Enhanced Privacy Based Authenticity for Smart e-Health Cares using Light Weight ECC

Keerthana N V[1], Deepika Sakthivel[2], Divyathaila Balasubramaniyan[3], Karthika Gunasekaran[4], Madhumitha Marimuthu[5]

[1]Assistant Professor, Department of Information Technology, Tamilnadu, INDIA

(Email id:nvkeerthu@gmail.com whatsapp no 9994180869)

[2]Student,Department ofInformation Technology, Tamilnadu), INDIA

(Email id: deepikasakthivel2016@gmail.com whatsapp no 9600990605)

[3]Student,Department ofofInformation Technology, Tamilnadu,INDIA

(Email id: divyathailadt22@gmail.com whatsapp no 9500836223)

[4]Student, Department ofofInformation Technology, Tamilnadu,INDIA

(Email id: skkarthika99@gmail.com whatsapp no8667699192)

[5]Student, Department ofofInformation Technology, Tamilnadu,INDIA

(Email id: madhumitha.vcet@gmail.com whatsapp no 8946030842)

(Corresponding author: Keerthana N V Email id: nvkeerthu@gmail.com whatsapp no9994180869)

ABSTRACT: *Emerging technologies apace ever-changing the essential qualities of contemporary societies in terms of good environments. Aside from the alleged good environments, together with good town, good agriculture, Internet of Things (Iots) are enclosed recently in e-healthcare systems additionally for time period diagnosis and medical practice. The Internet of Medical Things (IoM) has become an expert application system and is used to gather and analyze the medical records of patients. During initial stage, such technology has constantly run into fewer privacy controls. Since the patient info is thus sensitive to reveal aside from a medical skilled, the protection and privacy of medical information are getting a difficult problem in IoM. Therefore, our present work is about a smart e-healthcare framework which deals with electronic medical records (EMRs) that preserves the privacy issues. Moreover, we have experimented the proposed work with respect to security constraints and have compared with recent works. The result shows that the proposed work is efficient in providing privacy along with Elliptic Curve Cryptography (ECC) token authentication on smart e-health care.*

Keywords: **Cryptographic system**, **ECC Token authentication, Health care records, Privacy control, Security protection and User privacy.**

Abbreviations: EMR, electronic medical records; ECC, elliptic curve cryptography; WSN, wireless sensor network; IOM, internet of medical things; IOT, internet of things; MAC, Mandatory Access Control; ACL, Access Control List.

I. INTRODUCTION

There is a global trend to an active involvement of persons in the maintenance and restoring of health. An electronic healthcare system has a wireless sensor network (WSN), which has lightweight resources with limited memory, bandwidth, and processing power-health grown out of a need for improved security of stored data and tracking of patient's health and procedures. Providing health care management services means the timely use of personal health services to achieve the best possible health outcomes. From the past, health care providers kept paper records on the history and status of their patients. In general, information is conveyed from one healthcare professional to another through paper notes or personal communication. Multiple copies of the repeated data exist in the hospital may lead to inconsistencies of data in various data stores. Most of the systems have found to be unsuitable to claim the security goals. It ensures the confidentiality of the health records but the privacy and reliability are not ensured. However, the rising health care costs and technological advancements encouraged the development of electronic tracking systems. Internet of Medical Things (IoM) for hospital environment is used to analyses the security and performance issues. This system includes patient, medical professional, system database, gateway and server that are used to provide incredible application benefits namely large-scale medical monitoring, casualty emergency medical tracking and responses. In healthcare application system, the security and privacy of patient's data are one of the biggest concerns to adopt wireless communication technologies such as wireless gateway access, mobile computing devices. To enhance the privacy issues, Electronic Medical Records (EMRs) are used. Various techniques are used for the privacy in e-healthcare such as pairwise key establishment, multibiometric key generation, hash function, attribute-based encryption, hybrid encryption, Number Theory. In the proposed model Elliptic Curve Cryptography (ECC) token authentication is efficient in providing privacy in smart e-health care.

