ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-3, 737 – 741

HYBRID ENCRYPTION FOR CLOUD DATABASE SECURITY

Amanjot Kaur[1], Manisha Bhardwaj[2]

[1]*MTech Student, Computer Science Department, LPU, Jalandhar, Punjab, India,* ***er.aman_jot@yahoo.co.in***
[2]*Assistant Professor, Computer Science Department, LPU, Jalandhar, Punjab, India,* ***ermanisha.cse@gmail.com***

Abstract

In cloud computing environment the new data management model is in use now a days that enables data integration and access on a large scale cloud computing as a service termed as Database-as-a-service (DAAS). Through which service provider offers customer management functionalities as well as the expensive hardware. Data privacy is the major security determinant in DAAS because data will be shared with a third party; an un-trusted server is dangerous and unsafe for the user. This paper shows a concern on the security element in cloud environment. It suggests a technique to enhance the security of cloud database. This technique provides the flexible multilevel and hybrid security. It uses RSA, Triple DES and Random Number generator algorithms as an encrypting tool.

Index Terms: *CSP, Cloud Computing, encryption, hybrid/multiple encryption*

---------- *** ----------

1. INTRODUCTION

Taking into account the services provided by cloud computing is numerous. But still there are some security concerns that are to be redressed. Especially because cloud users have no choice but to rely on the service provider. Amongst the possible solutions one can keep a local copy of its data which is not feasible as we are taking the benefit of the services of the CSP (cloud service provider) [1]. Another factor of concern is that the cloud is still under development process and there are no set standards for the data storage and application communication. So one couldn't move his data by changing service provider though some organizations are working towards this direction and will soon come out with a solution but till that time, we must have some mechanism to provide security to the critical and private data stored in the cloud like credit card information and passwords. Keeping in view this fact, some application must be developed that will implement multi-level hybrid encryption mechanism by using some strong cryptographic algorithms viz. RSA, Random Number Generator and 3DES.

1.1 3DES

DES was superseded by triple DES (3DES) in November 1998. 3DES is exactly what it is named–it performs 3 iterations of DES encryption on each block. It can do this in a number of ways, but the most common method is the Minus Encrypt-Decrypt-Encrypt (-EDE) method. Each iteration of 3DES using –EDE will encrypt a block using a 56-bit key. After encryption, use a different 56-bit key to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key. Another method that can be used is Minus Encrypt-Encrypt-Encrypt (-EEE). This is three successive encryptions using a different 56- bit key. There are several keying methods that 3DES uses. All three keys can be independent of each other, or the first and third keys can be identical, with the second key being unique. [2] All three keys can also be identical, which provides the least security, but is also the fastest to encrypt with. 3DES is still approved for use by US governmental systems, but has been replaced by the advanced encryption standard (AES)

1.2 Random Number Generator

The cryptography mechanism lot of random numbers would be needed for the purpose of creating random
Keys. The best a computer can produce is a pseudo-random-sequence generator. A pseudo-random sequence is one that looks random. [3] The sequence's period should be long enough so that a finite sequence of reasonable length—that is, one that is actually used—is not periodic. If it has been needed a billion random bits, don't choose a sequence generator that repeats after only sixteen thousand bits. These relatively short non periodic subsequences should be as indistinguishable as possible from random sequences.

1.3 RSA

RSA is a commonly adopted public key cryptography algorithm. The first, and still most commonly used asymmetric algorithm RSA is named for the three mathematicians who developed it, Rivest, Shamir, and Adleman. RSA today is used

in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules. Since it was introduced in 1977, RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium. In the authentication scheme, the server implements public key authentication with client by signing a unique message from the client with its private key, thus creating what is called a digital signature. [4] The signature is then returned to the client, which verifies it using the server's known public key.

