Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security of N-Tier Architecture using NTRU

Amandeep Kaur Gill*
M.Tech, Research scholar
CSE, RIMT-IET, Mandi-Gobindgarh,
India

Charanjit Singh
Assistant Professor
CSE,RIMT-IET, Mandi-Gobindgarh,
India

Abstract— In these days, the security is essential for all the applications on the network. For providing the security to many applications on the network, numbers of mechanisms are used. But there is no implementation of any mechanism for security on the N-tier architecture till now. The NTRU algorithm is concluded as a best and fast algorithm for providing security on the clouds. NTRU is a public key cryptosystem, which provides best security to cloud computing by encrypting and decrypting the data. This paper focuses on the security of the N-tier architecture using NTRU algorithm. The main aim of this research is providing the security to the applications which uses the N-tier architecture.

Keywords— Encryption, Decryption, N-Tier architecture, NTRU cryptosystem, Security.

I. INTRODUCTION

Cloud Computing is an emerging paradigm in which users can store data online on cloud storage and access anytime, anywhere according to their requirements. There are number of issues related to the cloud computing like Security, Access Control, Authentication, Auditing issues etc. but one of the most important issues is the DATA SECURITY. Many applications like ebay.com make use of extensive databases to store the data and are accessible from anywhere by the multiple people simultaneously via World Wide Web. Applications that uses database and are accessible can be implemented using 3-tier architectural model. There is 1, 2, 3 or more tier architectures [9, 10].

1-Tier: In 1-tier architecture, data and application layers can run in one computer only. In order to achieve 1-Tier architecture, we have to use the embedded database system. It is that system which cannot run in an individual process. Otherwise, there will be at least 2-Tier architecture exists because non-embedded databases can run only in an individual computer (tier).

2-Tier: Either application and presentation layer can only run in one computer or application or data layer can run in one computer only but the whole application cannot run in more than 2 computers.

3-Tier: This is a easiest case of N-Tier architecture. All the three layers application, presentation and data layer are able to run in three different computers. These three layers can also be deployed in one computer practically.

N-Tier: Also known as the “layered” architecture. N usually denotes 3 or more tiers (layers). It can be used to model both a web-based application and a desktop application.

II. CLOUD COMPUTING & ITS SECURITY ISSUES

A. Cloud Computing

A **cloud** is a large pool of easily accessible virtualised resources, such as hardware, software, development platforms and/or services. So, the users don’t need to store their data at their end as all the data is stored on remote server. **Cloud Computing** is internet based computing whereby shared resources, information and software are provided to computers and other devices on demand. Users are billed for the services according to how much they have actually used the resources or services. Cloud Computing is also defined as a model for enabling on-demand network access to a shared pool of configurable computing resources like networks, services, applications, storage and servers, that can be provisioned and released very fast with minimal service provider interaction or management effort [1, 2, 3].

B. Security Issues

The number of security issues in cloud computing are explained below [4]:

1) Privacy and Confidentiality: When the client host data to the cloud storage there should be some guarantee that only authorized users can access to that data. Proper practices, privacy policies and procedures should be provided to the cloud users to assure their data safety. It should be assured to the cloud seekers that data will be confidential that is hosted by them.

2) Data Integrity: Data Integrity which means data sent is same as the message received i.e. it is not altered in between. It is ensured by the firewalls and intrusion detection system (IDS). For ensuring the data integrity, cloud service providers should have to implement one mechanism among many mechanisms.

3) Data Location and Relocation: It offers a high degree mobility of data. The location of data is not always known to the cloud users. There should be responsibility of the cloud providers should to ensure the data security of systems and provides the authentication mechanism to safeguard the cloud user's information. The movement of data between different locations is another issue. Firstly the data is stored at the location that is decided by the Cloud provider. data is often moved from one place to another because cloud service providers have contracts with each other so that they can use each other's resources.

4) Data Availability: The data which is normally stored in the form of chunk stored on different servers always residing in different locations or in different Clouds. In this case, the major issue is data availability because it becomes difficult, the availability of uninterruptible and seamless provision.

5) Storage, Backup and Recovery: The cloud provider should have to ensure the adequate data resilience storage systems for the movement of data to the cloud. At least they should be able to provide RAID (Redundant Array of Independent Disks) storage systems. They should have to provide the backup services for the certain application that are important for the business, those running the cloud base application so that in case of a serious hardware failure they can roll back to an earlier state.