II. RELATED WORK

Privacy Ensured e-Healthcare for Fog- Enhanced IoT Based Applications [26] was contributed by Rahul Saha, Gulshan Kumar, Mritunjay Kumar Rai, Reji Thomas And Se-jung Lim (2019). This paper addresses the privacy issues in e-healthcare. This framework uses numerous end-user devices like health observance systems, mobile devices and laptops, a fog layer comprised of fog accumulators as knowledge aggregators, fog devices like access points, servers, switches and routers and cloud servers. The various techniques and algorithms proposed in the article are shown. Data aggregator at the fog level to restrict the one-point authentication. It reduces communication overhead at each level. Elliptic curve cryptographic (ECC) approach ensures

confidentiality. Consensus algorithm is used to enhance the reliability and trust in the EMR transactions.

Security and privacy issues in e-health cloud-based system [11] was an IEEE paper published by Azeez N.A and van der Vyver C (2019). The motive of this architecture is to provide a secured, dynamic and dependable framework for E-Health care system. Thisframework is to be completely controlled by the patient WHO is taken into account as a significant neutralin E-health system. The proposed system has used two security protocols such as Mandatory Access Control (MAC) and Access Control List (ACL) to ensure authentication. Mandatory Access Control is a type of security framework model that permits operating system to obtain the ability of an initiator of an action. It is used to carry out some operations on a target or an object. An object is referred as constructs such as files, IO devices or memory segments and a subject could be regarded as a thread or a process. On the other hand, Access Control List is a security model that provides a set of permission attached to the objects. It identifies who among the users or processes should be granted access privilege to objects. It also shows what operations are permitted on given objects.

Provably secure ECC-based device access control and key agreement protocol for IoT environment [28] was the major contribution of Das A.K, Park Y, Rodrigues J.J.P.C,Wazid M, Yannam A.R (2019) . In this paper, there is an efficient protocol for device access control and key agreement, called Light weight access control and key agreement protocol (LACKA-IoT) in the IoT environment. It is a lightweight protocol and utilizes ‘‘ECC primitives and one-way cryptographic hash function’’. LACKA-IoT contains the following phases System setup phase, Device registration phase, Device access control phase and Dynamic device addition phase. It has shown that LACKA-IoT can resist other known attacks that are needed for securing IoT environment through access control mechanism and it is secure against the man-in the-middle attack. It provides security against the malicious device deployment attack.

III. SYSTEM ARCHITECTURE

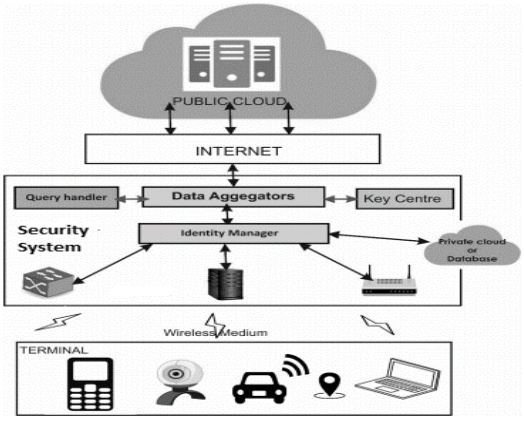

Fig.1.Proposed framework for the privacy ensured e-healthcare network

The functions of every modules area unit as follows.

- **Key Centre:** Key center is responsible for generation and verification of keys.
- **Query Handler:** Handles and responses with a query which is beyond a specific view request.
- **Identity Manager:** Maps the identity to a pseudo-identity to cover the patient details as needed.
- **Data Aggregators:** All the data from the nodes are aggregated by the data accumulator and then outsourced to the public cloud.

IV. PROPOSED SYSTEM

In the present work the proposed framework addresses the privacy issues in e-healthcare. This framework uses various end-user devices such as health monitoring systems, mobile devices and laptops, connectivity devices such as access points, servers, switches and routers and cloud servers. For ensuring privacy, Aadhar number verification by using token-based encryption. There are four types of privacy i) privacy of personal information also referred as data privacy, ii) privacy of personal behavior, iii) privacy of personal communication and privacy of the person.

In this approach to enable a highly secured privacy authentication by two modules are added in the framework.

- Key center
- Query handler.

