get file.encrypt , we can double encrypt by selecting the encrypted file which have an extension file.encrypt.encrypt which is more secure encryption process. Using Rijndael for double encryption of files (text, images) provides more security and avoids security attacks on cloud computing when storing data to cloud.

REFERENCES

[1] Masayuki Okuhara et al, “Security Architecture for Cloud Computing”, FUJITSU Sci. Tech. J., Vol. 46, No. 4, pp. 397-402 (October 2010)
[2] Sun Microsystems, Inc., “Introduction to Cloud Computing Architecture”, White Paper, 1st Edition, June 2009
[3] Gerald Kaefer, “Cloud Computing Architecture”, Corporate Research and Technologies , Munich, Germany, Siemens AG 2010, Corporate Technology
[4] Peter Tseronis, “Cloud Computing Overview: A Federal Government and Agency Perspective”, ArchitecturePlus Seminar -Cloud Computing, Web 2.0 and Beyond: A Vision of Future Government Operations, August 13, 2009
[5] Kangchan Lee, “Cloud Computing”, Vice Chairman of ITU-T FG Cloud Chairman of Mobile Cloud WG in CCF in Korea, ETRI.
[6] Singh, Aarti, and Manisha Malhotra. "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review." International Journal of Computer Networks and Applications 2.2 (2015): 41-45.
[7] A Nithya, B Ramakrishnan, Resul Das, “A Novel Approach for Data Privacy Using Attribute Based Scheme Algorithm for Cloud Computing”, International Journal of Computer Networks and Applications (IJCNA), 3(4), PP: 70 – 77, 2016, DOI: 10.22247/ijcna/2016/v3/i4/48567.
[8] Souryendu Das, “Distributed File Systems Implementation on an Edge Router using GlusterFS for Cloud Applications”, International Journal of Computer Networks And Applications (IJCNA), 3(1), PP: 1 – 8, 2016.