2. METHODOLOGY & TOOLS

The methodology used is proposed by Craig Gentry of IBM who suggested Lattice based Homomorphism Encryption technique to ensure privacy and security of data. [5] The technique suggested here is based on three encrypting algorithms RSA, Random Number Generator and 3DES to ensure the data security and privacy in a multi-level hierarchical order i.e. one after the other. The design and implementation of this proposed methodology is achieved using Microsoft Technologies i.e. **ASP.Net and SQL Server 2012** which is best compatible and being used in the cloud service by Microsoft. For the Implementation we will demonstrate the functionality using Microsoft Window Azure Service. A layered architecture is used for developing and implementing the functionality as described:

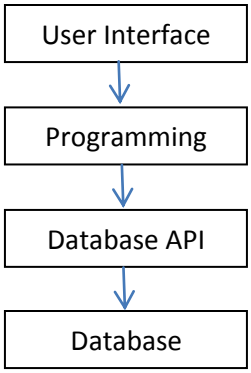

Fig 1: Layered architecture

The user interface will be developed using ASP.Net Framework 4.0.

The Programming Language used will be C#. In this layer different algorithms will be implemented. The data received from the Programming layer will be sent to the SQL Server using ADO.Net SQL Client API for SQL Server communication. SQL Azure interface is used to store the data in the Cloud.

3. PRACTICAL PROCEDURE TO BE FOLLOWED FOR IMPLEMETATION

3.1 Developer's part:

1. Install Visual Studio 2010 and SQL Server 2012.
2. Design the Code for three encryption algorithms in C#.
3. Design the Front End using Asp.Net.
4. Setting Database in Application SQL Azure Service Configuration [Storage Section].
5. Connect the SQL Azure Database with SQL Server.
6. Host the Website on Domain.

3.2 Admin' part:

1. Select encryption algorithm that will be used to generate keys for user's authentication.
2. Can view all users' database.

3.3 User's part:

1. Registration at front end website to create user id.
2. Received public & private key of RSA, vector & key of 3DES from registered id in step1, forwarded by admin.
3. Use keys received in step2 to login as authenticated user.
4. If authentication is succeeded, then only services can be used.

