AUTHENTICATION USING AES ALGORITHM AND SECURE COMMUNICATION BY USING NTRU ALGORITHM FOR MOBILE GRID COMPUTING

[1]Malwinder Kaur, [2] Mrs. Meenakshi Bansal
[1]M.Tech Student, [2]Assistant Professor,
Department of Computer Engineering,YCoE, Talwandi Sabo, Punjabi University, Patiala.
Email: [1]malwinderkr2@gmail.com, [2]ermeenu10@gmail.com

Abstract - Mobile Grid Computing (MGC) is the combination of Grid Computing and Mobile Networks to bring benefits for mobile users, network operators, as well as grid computing providers. Mobile Grid Computing provides new technology for solving complex and compute intensive problems in mobile environments. With the increasing use of technology in all walks of life - be it the banking system, education, or other services related to industry and security - transferring of information from one place to another without compromising its security has become a necessity. Fast access of precise information is basic need and securely transfer confidential data from one place to another are major issues. Different cryptography techniques are used for making our data secure. In this research work, data security is enhanced by Number Theory Research Unit known as NTRU Algorithm. It is a asymmetric key algorithm. AES algorithm is used for authentication, because it is symmetric key algorithm and is very fast and easy algorithm. NTRU algorithm is used for files (documents) operations. NTRU is very secure and latest algorithm, and it is specially formed for smart-phones and tablets (Devices having scarce power). NTRU is having polynomial solving operations. For providing the security to the data transferred on the network, NTRU algorithm is seen as fast and best algorithm. This paper represent the implementation of AES algorithm for authentication and NTRU for security and focus on comparison on the basis of authentication time, key agreement scheme/ key generation time & power consumption.

Keywords - Grid computing, Mobile grid computing (MGC), Client server architecture, AES (Advanced Encryption Standard) algorithm, NTRU (Number Theory Research Unit) algorithm, Authentication, Key generation, Power Consumption. Encryption, Decryption etc.

I. INTRODUCTION

A. Grid Computing

A Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains with intent of providing users easy access to these resources.

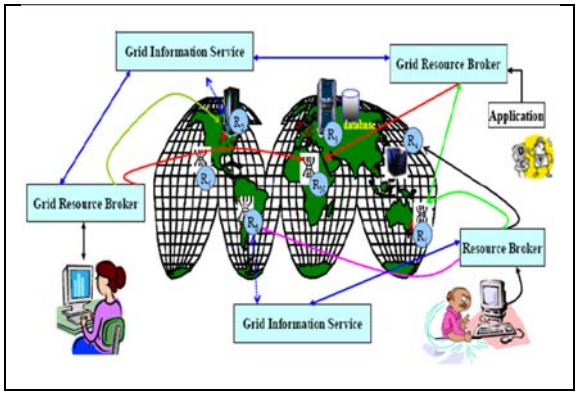

Figure 1 A world-wide Grid computing environment [12].

The major aim is to study about data grid security issues and provide solution to guard data or information in Grid Services that are appeared while operating in data storage systems and we present a cryptographic & fragment based scheme to accomplish the server protection requirements associated with a standard Data Grid environments.

The Data Grid is kind of distributed structure in which mutual assets (CPU or storage space) are offered. These surroundings likely to present the productive assets not only for processor - based jobs, but as well for the programs which need major sum of primary memory, physical memory space and network performance. A high-level view of activities involved within a seamless, integrated computational and collaborative Grid environment is shown in Figure 1 [12].

B. Mobile Grid Computing(MGC)

Mobile Grid computing extends traditional Grid computing paradigm to include a diverse collection of mobile devices that communicate using radio frequency, infrared, optical and the other wireless mechanisms. The prominent feature of mobile grid computing is collaboration of multiple entities to perform collaborative tasks using mobile devices that rely on two fundamental functions: communication and resource sharing. The fundamental function is to enrich one another and provide new solutions that solve many of limitations and problems found in different technologies, such as reduced CPU performance, limited secondary storage, heightened battery consumption sensitivity, and unreliable low band width communication.

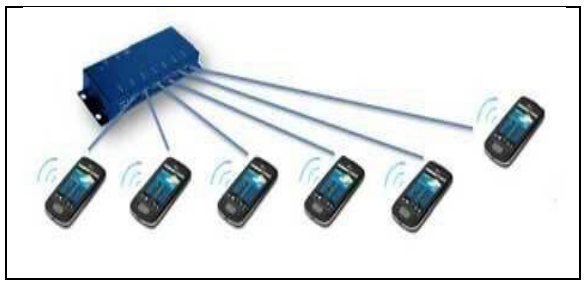

Figure 2 Mobile grid computing[37].

In Figure 2 shows six low-end Android phones which are connected to create a mini-grid. Security is a very important factor in mobile grid Computing and is also difficult to achieve owing to open nature of wireless networks and heterogeneous and distributed environments. Since Internet is not security oriented by design, there exist various threats, in the particular, malicious internal and external users. Securing communication and fine tuning controlling access to shared resources are the important issues for mobile grid services.

