Security of Data in Cloud based E-Governance System

Smitha K K
Department of Computer Science & Engineering
SCT College of Engineering
Trivandrum, India

Chitharanjan K
Department of Computer Science & Engineering
SCT College of Engineering
Trivandrum, India

ABSTRACT
The overwhelming success and the rapid growth of the Internet change our lives; the way we interact, learn and work. Now a day's most of the organizations including government deliver their services through internet. E-governance is the application of information and communication technologies to exchange information between government and the citizens, government and business organizations and between government organizations. Cloud computing is a new way of accepting and providing services over internet. Cloud based e-governance system provides many benefits to Government like reduced cost, distributed storage of data, availability of resources at lower cost ,manages security, scalability, accountability and modifiability.

Security is the one of the crucial issue in Cloud based E-governance system. As the number of services provided by the E-governance system to the users increases a high level of E-Government security is required. Security of information is concerned with the properties like confidentiality, integrity, authentication, availability and reliability. In an E-governance system databases contain all the government information so that it should keep very confidentially. The government databases deployed to the cloud contain critical and private information. The databases are uploaded to the storage facility provided by the cloud service provider, who has higher priority to access the data. Since data are exposed to a third party, several security threats may occur. For ensuring confidentiality of government data they are encrypted before storing in to cloud. This paper proposes a new mechanism for database encryption with flexible data granularity and safe key management for high security and better performance for database access.

General Terms
Cloud computing, Security.

Keywords
Cloud computing, e-governance, security, confidentiality and Encryption

1. INTRODUCTION
The overwhelming success and the rapid growth of the Internet changes our lives, the way we interact, learn and work. Most of the organizations deliver their services through internet. Traditionally accessing government services is more difficult, as one needs to go through so many procedures and formalities. Hence the government across the world aims to deliver their services through electronic media under the name e-governance. The different users of the E-governance include government, citizens, and Businesses. With E-Governance, Government interacts with the citizens more easily and rapidly. An effective E-governance system should be cost effective, reliable and easy to maintain. Unfortunately current technologies are not enough to meet the overall requirements of E-Governance. Cloud computing provides a platform for efficient deployment of E-governance system. It leads to substantial cost savings. Cloud computing provides hardware, software and network as a service. It provides better technological solutions for E-Governance.

Cloud based E-governance represents an emerging paradigm for distributed computing of E-governance applications that utilizes services as fundamental elements in building agile networks of collaborating applications distributed within and across government boundaries. In such open distributed computing environments, security is of paramount concern.

1.1 E-governance
E-governance is the application of Information and communication technologies (ICT) to exchange information between the government and the citizens, government and businesses and between government organizations [1]. E-governance is used to improve the interaction between Government and Citizens, Government and Businesses by the application of some electronic means. It also employ electronic means in internal Government operations to simplify them. E-governance system helps to improve the productivity of Government and helps in decision making [2].

For developing an E-governance system first we identify different users of the system, they are Government, Citizens, Businesses and Enterprises. E-governance aims to deliver more reliable services to all these users. E-governance applications are classified into four broad categories.

- Government to Government (G2G) E-governance supports the exchange of information, decision making, fund transfer, shared services, revenue and law enforcement between the inter organizational Government departments.
- Government to Business (G2B) E-governance provides the services like registration, tax filing, transactions and payments. Businesses should aware and use the services provided by Government through a secure mechanism.
- Government to Citizens (G2C) E-governance supports the services like registration/land/revenue services, agricultural services, employment etc.
- Government to Enterprise (G2E) E-governance supports some enterprises like water board, electricity board etc are controlled by the government which where some policies and standards are to be enforced.

1.2 Cloud computing
Cloud computing is a new way of accepting and providing services over internet. Cloud based E-governance system provides many benefits to Government like reduced cost, distributed storage of data, gets more resources at lower cost , manages security, scalability, accountability and

modifiability. Cloud computing can be treated as a future of computing [3]. At present many Cloud services providers like Hadoop, Amazon Compute Cloud EC2, Microsoft Azure, Aneka and Google AppEngine are in use.

According to the IEEE Computer Society Cloud Computing is:"A paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include desktops, entertainment centers, table computers, notebooks, wall computers, handhelds, etc." Cloud computing provides every facility as a service. It provides infrastructure as a service, software as a service and platform as a service.