3.4 Research Design:

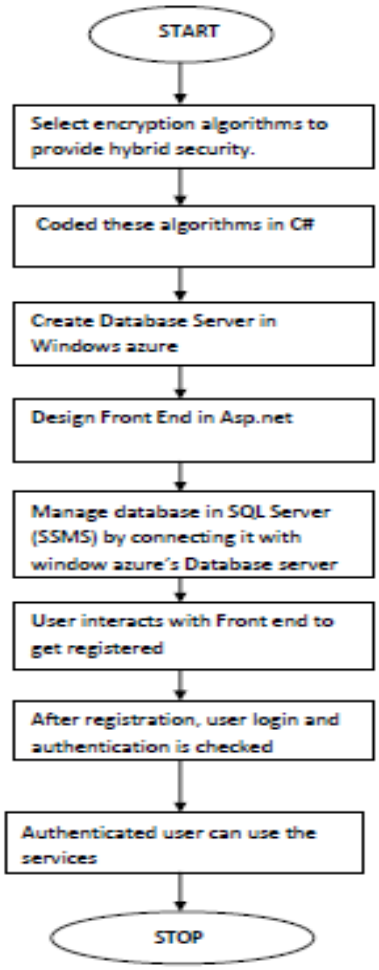

Fig: 2 Research Design

4. RESULTS

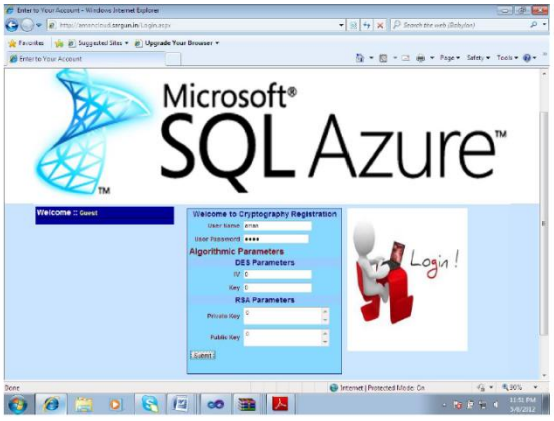

Fig 3: Admin's login

Fig 4: Algorithm Selection

Fig 5: User's registration

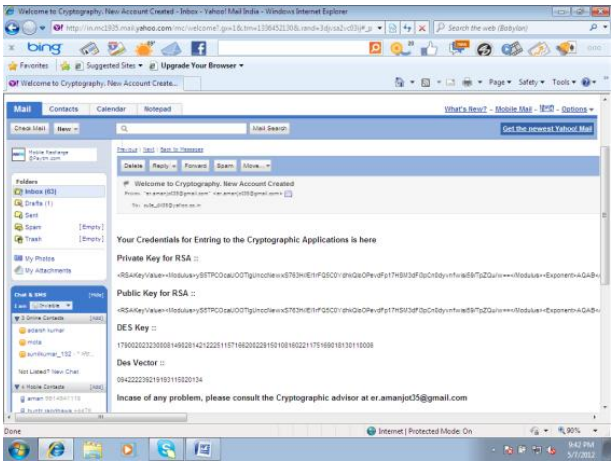

Fig 6: Received keys in mail

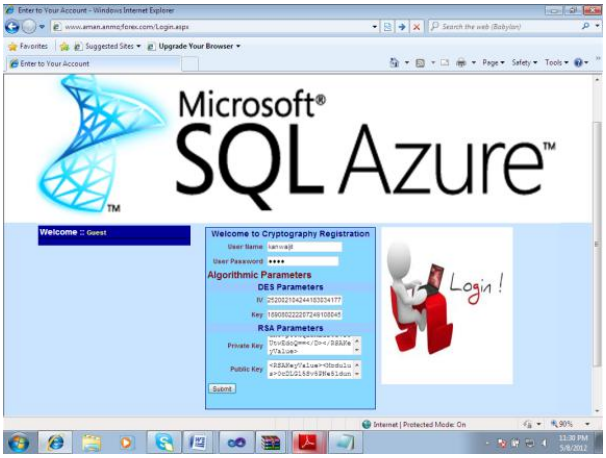

Fig 7: Registered user' login

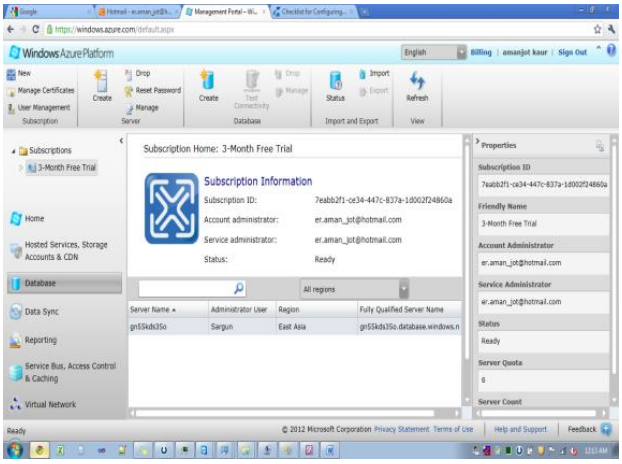

Fig 8: Server is created in windows azure

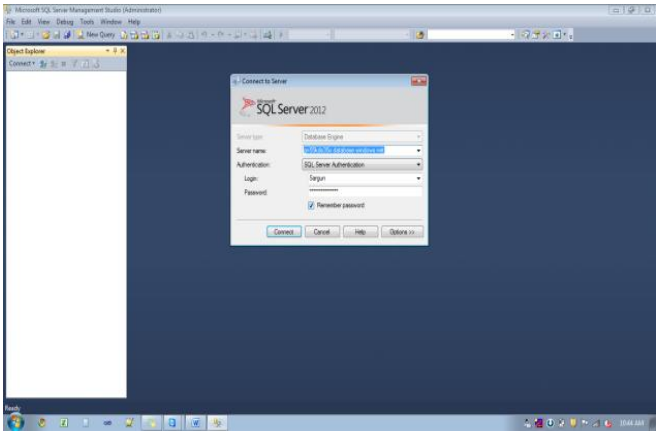

Fig 9: Connect SQL server with windows Azure

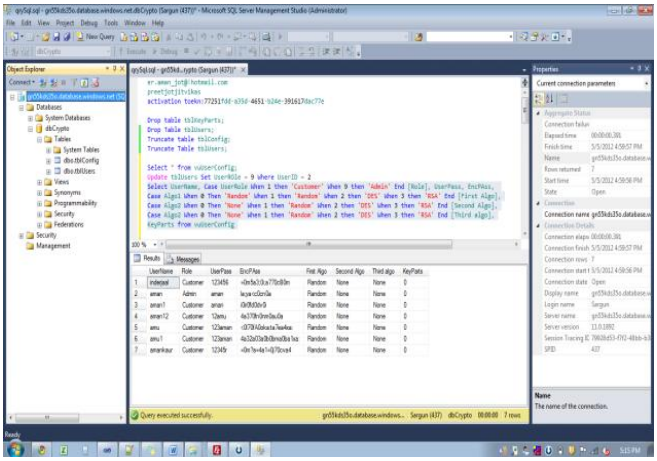

Fig 10: Database of Azure Server

5. CONCLUSION

From the implementation of code the security has been enhanced. One can have hierarchy of application of algorithms. The Encryption Algorithm applicability provides the flexibility in range and sequence to the user's choice because from the three of the Encryption Methods a user can apply all or omit any in any order. Even if the user does not select any encryption technique, then random number algorithm will be implemented by default thus providing atleast a single level security. The opted sequence will also be stored in the database so that the decryption may be possible.

The negative effect of this scheme is that it creates an overhead on the query performance due to multilevel of encryption and decryption but for the sake of security the performance issue can be over looked as we are concerned with only a small amount of data like that of passwords and not the large files. In this way we can conclude that multilevel hybrid encryption enhances security.

6. FUTURE WORK

When the size of data is increased then its computation time is increased, one can decrease computation time by using appropriate methods. In ADO.NET, when decryption process is carried down then private key corrupts occasionally. To resolve this problem one can generate one's own code without using any encoding method built in .net framework.