III. N-Tier Architecture

A. *N-Tier Architecture*

N-tier architecture is that architecture which consists of n tiers, including a client tier, a database tier, and n-2 tiers in between them. The client tier is that tier which acts as an interface between the system and the user, the database tier is that which manages the database and middle tier is used to provide the communication between other tiers. For n-tier, some of the layers of 3-tier architecture have been broken into number of layers and these layers may be able to run on more tiers. For example, Application layer can be broken into persistence layer, business layer or more and Presentation layer can be broken into client and client presenter layer. In Fig. 1, in order to claim a complete N-Tier architecture, client business layer, presenter layer and data layer should have an ability to run in three separate computers (tiers). Practically, all these layers can also be deployed in one compute (tier) [9].

- **Client layer**: This layer is interacts with users directly. There may be different types of clients coexisting, such as Window form, WPF, HTML web page and etc. [9]
- **Client presenter layer**: This layer consists of the presentation logic required by clients, such as ASP .NET MVC in IIS web server. It also adapts different clients to the business layer [9].
- **Business layer**: This layer is also known as domain layer because it handles and encapsulates all the business logics and domains [9].
- **Persistence layer**: This is known as data access layer (DAL) because it handles the read/write of data to data layer [9].
- **Data layer**: It contains the external data source, such as a database [9].

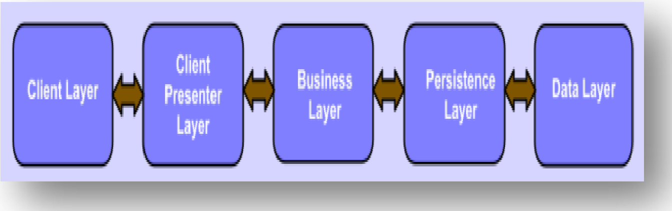

Fig. 1 N-tier architecture

B. *Benefits of N-Tier Architecture*

1) *Scalable:* This is due to its capability of deployment of multiple tiers and the tier decoupling it brought. For example, with the help of database clustering data tier can be scaled up without affecting other tiers.

2) *Better fault tolerance ability:* The N-Tier architecture has an ability of fault tolerance. For example, for load balance purpose, databases can be clustered without affecting the other layers.

3) *Independent tier upgrading and changing without affecting other tiers:* Interface-dependency implementation can decouples all layers very well in the object-oriented world, so that, each layer can change individually without affecting the other layers too much.

4) *Friendly and efficient for development:* The decoupled layers are very software development friendly and efficient. Each layer can be assigned to a team individually, who experts in the specific functional area; an expert team can handle the relevant functional area better and more efficiently.

5) *Friendly for maintenance:* The N-Tier architecture do the grouping of different things together according to the functionality and then makes things easily understandable, clear and manageable.

6) *Friendly for new feature addition:* N-Tier architecture has the capability to add new features to the system without affecting it due to the logical grouping of components.

7) *Better reusability:* Due to the loose couplings among layers, reusability can be done well. In general ways, loosely-coupled component groups implemented, so they can be reused by other applications.

C. Disadvantages of N-Tier Architecture

1) Since the tiers are physically separated, they must communicate across the machine boundaries, process boundaries. This results in high communications overhead.
2) Software installation and up gradation costs and other administration costs are high.
3) It's complicated to design and model.
4) If the network bandwidth and hardware aren't good enough, the performance of an application may be slow [13]**.**

D. Applications of N-Tier Architecture

It plays a major role in intranet and internet services, distributed computing, transaction processing monitors and other growing software technologies.

N-Tier provides a wide range of advantages to the companies longing for reliable and flexible solution to the complex and constantly changing problems. It also provides the tools to solve some of the challenges faced by IT professionals.

IV. RELATED WORK

In literature reviewed, several researchers have shown their interest in evaluating and presenting performance of various encryption algorithms. Numbers of conclusions have been made with regard to the performance of encryption algorithm in terms of encryption and decryption time, throughput.

Sukhjinder Singh et al [1], their work showed the implementation of NTRU algorithm on Cloud network with an android platform and comparison between NTRU, RSA and DES algorithms based on three parameters: encryption time, decryption time and throughput. They concluded that NTRU algorithm is more secure and faster than other algorithms. It improved the security level, speed and provided reliable message with respect to key generation, encryption and decryption at the receiver end.