The main factors that hinder the growth of this paradigm as compared to the grid computing paradigm are the issues related to mobility and the constraints of mobile computing, mobile devices are poor in available resources as compare to wired systems, mobile devices are more prone to security breaches, mobile connectivity is highly variable in performance and reliability, mobile devices relay on a finite energy source.

C. Client server computing in mobile environment

Advances in wireless networking technology and portable information appliances have engendered a new paradigm of computing, called mobile computing, in which users who carry portable devices have access to information services through a shared infrastructure, regardless of their physical location or movement behavior. Mobile computing is distinguished from classical, fixed-connection computing due to [19]:

(1) The mobility of nomadic users and their computers

(2) The mobile resource constraints such as limited wireless bandwidth and limited battery life.

Paradigms of Mobile Client-Server Computing

In this section, we briefly examine the impacts of mobility on information services and applications, and the new paradigms of client-server computing needed to deal with these impacts. A categorization of these computing paradigms is given below. This examination should facilitate our analysis and review of the various proposed techniques for mobile information access. Existing research on mobile client server computing can be categorized into the following three paradigms:

(1)Mobile-aware Adaptation: The paradigm of mobile-aware adaptation covers various strategies and techniques in how systems and applications respond to the environmental changes and the resource requirements. It also suggests the necessary system services that could be utilized by mobile-aware applications.

(2)Extended Client-Server Model: The extended client-server model facilitates mobile client-server information access. One distinguishing feature is the dynamic partitioning of client-server functionality and responsibilities. The extended client-server model provides a way to support the adaptation of mobile systems and applications. The paradigm of the extended client-server model includes various client-server computing architectures that enable the functional partitioning of applications between clients and servers.

Extended Client Server model is of following three types:

i. Thin client architecture
ii. Full client architecture
iii. Flexible client architecture

(3)Mobile Data Access: Mobile data access addresses issues such as how server data can be delivered to client hosts, how data over wireless and mobile networks is structured, and how the consistency of client cache is ensured effectively. The adaptive strategies for mobile data access depend largely on the type of communication links, the connectivity of mobile hosts, and the consistency requirements of applications. In our view, mobile data access provides another way to characterize the impact of mobile computing constraints on information access.

This paper is organized as follows: Section 2 reviews the research related to this research work. Section 3 describes the algorithms used for this research work like AES is used for authentication purpose and NTRU is used for document encryption & decryption means secure communication. Section 4 gives the brief idea about proposed work. Section 5 describes in detail the research methodology. Section 6 shows results which are concluded by comparing the NTRU & AES algorithms with different techniques that NTRU is best for secure communication and AES is fastest for authentication purpose. Section 7 describes the conclusions drawn.

II. RELATED WORK

In literature review goes beyond the search for information and includes the identification and articulation of relationship between the literature and our field of research.

Begam and Mohamed [4], their work showed the focus to provide security and efficient power management. In this a framework of dynamic secure routing protocol called select successive hop routing(SSHR) algorithm using Abstract monitoring objects.(AMO) and Secure service certificate(SSC). It includes: Authentication of Mobile nodes, Security flow between Mobile devices and Saving battery power.

Gill *et al.* [11], described the study of N-Tier architecture, grid computing and its security issues.

By the study of NTRU it is concluded that it is fast and best for providing security.

Gulmeher and Waheed [12], discussed that grid computing is a modern concept and it not just speedup computing and cut costs but causes a paradigm shift in computing. It adds security needs of both resource consumer and resource provider.

Ranjan *et al.* [35] discussed that NTRU cryptosystem can be used in a range of application which involves security in a network. NTRU is depending upon the algebraic structures of certain polynomial rings. The NTRU Encrypt is a public-key cryptosystem which is based on the shortest vector problem. Its main characteristics are low memory and computational requirements as providing a high security level. It is very well-organized public-key cryptosystem based on polynomial arithmetic. We introduce the description of NTRU cryptosystem, its analysis and some improvement for the security.

Singh and Majithia [36], discussed the various algorithms used to secure data send by mobile phone using an android platform on network. It concluded that NTRU is faster and provide stronger security level than other traditional algorithms like DES(Data Encryption Standard) and RSA(Rivest-Shamir-Adleman).

III. OUTLINE OF ALGORITHMS

A. NTRU (Number Theory Research Unit) Algorithm

NTRU cryptosystem is a relatively new Public Key Cryptosystem. Public Key Cryptography or Asymmetric Cryptography is used in areas of digital signatures and key exchange. RSA is an acclaimed Public Key cryptosystem that is in use since 1977. However, it is very slow in comparison with Symmetric Cryptography systems in processing bulk data encryption and decryption. In contrast, NTRU runs much faster on large data systems than RSA and has become a very popular algorithm today in terms of data encryption and decryption. The key generation process in NTRU is much faster than that in RSA and this process is one of the most important processes in Public Key Cryptography.

