ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Grid computing based RSA security in Telemedicine Centre using Computer Communication Network

S.Saravanan[1], V.Saranya[2], J.Suganthi[3], B.Abinaya[4], A. Anbarasi[5], D.Vinoth[6]

Assistant Professor(SL.G), CSE Dept, Rajiv Gandhi College of Engineering and Technology, Puducherry, India [1,5,6]

M.Tech Student, CSE Dept, Rajiv Gandhi College of Engineering and Technology, Puducherry, India [2,3,4]

Abstract: HTTP is the communication protocol between the PCs and the canter of telemedicine server. Even if some form of encryption is used in transit, the medical data usually reside in an unencrypted format on the enrolled PC. This limits the nature of the problems that can be attempted over the public internet to those in which compromise of the data is not a pressing issue. Grid computing most simply stated is distributed computing taken to the emerging standardization for the flexible, secure coordinated resources sharing among dynamic collections of Telemedicine resources. Grid computing based RSA Security in Telemedicine canter is one of the most important issues facing encryption to need security the big data of patient details . In this paper explained the computing grid is Reliability and RSA Security in Grid computing support complexity management of Telemedicine center using computer communication network. The architecture of the RSA-Grid is presented and a prototype system has been built for further development of Grid-based telemedicine canter services for Emergency treatment with reliability and security assessment based on probabilistic techniques, which require high performance computing for big data of patient details.

Keywords: RSA Security, Grid Computing, Computer Communication, Telemedicine.

I. INTRODUCTION OF GRID COMPUTING IN TELEMEDICINE CENTER SERVICE

The aim of this research is to analysis for maintaining security to complexity of patient's documents in the Telemedicine resources of centre. RSA security is warranted to complexity of telemedicine service environment for data security. Grid computing technology can compute and given solution for maintaining the increasing Telemedicine node service environment. Grid computing can maintain the management of telemedicine service, transmission of data through internet, load balance, delivery patient big data to Telemedicine networks and monitoring Telemedicine resource as shown in Figure1.

The security need in complexity of Telemedicine service. RSA security is supported to security of telemedicine service Grid to manage the resources, communications authorization and authentications, system monitoring and control. Grid computing is an emerging technology for providing the high performance computing capabilities and collaboration mechanism for the collaborated and complex problems while using the existing telemedicine canter service resources.

Grid computing in turn provides highly scalable, highly secure and extremely high performance mechanisms for resource sharing of infinite number of geographically distributed groups.

II. TELEMEDICINE RESOURCE SHARING

Figure 1 represent the Telemedicine resource sharing, A computational grid is a hardware and software infrastructure that provides,

- Resource Consistent and inexpensive access to high end computational capabilities.
- Grid computing focus on coordinated Telemedicine service sharing and problem solving in multi connection of telemedicine resource connection

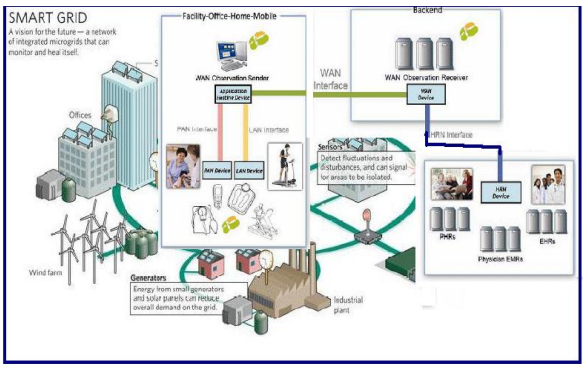

Fig 1 Telemedicine resource sharing

A. JINI Technology and JINI system

Globus Toolkit Version 4.0 (GT4) as a stable, enterprise ready set of services and software libraries incorporating the latest web services standards, with new security and authorization features

III. GRID SECURITY ARCHITECTURE AND GRID SERVICE LAYERS IN TELEMEDICINE CENTRE

The Architecture of Grid security and Grid service layers is proposed as shown in Figure 2

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

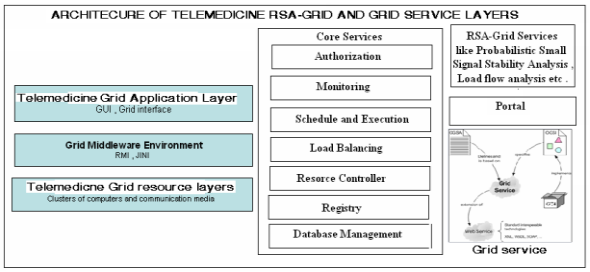

Fig 2 Grid Security Architecture and Grid service layers of Telemedicine centre.