Key Centre: Key center is responsible for generation and verification of keys.
Query Handler: Handles and responses with a query which is beyond a specific view request. The queries are based upon the consensus to access the view of EMR.
The benefits of the proposed framework are as listed below:

- Data aggregator is used reduce communication overhead at each level.
- Elliptic cryptographic approach is used to ensure confidentiality.
- Consensus algorithm is used to enhance reliability and belief in the EMR transactions.

To design security system with enhanced privacy based Light Weight ECC token authentication on smart e health care. In Lightweight cryptography, ECC is strong and fast algorithm against numerous attacks in wireless sensor networks (WSN) and other wireless suitable environments. It gives the same level of privacy in a 160-bit key size when compared to privacy provided by 1024-bit key size.
To generate a strong key value has a minimum length of bits that will be useful in lightweight cryptography. Using Elliptic Curve Cryptography (ECC) with algebraic graph to found a secret key value. ECC is the strongest algorithm and it produce a pair of public and private keys. With the help of public and private keys to generate a secret key value.

V.SECURITY ANALYSIS ON THE PROPOSED METHOD

The proposed cryptography method satisfies all the security measures needed for the applications such as link ability, ident ability, nonrepudiation, detectability.

Linkability: An individual could plan to distinguish whether two or lot of EMRs like medical information are associated with constant user. It might try to correlate that sensitive information and gather a logical access provisions for the user who accessed this service with a device at a particular location, thus exhibits the habits of the patient. The proposed model is used to ensures a solution by providing 'unlink ability' with token based-identity and view access.

Identiability: A patient could plan to correspond and establish the sorts of messages or EMRs that is retrieved or changed. Thus, the token based-identity preserves 'ident ability' in the proposed approach.

Non-repudiation: It can be used to preserve patient's privacy. An opponent may attempt to collect EMRs stored and exchanged data within the cloud infrastructure and be able to deduce some information about a patient or medical consultancy.

Detectability: An opponent may tend to correspond and infer stats about the type of EMRs with the messages exchanged amongst communication service provider (CSPs) entities. For e.g., an adversary finds to identify the timing elements for the heart patient when the monitoring system incessantly sends monitored data to the private health cloud. The proposed framework ensures these by using cryptography with ECC.

Algorithm

Light Weight ECC:

Step 1: Elliptic curve cryptography can be used to encrypt plaintext message, M, into ciphertexts. The plaintext message M is encoded into a point PM from the finite set of points in the elliptic group, Ep(a, b).

Step 2: The first step consists in choosing a generator point, G ε Ep(a, b) such that the smallest value of n for which nG = O is a very large prime number. The generator G and the elliptic group G are made public.

Step 3: Assume that Bob and Alice intend to communicate. Each user selects a private key and uses it to enumerate their public-key. For example, Alice (A) selects a private-key nA<n and computes the public-key PA as: PA = nAG.

Step 4: To encrypt the message PM for Bob (B), Alice chooses a random integer k and computes the ciphertext pair of points PCs using Bob's public-keyPB:

Step 5: PC = [(kG), (PM+k PB)]

Step 6: After receiving the cipher text pair of points, PC, Bob multiplies the first point, (kG) with his private-key, nB and then subtracts the result to the second point in the ciphertext pair of points, (PM+k PB)

Step 7: (PM+k PB)-[nB(kG)] = (PM+knBG)-[nB(kG)] = PM

Step 8: which is the plaintext point, corresponding to the plaintext message M. Only Bob, knowingthe private-key nB, can remove nB(kG) from the second point of the ciphertext pair of point, i.e., (PM+k PB) and hence retrieve the plaintext information PM.

Table 1: Comparison of Features

	Data aggregator	View controller	Consensus	Un-Linkability	Non-Identiability	Non-repudiation	Un-Detectability
Masood et.al.[20]	no	no	no	yes	no	yes	no
Menaka et.al.[29]	no	no	no	no	no	yes	no
Lamport et.al.[30]	no	no	no	no	no	yes	no
Proposed approach	yes	yes	yes	yes	yes	yes	yes

VI. RESULTS AND DISCUSSION

The above-mentioned model is tested in practical scenario involving cloud infrastructure in the network fore-healthcare services. A consensus is implemented with the Hyperledger composer. For the convenience of query parsing a SQL data querying system is used.