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 log(n)). The operations are based on objects that are in a polynomial ring[11]:

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

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

$a = \alpha 0 + \alpha 1X + \alpha 2X2 + ….. + \alpha N\text{-}2XN\text{-}2 + \alpha N\text{-}1XN\text{-}1$

Actually the NTRU is a parameterized 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, N is assumed as prime, where p and q are co-prime. Suppose f, g, r, e, and a are all ring polynomials.

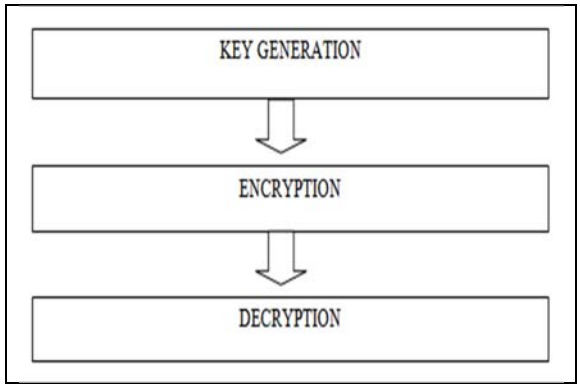

Figure 3 NTRU algorithm operations.

i. Key Generation: NTRU involves a public key and a private key. The public key is used for encrypting message and can be known to everyone. Messages encrypted with this key can only be decrypted in a reasonable amount of time using the private key.

ii. 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:

$e \equiv r * h+ m \pmod q$

iii. Decryption: For decryption of the ciphertext e using the f as a private key, Bob firstly computes the value:

$a \equiv f * e \pmod q$

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 $fq -1 * a \pmod p$ and the value he calculates is equal to m modulo p.

The main characteristics of NTRU algorithm are low computational and memory requirements for providing a high level security. In this algorithm the difficulty is faced during the factorization of the polynomials into two different polynomials having very less coefficients. NTRU is a widely usable, well-accomplished and promising cryptosystem. NTRU is better than all other algorithms in throughput and power consumption.

Advantages of NTRU algorithm

- The key generation process in NTRU is much faster than that in RSA and this process is one of the most important processes in Public Key Cryptography.
- Encryption and decryption of data that uses NTRU is better than all other algorithms in throughput and power consumption.
- NTRU is a widely usable, well accomplished and promising cryptosystem.
- NTRU is having polynomial solving concept, so it is hard to break.
- NTRU is the latest in the line of Public Key Cryptographic Systems.

NTRU algorithm is next to RSA and ECC algorithms. NTRU is ideally suited for applications where high performance, high security and low power consumption are required. NTRU has its unprecedented performance advantages open up new options for security.

Table 1 Distinction between NTRU, DES and RSA Algorithms[36].

Features	NTRU	DES	RSA
Approach	A-symmetric	Symmetric	A-symmetric
Encryption Time	Low	Moderate	High
Decryption Time	Low	Moderate	High
Throughput	High	Moderate	Low
Power Consumption	Low	Moderate	High
Confidential	High	Moderate	Low

Table 1 describes that NTRU is better than DES and RSA algorithms.

B. AES (Advanced Encryption Standard) Algorithm

In 1997, NIST initiated a very public, process to develop a new secure cryptosystem for U.S. government applications. The result of the Advanced Encryption Standard, became official successor to DES in December 2001. The AES uses an SKC scheme called Rijndael, block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. Algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits & blocks of lengthof 128, 192 or 256 bits.

(i) Do the following one-time initialization process:
   (a) Expand the 16-byte key to get actual key block to be used.
   (b) Do the one time initialization of 16-byte plain text block.
   (c) XOR the state with the key block.

(ii) For each round, do the following:

   (a) Apply S-box to each of plain text bytes.
   (b) Rotate row k of plain text block by k bytes.
   (c) Perform a mix columns operation.
   (d) XOR the state with the key block.

we use AES for user authentication purpose. According to designers, the main features of AES are as follows:

- Symmetric and parallel structure – It gives the implementers a lot of flexibility.
- It is also stands up well against cryptanalysis attacks.
- Adapted to modern processors – The algorithm works well with modern processors (Pentium, RISC, parallel).
- Suited to smart cards – The algorithm can work well with smart cards.

IV. PROPOSED WORK

In this research work AES algorithm is implemented for authentication purpose and NTRU algorithm is used for file (document) encryption in mobile grid. There is facility to block unauthorized user, forget password and secret no. is sent to personal email account along with file encryption, upload, download and decryption.

First objective of proposed work is to make the system secure so that only authorized user can login in the grid, if any unauthorized user try to access our private grid we can easily track and permanently block his/her IP and even MAC address of device from where he/she is try to access our private grid. Second is to make the file sharing in private grid totally secure using NTRU algorithm, and which is hard to decrypt and to make the packets travel securely in network using NTRU, so that any hacker cannot intercept or decrypt any packet.