A. Telemedicine Grid Application Layer

The application layer defines protocols and services that targeted towards a specific telemedicine application. This layer is currently the least defined in the Grid architecture. The core services are used to manage the Telemedicine resources using computer communications through Internet with authorization and authentications, system monitoring , patient remote monitoring and control accessed securely based on a set of rules. Grid services layer as shown in Fig 2.

B. RSA Security in Big data of Telemedicine centre

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977 The basic technique was first discovered in 1973 by Clifford Cocks (part of the British GCHQ). The RSA algorithm can be used for both public key encryption and digital signatures.

C. Key Generation Algorithm

- Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
- Compute n = pq and (φ) phi = (p-1)(q-1).
- Choose an int e, 1 < e < phi, such that gcd(e, phi) = 1.
- Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi).
- The public key is (n, e) and the private key is (n,d). The values of p, q, and phi should also be kept secret.
- n is known as the modulus.
- e is known as the public exponent or encryption exponent.
- d is known as the secret exponent or decryption exponent.

Encryption

- Sender A does the following:-
- Obtains the recipient B's public key (n, e).
- Represents the plaintext message as a positive integer m .
- Computes the cipher text c = m^e mod n.
- Sends the cipher text c to B.

Decryption

Recipient B does the following:-

- Uses his private key (n, d) to compute
- m = c^d mod n.
- Extracts the plaintext from the integer representative m.

D. Authentication and Authorization

Authorization: This telemedicine service will provide the security service for the authentication and authorization of the grid users to provide the access to the resources according to policies. WS Authorization and Authentication Service Interface of Globus toolkit are used in telemedicine service. RSA Security Cryptography is used in support of mechanism for authentication Communication between the patients of doctor to Specialist doctor principals. A principal who decrypts a message successfully using a particular keys can assumes that the message is authentic if it contains a connect check sum or some expected value. They can infer that the sender of the message processed from doctor to Specialist doctor in telemedicine Grid area of the corresponding encryption key and hence deduce the identity of the sender of telemedicine resource area if the key is known only to the two parties of Telemedicine service Grid Areas. Thus if keys are held in private a successful decryption. Authenticates the decrypted message as coming from a particular sender Telemedicine system Area. Authorization to access a resource is connected by polices enforced in the resource provider side of the Grid. The most prominent once are role based authorization , rule based authorization, and identity–based authorization. The selection of these mechanism is entirely based on the service requirement , hosting platform capabilities and the application domain of Grid to Grid Telemedicine system. The RSA algorithm can be used for both public key encryption and digital signatures to Telemedicne system.

$$Z = E\,KUb\,[\,EKRa(X)] \quad \ldots\ldots\ldots \quad 1$$

$$X = D\,KUa\,[DKRb(Z)] \quad \ldots\ldots\ldots\ldots \quad 2$$

In this case Encrypting a Message using the Sender's Telemedicine area Private Key , this provides the digital Signature , next we encrypt again using the receiver's Telemedicine hospital area Public Key from equation 1. The Final Cipher text can be decrypted only by the intended receiver of hospital area ,who alone has the matching private key using equation 2. Thus confidentiality is provided to Telemedicine system as shown in Figure 3.

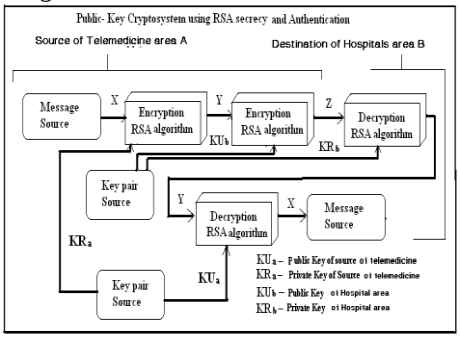

Fig 3 Public- Key Cryptosystem using RSA Security algorithm and Authentication

DOI 10.17148/IJARCCE.2015.4513

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Enter the destination IP address for send Medical data of Plane text convert to Cipert text with keys Enter the system details as shown in Figure 4