Parsi Kalpana et al [4], provides a method to provide the security to the cloud data by implementing the RSA (Rivest, Shamir and Adleman) algorithm. This paper also focuses on the security issues arise in cloud computing like Confidentiality, location and relocation, integrity etc.

Subedari Mithila et al [5], describes the security control process by describing the security controls like technical, operational and management as well as security control families. Their research provides a list of required technical controls in order to match security requirements of any information system given the confidentiality impact level of the information system.

Yashpal Mote et al [6], addressed about the Authentication, Confidentiality and Integrity in SMS (Short Message Services). The transfer of the SMS over the network is insecure, so, it is important to secure the SMS with the help of encryption algorithm. They have used the two parameters: its ability to secure the protected data against attacks by hackers and its speed and efficiency, to show the comparison between encryption algorithms to evaluate the algorithm's speed. Their result showed the superiority of the NTRU algorithm in terms of the processing time over the other algorithms.

Ranjeet Ranjan et al [7], gives the brief description of NTRU cryptosystem, its analysis and some improvement in it for the network security. Their research showed that improved NTRU works better than existing NTRU because it encrypts and decrypts the large files quickly.

Leena et al [2], proposed a security framework for centralized database security in cloud by combining RSA and TORDES algorithms. TORDES is symmetric key algorithm which is used for two factor authentication process. RSA is used to enhance the authentication process by integrating the digital fingerprint mechanism.

V. PROPOSED FRAMEWORK

A. Objectives

The first objective of proposed work is to study the various encryption/decryption algorithms either they are symmetric or asymmetric. Symmetric key algorithms are those algorithms which use the same key for the encryption and decryption of data but in case of asymmetric key algorithms, the key used for encryption of data is not same with the key used for decryption of data. The second objective is to implement the NTRU algorithm on cloud database system and third one is to enhance the security of the application which has 'n' number of tiers. The last objective is to analyse the results of proposed work.

B. Outline of Algorithm

NTRU is an open source and patented public-key cryptosystem which uses lattice-based cryptography for encryption and decryption of data. This algorithm uses two keys: public key and private key. Public key is used for the encryption or to verify the digital signature but private key is used for decryption or to create digital signature. It is based on polynomial arithmetic, therefore it provides very fast computation for the encryption and decryption of the message. NTRU has less complexity i.e. $O(N^2)$ [7, 8]. In this, operations are based on objects in a polynomial ring:

$$R = Z [X] / (X^N - 1)$$

The polynomials, present in the ring have integer coefficients and degree N – 1:

$$a = a_0 + a_1X + a_2X^2 + ….. + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$$

Actually the NTRU is a parameterised family of cryptosystems; in which each system is defined by three parameters (N, p, q), which represents the maximum degree N-1 for all of the polynomials in the ring R, small and large modulus respectively, where it is assumed that N is prime, and p and q are coprime. Suppose f, g, r, e, and a are all ring polynomials.

1) Key creation: Assume Bob creates h as a public key by selecting elements f: g ε R, calculating the mod q inverse f_q^{-1} of f, and setting:

$$h \equiv f_q^{-1} * g \text{ (mod q)}$$

The private key of Bob is the element f. Bob also pre-calculates and stores the mod p inverse f_q^{-1} of f.

2) Encryption: For encryption of a plaintext message m ε R using h as the public key, Alice chooses a random element r ε R and creates the ciphertext:

$$e \equiv r * h+ m \text{ (mod q)}$$

3*) Decryption:* For decryption of the ciphertext e using the f as a private key, Bob first computes:

$$a \equiv f * e \text{ (mod q)}$$

Bob then selects a ε R to satisfy this congruence and to lie in a certain pre-specified subset of R. He next does the mod p computation $f_q^{-1} * a$ (mod p) and the value he calculates is equal to m modulo p [11].

The main characteristics of NTRU algorithm are low computational and memory requirements for providing a high level security. But this algorithm faces the difficulty during the factorisation of the polynomials into two different polynomials having very less coefficients [12]. NTRU is a widely usable, well-accomplished and promising cryptosystem.

VI. RESEARCH METHODOLOGY

The research methodology is divided into 5 steps as shown in Fig. 2 to achieve our desired goal:

Step 1: In this phase, we will create a cloud database, for the job portal application which has 'n' number of tiers, which will be queried.