V. WORKING METHODOLOGY

The research methodology is as follows:

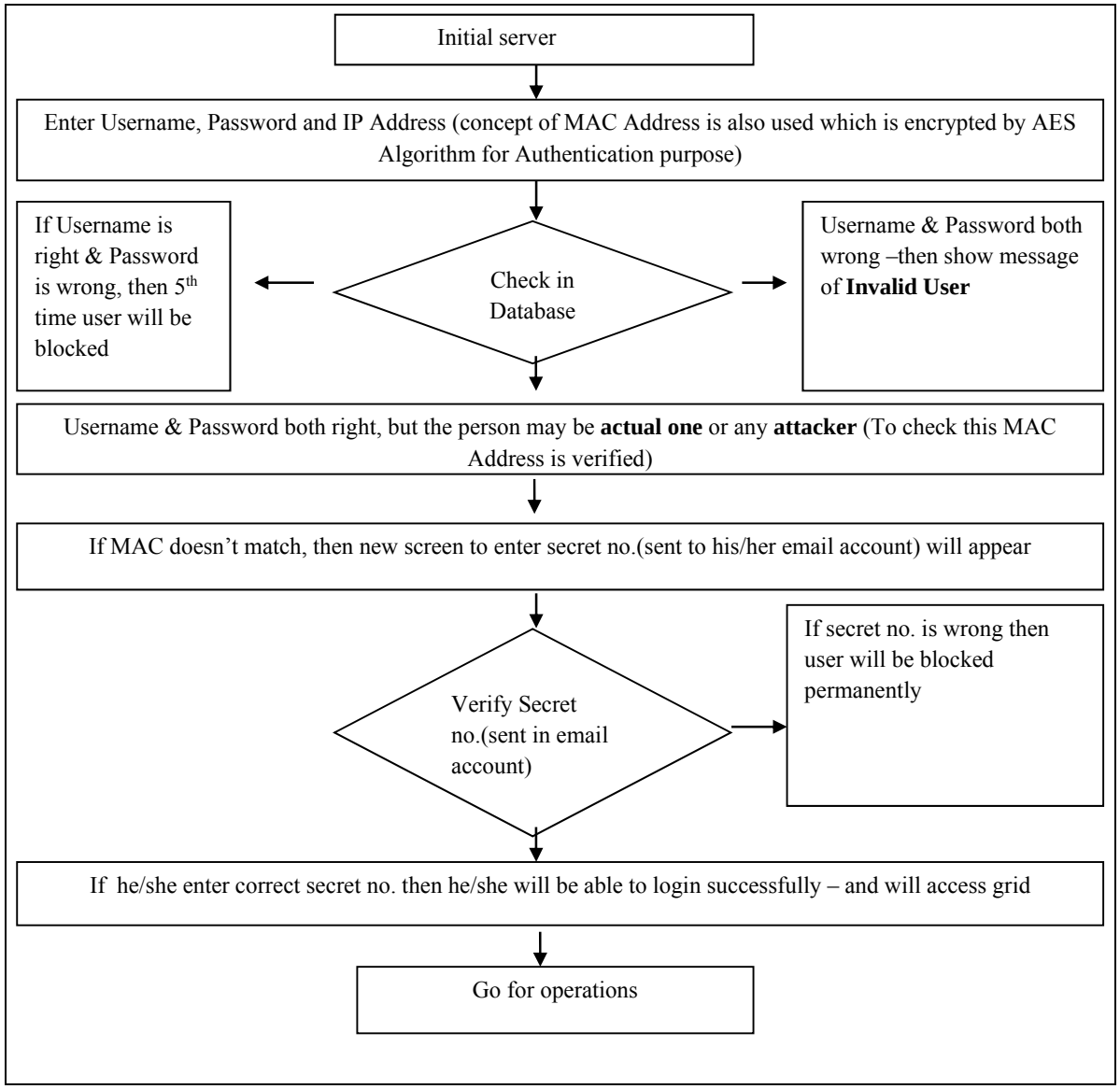

Figure 4 The flowchart for complete process.

Figure 4 shows the complete working for proposed system. Which describes that after registration if any user is trying to login and if password is wrong or MAC address is wrong then what will happen and Figure 5 describe the possible operations for proposed system, these operations can be applied on document (files) for their security.

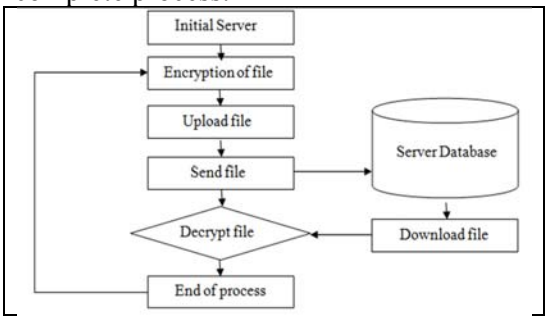

Figure 5 Flowchart of operations on file (document).