Fig 4. Enter the system Details

The execution of client side or sender side as shown in Figure 5

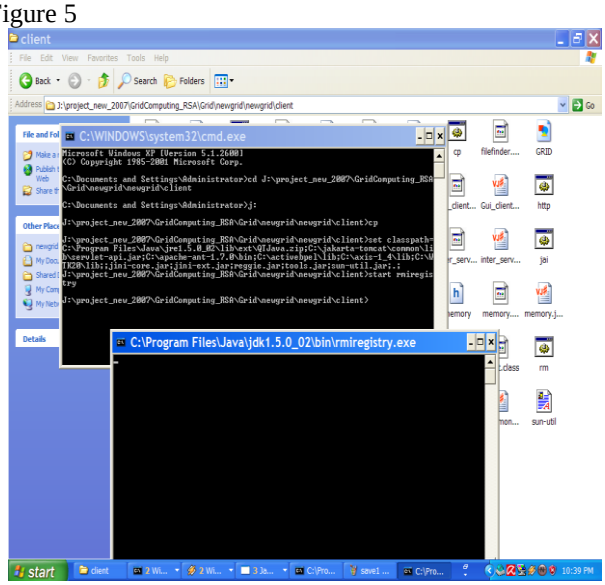

Fig 5. Execution of client

The execution the system details monitoring by Grid computing as shown in Figure 6

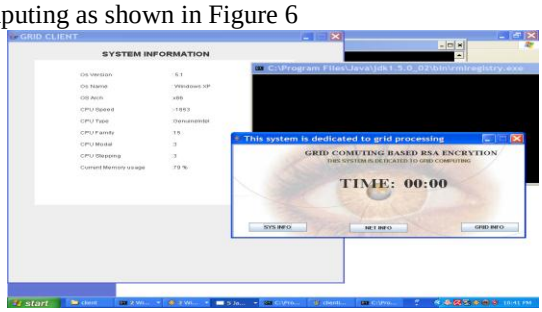

Fig 6 System information

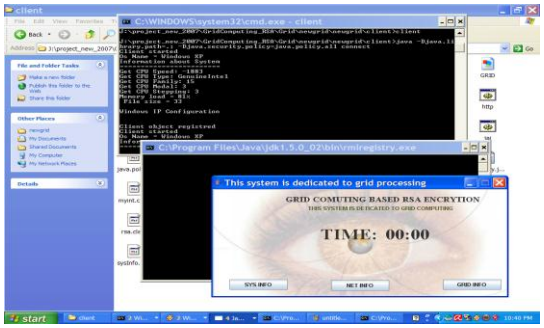

Fig 7 Display about of system details

Monitoring and display the available system details as shown in Figure 7.

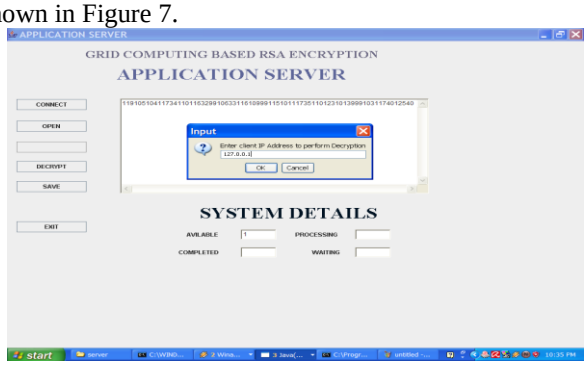

Figure 8 Enter the IP address to perform Decryption

The decryption of destination Address enter as figure 8.