Table 2: Average EmrTransaction Time (Milliseconds)

No.Of EMRs	Masood et.al.[20]	Menaka et.al.[29]	Lamport et.al.[30]	Proposed approach
100	20.433	20.133	23.500	18.543
200	20.633	22.500	25.667	19.023
300	23.176	24.017	26.333	21.777
400	24.500	27.433	26.919	21.500
500	24.337	27.237	27.000	22.334
600	25.474	31.717	28.133	23.003
700	26.333	32.333	29.500	25.993
800	28.777	35.767	30.777	27.333
900	30.011	37.000	31.808	27.886
1000	32.500	39.977	32.617	29.717
Time complexity	O(n2) + O(C)	O(n2) + O(C)	O(n) × O(C) × O(nlogn)	O(n) × O(C) × O(d)

n is the number of EMRs and C is the cryptographic timings, d is the data aggregator consensus time.

The obtained results using proposed model are estimated with the other recent works described in [20],[29], [30]. The performances are analyzed by using two basic measurable aspects: time consumption and memory consumption. For consensus implementation, 1 TB of memory is used inL1-L2 cache for the experimentation.

The cache is used to helps the data aggregators with the minimum delay. The delay of EMR transaction is measured in milliseconds and is shown in Fig-2. Average time of EMR transactions and time complexity are mentioned in Table-2.
The results described in the Table-2 shows that the proposed work has less transaction time that is 13.84% less as compared to other algorithms. It is due to the one-point cryptographic exchange with data aggregators in the framework.The comparison results shown in Fig-2. It shows reduced delay which is approximately 23.6% with the proposed algorithm. If one corresponds the average EMR transmission data and overall delay, the delay gets double due to multiple cryptographic exchanges between nodal points. In the proposed framework, only one-time signature exchange is done. It makes the overall process less time consuming and faster processing of information can be done.

A new variable is introduced and is used to compared view utilization ratio with no of queries managed by the algorithms within a specific time duration. The variable has been defined as:

$$\text{QVR } \% = \frac{\text{No. of allowed queries of EMR}}{\text{Total number of queries for EMR}} \times 100$$

QVR values possess almost 100% for all and the other algorithms whereas theproposed model QVR is much less. It controls the access view of the EMRs and hence obtaining less QVR. With regards to privacy, the less QVR also becomes an advantage. The results in Fig-3 shows theworking functionality of the query handler in the framework.