VI. EXPERIMENTAL RESULTS AND DISCUSION

This research work is to measure the Authentication time which is on the basis of AES algorithm and Key generation time & Power consumption on the basis of NTRU algorithm.

A. Authentication time

Here DRCP-AB is Dynamic Re-encrypted Ciphertext Policy - Attribute Based encryption. The graph in Figure 6 shows the authentication time taken by AES algorithm and DRCP-AB approach, here time is taken in milliseconds. The relation shown is number of user with respect to time. AES is a symmetric key algorithm it is fast and simpler to implement. The value for authentication in DRCP-AB is 500 milliseconds per user and in AES this value is 470 when we tested. This value varies accordingly but always results in less value for AES than DRCP-AB. This factor is concluded after login process. We get positive results for AES algorithm. Table 2 shows the observation results in tabular form with reference to the graph of Figure 6.

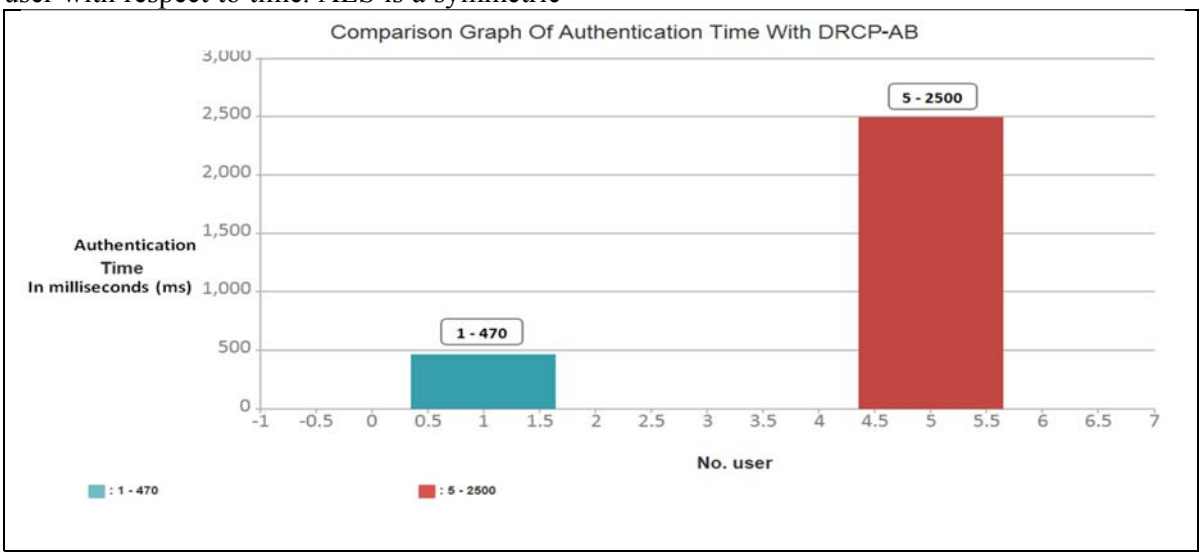

Figure 6 Graph for authentication time after login for AES and DRCP-AB.

Table 2 Comparison for Authentication time.

Algorithm	AES	DRCP-AB
No. of user	1	5
Time (For authentication)	470 ms	2500 ms

B. Key agreement scheme/ Key generation time

Key generation time for NTRU and GPC-AKA approach are compared. NTRU is having key generation as its strong feature. So when values for key generation time are calculated they come out to be very less.