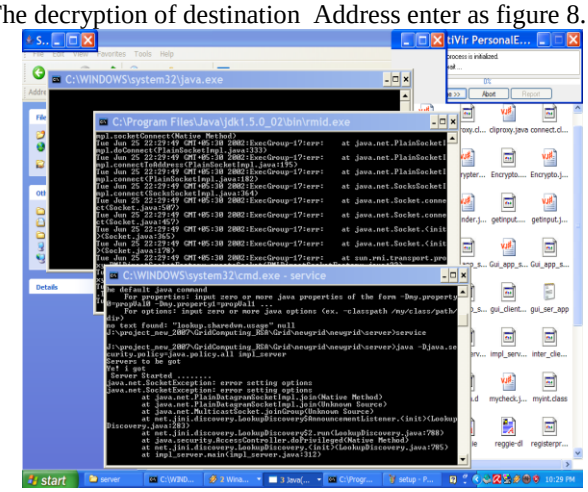

Fig 9 Execution of Server side

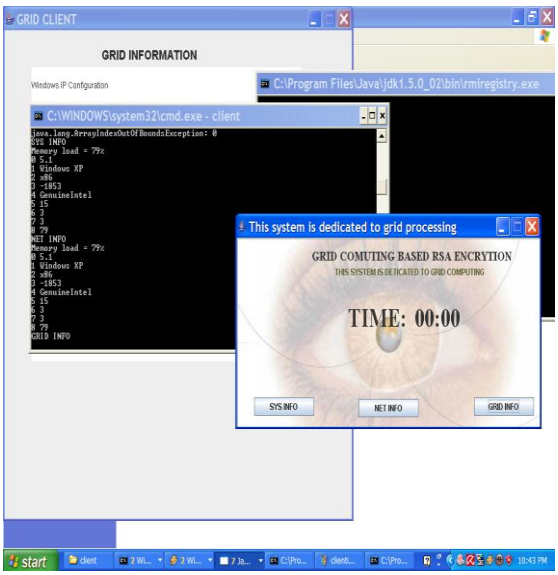

Fig 10 Display Grid information

The decryption file converted into plain text to destination of system. Collection of available systems Grid information as shown in Figure 10.

IV. CONCLUSION

RSA is a strong encryption algorithm that has stood a partial test of time. RSA implements a public-key

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

cryptosystem that allows secure communications and \digital signatures", and its security rests in part on the difficulty of factoring large numbers. Grid computing presents a number of security challenges that are met by the Globus Toolkit's Grid Security Infrastructure (GSI). Version 3 of the Globus Toolkit (GT3) implements the emerging Open Grid Services Architecture; its GSI implementation (GSI3) takes advantage of this evolution to improve on the security model used in earlier versions of the toolkit. Its development provides a basis for a variety of future work.GT4 Security Infrastructure implements the existing and emerging standards which are used by the broader Web Services community of Health care service of Telemedicine.

REFERENCES

[1]. Draft smart grid cyber security strategy and requirements, NIST IR 7628, Sep. 2009 [Online].Available :http://csrc.nist.gov/ publications/ drafts/nistir-7628/draft-nistir-7628.pdf
[2]. "Public key infrastructure," Wikipedia Feb. 18, 2010 [Online]. Available: http://en.wikipedia.org /wiki/Public_ key infrastructure
[3]. Smart, Nigel (February 19, 2008). "Dr Clifford Cocks CB". Bristol University. Retrieved August 14, 2011
[4]. Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM **21**
[5]. RSA Security Releases RSA Encryption Algorithm into Public Domain at the Wayback Machine (archived June 21, 2007)

BIOGRAPHIES

Mr.S.SARAVANAN Assistant Professor (selection Grade) in computer science Department in Rajiv Gandhi college of Engineering and technology, puducherry, India. He has completed B.E(Electronics and communication) in 1998, M.S (Information technology) in 2003, M.E (computer science Engineering) in 2008, MBA(Education management)in 2010, M.Tech (Communication System) in 2012,.Ph.D pursuing from 2009. He has teaching experience from 1998 in various Department of Electronics and communication, Biomedical Engineering and Computer science Engineering.

V. SARANYA has received B.Tech (Computer Science and Engineering) from 2008 to 2012 at Rajiv Gandhi College of Engineering and Technology , MBA (HRM) from 2012 to 2014 at Pondicherry University and Pursuing M.Tech (CSE) at Rajiv Gandhi College of Engineering and Technology from 2014 to 2016. **AREAS OF INTEREST** : CLOUD COMPUTING, NETWORKING

J.SUGANTHI has received B.Tech (Computer Science and Engineering) from 2009 to 2013 at Rajiv Gandhi College of Engineering and Technology, Pursuing M.Tech(CSE) at Rajiv Gandhi College of Engineering and Technology from 2014 to 2016. **AREAS OF INTEREST** : CLOUD COMPUTING

B. ABINAYA has received B.Tech(IT) Sri Manakula Vinayagar Engineering College from 2010 to 2014, Pursuing M.Tech(CSE) at Rajiv Gandhi College of Engineering and Technology from 2014 to 2016. **AREAS OF INTEREST:** CLOUD COMPUTING .

Mrs.A. ANBARASI Asst. Professor in CSE Department at Rajiv Gandhi college of Engineering and Technology, Puducherry, India. She has received M.tech(DCS) -2008 in Pondicherry Engg college and pursuing Ph.D (computer Science) St. Peters University, avadi, Chennai, Tamil nadu, India. Area of Interest: Image Processing, Networks, Grid computing, Artificial Intelligence.

Mr. D.VINOTH is received B.Tech (I.T) in 2011 at Christ College of Engineering & Technology, Pondicherry and M.Tech(I.T) in 2013 at Anna University, Regional Centre, Coimbatore. He is working as Assistant Professor in computer science Department at Rajiv Gandhi college of Engineering and Technology, Puducherry from January 2014. He has interested in computer communication network and mobile ad hoc network.