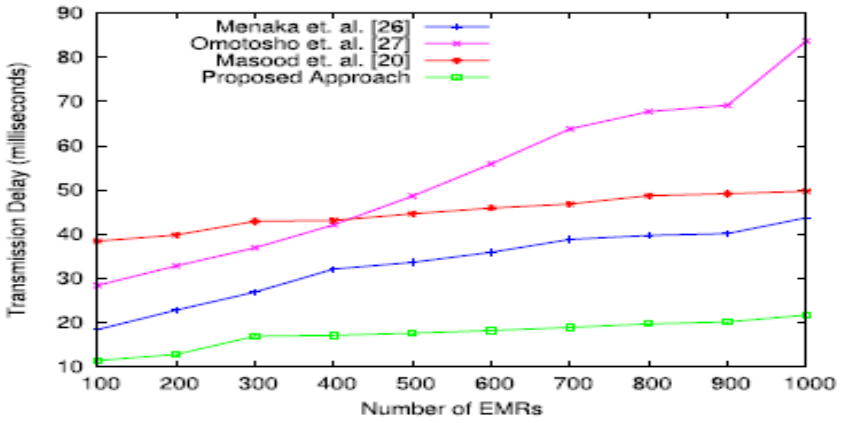

Fig.2. Comparison of Time Delay

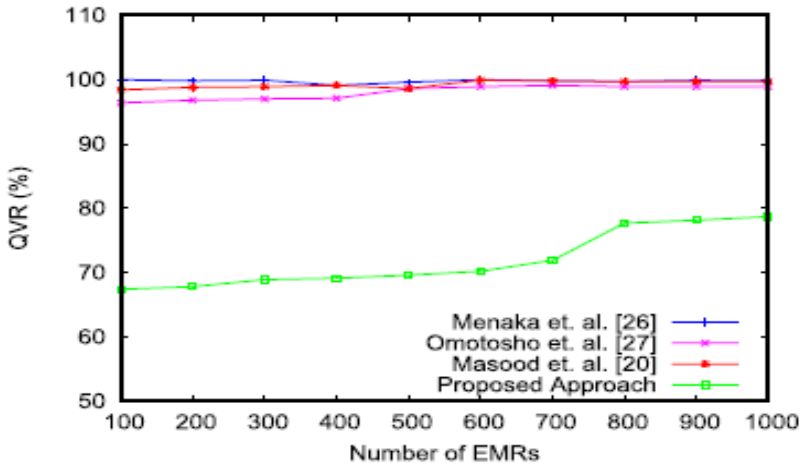

Fig.3. Comparison of Query View Ratio.

Finally, the features of the proposed framework with the other algorithms and the summarization are compared in Table-1. In Table-1 the comparison features how that the proposed approach (Lightweight ECC) is efficient and it has required features for any cloud-based smart e-healthcare.

VII. CONCLUSION

The e-Health care system made everything easier and more comfortable wherein the entered data and information are more accurate and safety. Now, it is considered as one of the most popular health technologies, it improved all the aspects of health care and thus providing accurate information and fast access regarding the patients. The application of e-health solutions has brought a number of advancements in the health care industry. E-health solutions across the globe have helped in improving the healthcare facilities acrossthe globe in the both developed and developing nations where e-healthcare system has been implemented.

VIII. FUTURE SCOPE

In the future, the system will integrate more apps tohealth care application to make it more advanced self– help tool and to give a wide range of facilities to the end user.The long run of tending is shaping up with advances in digital tending technologies like computing, VR/AR, 3D-printing, AI or engineering science.

CONFLICT OF INTEREST

The authors declare here that they have no conflict of interest.

REFERENCES

[1] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, ``IoT survey: An SDN and fog computing perspective," *Computer. Netw.*, vol. 143, pp. 221_246, Oct. 2018.
[2] M.B.M. Noor and W. H. Hassan, ``Current research on Internet of Things (IoT) security: survey," *Comput. Netw.*, vol. 148, pp. 283_294, Jan. 2019.
[3] P.P.Ray, ``A survey of IoT cloud platforms," *Future Comput. Inform. J.*, vol. 1, nos. 1_2, pp. 35_46, 2017.
[4] M.Armburst*et al.*, ``A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, p. 5058, 2010.
[5] *Cisco Global Cloud Index: Forecast and Methodology, 2016_2021*, Cisco,San Jose, CA, USA, 2018.
[6] L. Peng, A. R. Dhaini, and P.-H. Ho, ``Toward integrated cloud_fog networks for efficient IoT provisioning: Key challenges and solutions,' *FutureGener. Comput. Syst.*, vol. 88, pp. 603_616, Nov. 2018.
[7] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, ``Towards fog-driven IoT e-Health: Promises and challengesof IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659_676, Jan. 2018.
[8] R.Madhusudhan and R. C. Mittal, ``Dynamic ID-based remote userpassword authentication schemes using smart cards: A review," *Intell.Algorithms Data-Centric Sensor Netw.*, vol. 35, no. 4, pp. 1235_1248,Jul. 2012.
[9] C. Zhao, J. Jiang, Z. Xu, and Y. Guan, ``A study of EMR-based medical knowledge network and its applications," *Comput. Methods ProgramsBiomed.*, vol. 143, pp. 12_23, May 2017.
[10] A. S. M. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, ``Context aware access control with imprecise context characterization focloudbased
data resources," *Future Gener. Comput. Syst.*, vol. 93, pp. 237_255,Apr. 2019.
[11] N. A. Azeez and C. van der Vyver, ``Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Inform.*
J., vol. 93, pp. 237_255, Apr. 2019.
[12] S.Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon,and K.-Y. Yoo, ``Secure signature-based authenticated key establishmentscheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028_3043,2017.
[13]S.Otoum, B. Kantarci, and H. Mouftah, ``Empowering reinforcement learning on big sensed data for intrusion detection," in *Proc. IEEE Int.Conf. Commune. (ICC)*, May 2019, pp. 1_7.
[14] F. Al-Turjman, H. Zahmatkesh, and L. Mostarda, ``Quantifying uncertainty in Internet of medical things and big-data services using
intelligence anddeep learning," *IEEE Access*, vol. 7, pp. 115749_115759, 2019.
[15] F. Al-Turjman, ``Intelligence and security in big 5G-oriented IoNT: Anoverview," *Future Gener. Comput. Syst.*, vol. 102, pp. 357_368, Jan. 2019.
[16]F. Al-Turjman, H. Zahmatkesh, and R.Shahroze, ``An overview of securityand privacy in smart cities' IoT communications," *Trans. Emerge. Telecom-mun. Technol.*, vol. 8, p. e3677, Jul. 2019.
[17] M. A. Habib, M. Ahmad, S. Jabbar, S. Khalid, J. Chaudhry, K. Saleem,J. J. P. C. Rodrigues, and M. SayimKhalil, ``Security and privacy basedaccess control model for Internet of connected vehicles," *Future Gener.Comput. Syst.*, vol. 97, pp. 687_696, Aug. 2019.
[18] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues,``Design and analysis of secure lightweight remote user authentication and