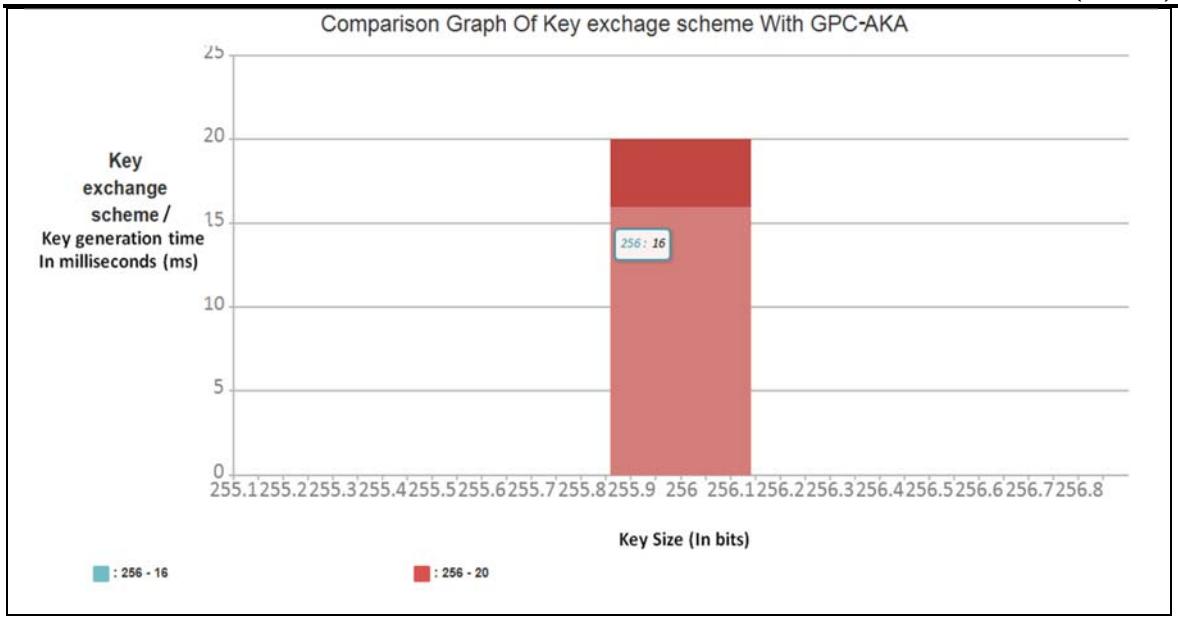

Figure 7 Key generation for NTRU algorithm.

Figure 7 shows the key generation time/ key exchange scheme for NTRU algorithm and Figure 8 shows for GPC-AKA. The graph is constructed with key size with respect to time. Both are overlapping because both are compared for key size 256 bits. This factor is concluded after encryption and decryption. Here GPC-AKA is Grid Pairing free Certificate less two party - Authenticated Key Agreement. Table 3 shows the observational results in tabular form with reference to the graphs of Figure 7 and Figure 8.

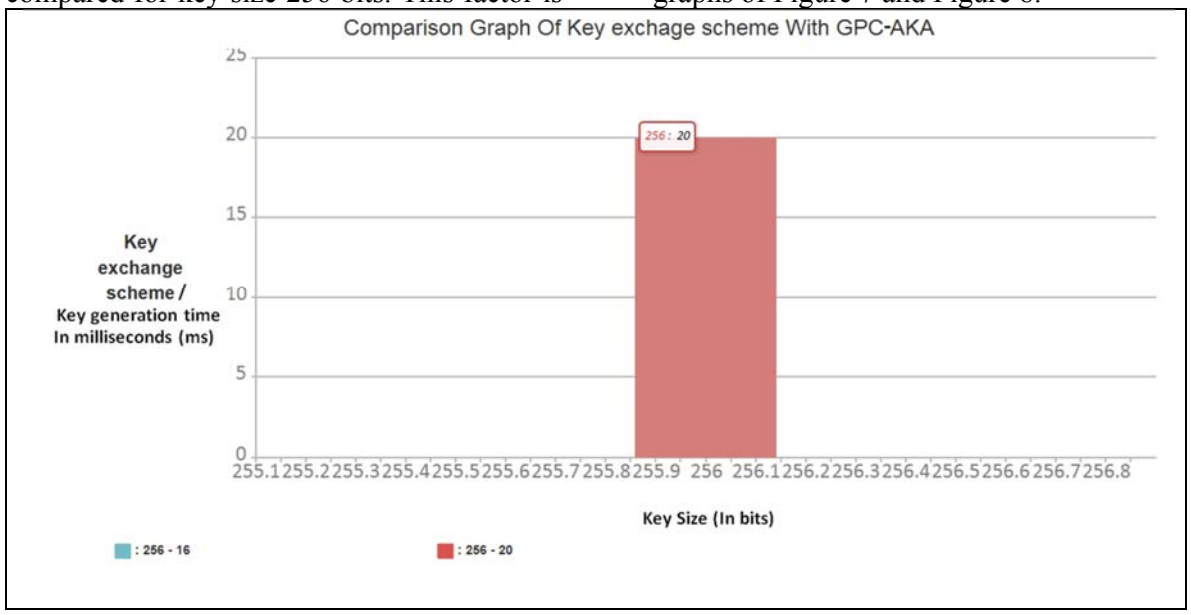

Figure 8 Key generation for GPC-AKA.

Table 3 Comparison for Key agreement scheme/ Key generation time.

Algorithm	NTRU	GPC-AKA
Key size	256 bits	256 bits
Time (For key generation)	16 ms	20 ms

C. Power consumption

Power consumption for NTRU algorithm and AMI are compared. Here graph is constructed with days (time) vs unit battery consumption. Low Power consumption of NTRU is its strong point, because it is specially formed algorithm for smart phones (devices having scarce battery power). As shown in Figure 9. This factor is concluded after uploading and downloading files. Here AMI is Advanced Metering Infrastructure.