Step 2: This phase includes the design of user interface for the Admin panel, Job Seeker and Job Recruiter. The user interface should be easily understandable by the user, so that he/ she can interact with it easily.

Step 3: This phase will include the encryption of data which is uploaded by the job seeker and recruiter. The encryption is done by NTRU public key algorithm.

Step 4: In this phase, if any user downloads or queried some data from database then data is provided to the user after decryption. For decryption same NTRU algorithm is used.

Step 5: Final result will be validated. The final results are analyzed and provide the conclusion on the basis of results obtained.

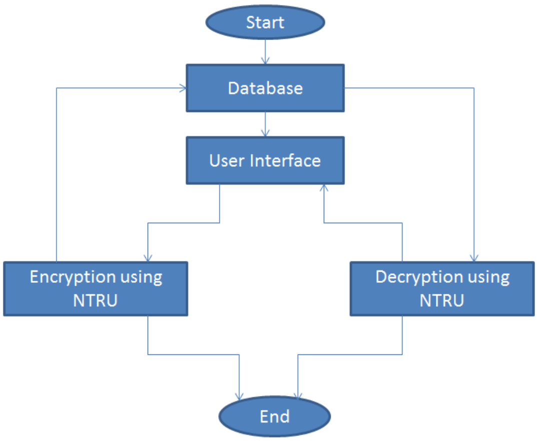

Fig. 2 Research Methodology of our Proposed Model

VII. CONCLUSION

In this paper, the study of N-tier architecture, cloud computing and its security issues etc. is done. Also the study of NTRU algorithm is done and concludes that it is a best and fast cryptosystem for providing the security. This paper proposed the methodology for the security of the N-Tier architecture, in which NTRU algorithm can be used for the encryption and decryption of data.

ACKNOWLEDGMENT

I express my sincere gratitude to my guide Er. Charanjit Singh, for his valuable guidance and advice. Also I would like to thanks all the faculty members and colleagues for their continuous support and encouragement and a special acknowledgement to the authors of various research papers and books which help me a lot.

REFERENCES

[1] Sukhjinder Singh and Mr.Sachin Majithia, "*Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA* ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013, pp-100-104.

[2] Leena and Miss A.Kakoli rao, "*Centralized Database Security in Cloud*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2012, pp-544-549.

[3] Dr.A.Padmapriya and P.Subhasri, "*Cloud Computing: Security Challenges & Encryption Practices*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013, pp-255-259.

[4] Parsi Kalpana and Sudha Singaraju, *"Data Security in Cloud Computing using RSA Algorithm",* International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012, pp-143-146.

[5] Subedari Mithila and P. Pradeep Kumar, "*Data Security through Confidentiality in CloudComputing Environment*" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, pp- 1836-1840.

[6] Yashpal Mote, Paritosh Nehete and Shekhar Gaikwad, "*Superior Security Data Encryption Algorithm(NTRU)*" An International Journal of Engineering Sciences ISSN: 2229-6913 Issue July 2012, Vol. 6, pp-171-181.

[7] Ranjeet Ranjan, Dr. A. S. Baghel and Sushil Kumar, "*Improvement of NTRU Cryptosystem*" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 9, September 2012, pp-79-84.

[8] http://en.wikipedia.org/wiki/NTRU.

[9] http://www.codeproject.com/Articles/430014/N-Tier-Architecture-and-Tips#Tier%20And%20Process%20Relationship.

[10] Amandeep Kaur Gill and Charanjit Singh, "*Survey on Encryption Algorithms to Overcome Security Issues in Cloud Computing*", International Journal of Advanced and Innovative Research (2278-7844) / # 475 / Volume 3 Issue 4, 2014, pp- 475-480.

[11] Fei Hu, Kyle Wilhelm, Michael Schab, Marcin Lukowiak, Stanislaw Radziszowski and Yang Xiao, "*NTRU-based sensor network security: a low-power hardware implementation perspective*" Security and Communication Networks Copyright # 2008 John Wiley & Sons, Ltd.

[12] https://www.cdc.informatik.tu-darmstadt.de/reports/reports/Nikolay_ Vizev.bachelor.pdf.

[13] http://matifnadeem.blogspot.in/2013/03/n-tier-architecture.html.