key agreement scheme in Internet of drones deployment," *IEEE InternetThings J.*, vol. 6, no. 2, pp. 3572_3584, Apr. 2019.
[19] C. Stergiou, K. E. Psannis, B. B. Gupta, andY. Ishibashi, ``Security, privacy& efficiency of sustainable cloud computing for big data & IoT," *Sustain.Comput. Inform. Syst.*, vol. 19, pp. 174_184, Sep. 2018.
[20] H. Dawood, I. Masood, N. R. Aljohani, A.Daud, and Y. Wang, ``Towardssmart healthcare: Patient data privacy and security in sensor-cloud infrastructure,"*WirelessCommun. Mobile Comput.*, vol. 2018, Nov. 2018,Art. no. 2143897.
[21] Z. Guan *et al.*, ``APPA: An anonymous and privacy preserving data aggregationscheme for fog enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125,pp. 82_92, Jan. 2019.
[22] M. A. Sahi*et al.*, ``Privacy preservation in e-healthcare environments: Stateof the art and future directions," *IEEE Access*, vol. 6, pp. 464_478, 2017.
[23] K. Zhang, X. Liang, M. Baura, R. Lu, and X. Shen, ``PHDA: A prioritybased health data aggregation with privacy preservation for cloud assistedWBANs," *Inf. Sci.*, vol. 284, pp. 130_141, Nov. 2014.
[24] D. Koo and J. Hur, ``Privacy-preserving deduplication of encrypted datawith dynamic ownership management in fog computing," *Future Gener.Comput. Syst.*, vol. 78, pp. 739_752, Jan. 2018.
[25] S. Rahul Saha, K. Gulshan Kumar,k.Mritunjay Kumar Rai, S. Reji Thomas and L, Se-jung Lim, "Privacy Ensured e-Healthcare for Fog-Enhanced IoT Based Applications ", 9 IEEE. Translations and content mining are permitted for academic research , Vol. 7, pp. 44536-44543, 2019.
[26] A.K.Das,Y. Park ,J.J.P.CRodrigues ,M. WazidA.RYannam and "Provably secure ECC-based device access control and key agreement protocol for IoT environment," IEEE Access, vol. 7, pp. 5538255397,2019.
[27] C.Menaka and R. S. Ponmagal, ``Patient-controlled personal health recordenforcing patient privacy in cloud based healthcare system," *Int. J. PureAppl. Math.*, vol. 119, no. 10, pp. 375_392, 2018.
[28] L.Lamport, ``Password authentication with insecure communication,"*Commun. ACM*, vol. 24, no. 11, pp. 770_772, Nov. 1981.
[29] Keerthana N.V, Roja.S, Santhiya S, Sowndharya L, Vennila N, " Data security using certificateless signature cryptosystem", South Asian Journal of Engineering and Technology, vol 8, No 1, pp 169-176.
[30] Keerthana N.V, Muralikrishnan K.S, "Secure and Trusted Resource provisioning for computational grid Infrastructure Using Gridsim", ITRAD, vol 2, No 3, pp 4-10.