REFERENCES

[1]. Farzad Sabahi (2011),"cloud computing security threats and responses", Azad university Iran.

[2]. Himani Agrawal and Monisha Sharma," Implementation and analysis of various symmetric cryptosystems" Indian

Journal of Science and Technology, Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

[3]. William Stallings," Cryptography and network security".

[4]. Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Iss ue 2, June 2011 I S S N : 2 2 2 9 - 4 3 3 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1

[5]. Craig Gentry of IBM(2010),"A dissertation submitted to the department of computer science and the committee on graduate studies of stanford university in partial fulfillment of the requirements for the degree of doctor of philosophy".

[6]. https://www.windowsazure.com /enus/home/features/sql-azure/

[7]. Manisha Bhardwaj, Sarbjeet Singh, Makhan Singh "Implementation of Single Sign On and Delegation mechanisms for Alchemi.NET based grid computing framework." The International Journal of Information Technology & knowledge management, Jan-June 2011, Vol -4 , pp 289-292.

BIOGRAPHIES

Amanjot Kaur received her B.Tech degree in Computer Science & Engineering from Punjab Technical University, Punjab, India, in 2009. Currently she is pursuing M.E degree in Computer Science & Engineering from Lovely Professional University Phagwara, India.

Manisha Bhardwaj received her M.E. degree in Computer Science & Engineering from Punjab University Campus, Chandigarh, India in 2010, working on grid security systems architecture. Currently she is working as assistant professor in Computer Science & Engineering Department at Lovely Professional University Jalandhar, India. She has 3years of Teaching Experience and her research interests include parallel and distributed systems, distributed security architectures, distributed services like grid and web services, privacy and trust related issues in distributes environments.