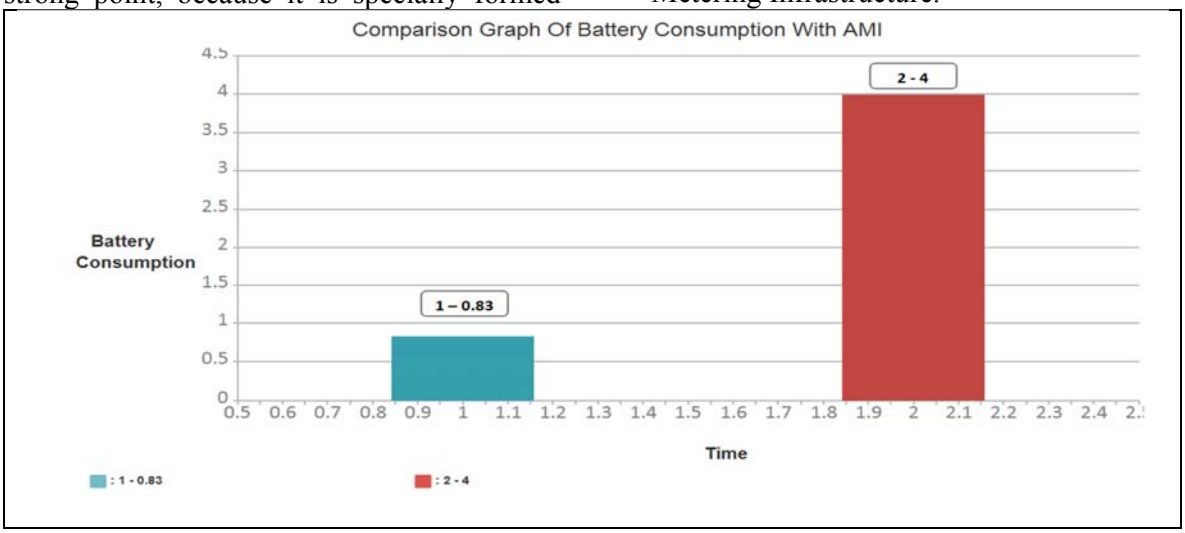

Figure 9 Power consumption for NTRU and AMI.

Table 4 Comparison for Battery consumption.

Algorithm	NTRU	AMI
Time	1	2
Consumption units	0.83	4

Here Table 4 shows the observational results in tabular form with reference to graph of Figure 9.

VII. CONCLUSION

Data has become more important as the methods which are used to ensure security not only need to be strong and efficient but should be easy to implement and execute. Grid computing is a modern concept that not just speeds up computing and cut costs. However, several challenges still weigh down the technology. Resolving security problems with grid computing is one such major challenge. It requires an adequate understanding of both the security issues in grid computing implementation as well as the solutions presently available to address these. The security model is used to improve security without degrading the performance of the system. Main goal of future improvement is provide more security by using more secure algorithm whose security can't be broken.

Simulation results shows that AES algorithm is best for authentication and NTRU algorithm used for security has better performance than other techniques. Since NTRU has not any known security weak points till now, it can be considered as an excellent standard encryption algorithm. The experimental results reveals that the proposed method offers better performance over previous work.

In future we can use NTRU algorithm for securing audio and video data. Because, In the area of security, research area of speech is very wide. The Android platform of smarphones is a powerful platform and is used in 80% of smartphones today. The sensors that come with the mobile devices further give a context to grid applications and opens up a new set of possibilities.

ACKNOWLEDGEMENT

I express my sincere gratitude to my guide **Mrs. Meenakshi Bansal** (Assistant Professor, GKC, Talwandi Sabo), 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] Abawajy, J.H., (2008), "An Online Credential Management Service for InterGrid Computing" *In the Proceedings of IEEE*, PP:101-106.

[2] Agarwal, A., (2014), "Performance Analysis of Cloud Based Load Balancing Techniques", *In the Proceeding of International Conference on Parallel, Distributed and Grid Computing*, pp: 49-52.

[3] AlHakami, H., (2012), "COMPARISON BETWEEN CLOUD AND GRID COMPUTING: REVIEW PAPER", *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, 2(4), PP: 1-21.

[4] Begam, P. and Mohamed, M., (2013), "ASAMO: Authentication and Secure Communication using Abstract Monitoring Objects for Mobile Grid Computing", *In the Proceeding of International Conference on Informatics and Creative Multimedia*, pp: 127-137.

[5] Bichhawat, A. and Joshi, R., (2010), "A Survey on Issues in Mobile Grid Computing", *Int. Journal of Recent Trends in Engineering and Technology*, 4(2), pp: 15-19.

[6] Buchade, A.R. and Ingle, R., (2014), "Key Management for Cloud Data Storage: Methods and Comparisons", *In the Proceeding of Fourth International Conference on Advanced Computing & Communication Technologies*, pp: 263-270.

[7] Challa, N. and Pradhan, J., (2007), "Performance Analysis of Public key Cryptographic Systems RSA and NTRU", *International Journal of Computer Science and Network Security (IJCSNS)*, 7(8), pp: 87-96.

[8] Flauzac, O.,(2010), "Grid of security: a new approach of the network security", *In the Proceeding of Third International Conference on Network and System Security,* pp: 67-72.

[9] Gama, N., (2007), "New Chosen-Ciphertext Attacks on NTRU", *International Association for Cryptologic Research*, pp: 89-106.

[10] Gangil, G. and Narvey, R., (2013), "Advanced Security Algorithm for Power Grid", *In the Proceeding of International Conference on Communication Systems and Network Technologies*, pp: 409-417.

[11] Gill, A.K. and Singh, C.**,** (2014), "lementation of NTRU Algorithm for the Security of N-Tier Architecture", *International Journal of Advanced Research in Computer Science and Software Engineering,*4(7), pp: 7631-7636.

[12] Gulmeher, R. and Waheed, M.A., (2014), " Security Analysis for Data Grid Middle wares", *International Journal of Advanced Research in Computer Science and Software Engineering,*4(5), pp: 416-422.

[13] Gupta, A. and Walia, N.K., (2014), "Cryptography Algorithms: A Review", *International Journal of Engineering Development and Research (IJERD)*, 2(2), PP: 1667-1672.

[14] Hagir, U.S.B. and Ugavel, S.S.H. (2009), "Optimized Resource Allocation in Grid Networks Using Genetic Algorithm with Error Rate Factor", *In the Proceedings of IEEE*, pp: 161-166.

[15] Hamlyn, A., (2008), "Computer Network Security Management and Authentication of Smart Grids Operations", *In the Proceedings of IEEE*, pp: 1-7.

[16] Hashemi, S. and Bardsiri, A., (2012), "Cloud Computing Vs. Grid Computimg", *ARPN Journal of System and Software*, 2(5), pp: 188-194.

[17] Hong, W., (2013), "An efficient quantum meet-in-the-middle attack against NTRU-2005",

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China, 58, pp: 3514-3518.

[18] Idrees, F. and Muttukrishnan, R., (2014), "War against Mobile Malware with Cloud Computing and Machine Learning forces", In the Proceeding of 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet), pp: 278-280.

[19] JING, J., (1999), "Client-Server Computing in Mobile Environments", *ACM Computing Surveys,* 31(2), pp: 118-157.

[20] Joseph, J., (2004), "Evolution of grid computing architecture and grid adoption models", IBM SYSTEMS JOURNAL, 43(4), PP: 624-645.

[21] Kausla, V.,(2007), "Performance Analysis of Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm" , *In the Proceedings of IEEE*, PP: 352-356.

[22] Kathrine,G.J.W.,(2011), "A Novel Security Framework for Computational Grid", *In the Proceedings of IEEE*, pp: 103-107.

[23] Kumar, A. and Qureshi, s.,(2008), "Integration of Mobile Computing with Grid Computing: A Middleware Architecture" , *Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology*, pp: 104-107.

[24] Kumari, A., (2011), "Grid Based Security Framework for Online Trading", I*n the Proceedings of IEEE*, pp: 1-4.

[25] Lonea, A.M. and Popescu, D.E., (2010), "Security Issues For GRID Systems", *In the Proceedings of IEEE*, pp: 73-76.

[26] Mandal, B., (2014), "A Comparative and Analytical Study on Symmetric Key Cryptography", *In the Proceeding of International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, pp: 131-136.

[27] Min, B. and Varadharajan, V., (2014), "Design and Analysis of Security Attacks against Critical Smart Grid Infrastructures", *In the Proceeding of 19th International Conference on Engineering of Complex Computer Systems*, pp: 59-68.

[28] Miri, A., (2014), "Efficient Pairing-Free, Certificateless Two-Party Authenticated Key Agreement Protocol for Grid Computing", *In the Proceedings of IEEE*, pp: 279-284.

[29] Mishra, N., (2014), "SECURITY ISSUES IN GRID COMPUTING", *International Journal on Computational Sciences & Applications (IJCSA)*, 4(1), pp: 179-187.

[30] Mo, L. and Lin, F., (2014), "A dynamic re-encrypted ciphertext-policy attributed-based encryption scheme for cloud storage", *In the Proceeding of Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp: 14-19.

[31] Mote, Y., (2012), "Superior Security Data Encryption Algorithm(NTRU)", *An International Journal of Engineering Sciences, 6(12*), pp: 171-181.

[32] Mukhin, V., (2007), "The Security Mechanisms for Grid Computers", *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pp: 584-589.

[33] Nandagopal, M. and Uthariaraj, R., (2011), "Performance Analysis of Resource Selection Algorithms in Grid Computing Environment", *Journal of Computer Science*, 7 (4), pp: 493-498.

[34] Narasimham, C. and Pradhan, J., (2008), "EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES", *Journal of Theoretical and Applied Information Technology*, pp: 55-59.

[35] Ranjan, R., (2012), " Improvement of NTRU Cryptosystem" , *International Journal of Advanced Research in Computer Science and Software Engineering*,2(9), pp: 79-84.

[36] Singh, S. and Majithia, S. and (2013), "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*,3(11), pp: 100-105.

[37] Purcell, A., (2012), Smartphone grids – the future for distributed computing?, from the website https://www.sciencenode.org/feature/smartphone-grids-future-distributed-computing.php accessed on 8/10/2015.