- Infrastructure as a service (IaaS) – In a cloud based E-governance system, cloud provides hardware, network and data storage as services. Cloud computing provides a common infrastructure to all application, so it is easy to use and deploy. E-governance applications requires huge amount of data. Cloud computing provides unlimited supply of cpu, storage and bandwidth for E-governance applications. So the designer has only focus on its features and usability.
- Software as a service (SaaS) – Cloud computing provides the use of complete applications, running on cloud to the consumers. Government departments may not want purchase the E-governance applications, but they can request and use these applications from the cloud. Many of the applications can be provided as standard services. Some of them are
    - Complaint Resolution System.
    - Employee Management Systems.
    - Attendance Resolutions Systems.
    - E-police, E-court.
    - Municipal Maintenance.
    - Water Boards, Billing, Payment Systems.
- Platform as a service (PaaS) – Cloud computing provides a virtual developing environment to the developers. Cloud offers standard platform for E-governance developers. Some of the platform they provided are
    - OS provisioning.
    - Queuing Service.
    - Database Services.
    - Middleware Services.
    - Workflow Services.

The different deployment models for cloud computing are as follows:

- Private cloud – The cloud infrastructure which is operated and used by a single organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud – The cloud infrastructure which is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on premise or off premise.
- Public cloud – The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud – The cloud infrastructure is a composition of two or more clouds such as private, community, or public that stands as unique entities but are bound together by standardized technology that enables data and application portability.

2. CLOUD BASED E-GOVERNANCE

Cloud based E-governance represents an emerging paradigm for distributed computing of E-governance applications that utilizes services as fundamental elements in building agile networks of collaborating applications distributed within and across government boundaries.

2.1 E-governance challenges and cloud benefits

E-governance faces some challenges like technical, economical and social challenges. Interoperability between the existing and current hardware and software are major technical issue. Some legal aspects like security and privacy issues are important. Social challenges like technical illiteracy are also a major challenge. The initial installation cost, implementation cost and maintenance cost are the economical challenges faced by the E-governance system.

Cloud computing can be capable of resolving several issues in E-Governance. Cloud computing offers several benefits to E-governance [4], some of them are

1. Data Scaling – E-governance applications deals with large data over the years, so the databases should be scalable. Relational databases ensure integrity of data at the lowest level, where as cloud databases can be scalable at any level and used for E-governance applications. Cloud databases must be considered if the foremost concern is on-demand, high-end scalability – that is, large scale, distributed scalability, the kind that can't be achieved simply by scaling up.
2. Auditing and Logging – E-governance services must be monitored and any change in information content must be traced. By keeping the providers of services accountable, Corruption in Government organizations can be controlled. Security audits and process audits must be done periodically to ensure the security of the system. Cloud computing help to analyze the huge volume of data for detecting fraud. It helps to provide defense mechanisms to enhance the security of the system.
3. Rolling out new instance, Replication and Migration – Typically E-governance applications works for departments of different states and municipalities and hence take more time, resources, effort and budget. Cloud architectures offer excellent features to create an instance of application for rolling out a new municipality. Cloud can reduce the time to deploy new application instances.
4. Disaster Recovery - Natural disasters like floods, earthquakes, wars and internal disturbances could cause the E-governance applications not only loose data, but also make services unavailable. The Cloud offers tools and technologies that make disaster recovery simple and easy. Cloud helps to increase the number of resources dynamically to maintain quality of service intact even at the times of high load, which generally happens in E-Governance.
5. Performance and Scalability – The technology and architecture used for implementing E-governance applications should be scalable and common across delivery channels. It is required to meet the growing number and demands of user. With cloud architectures, scalability is inbuilt. Typically, E-governance applications can be scaled vertically by moving to a more powerful machine that can offer more memory, CPU, storage. A simpler solution is to cluster the applications and scale horizontally by adding resources.

Reporting and Intelligence – For better utilization of resources the factors like Data center usage (CPU, storage, network etc), peak loads, consumption levels, power usage along with time etc are monitored and reported. This minimizes the cost and plan. Because of its sheer size and capabilities Cloud offers better Business Intelligence infrastructure compared to traditional ones. Cloud computing offers seamless integration with frameworks like MapReduce (Apache Hadoop) that fit well in cloud architectures. Applications can mine huge volumes of real time and historic data to make better decisions to offer better services.

6. Policy management – For dealing with citizens Government policies must be adhered and implemented in E-governance applications. Along with the infrastructure and data center policies has to be enforced for day to day operations. Cloud architectures help a great deal in implementing policies in data center. Policies with respect to security, application deployment etc can be formalized and enforced in the data center. With cloud, E-governance applications can manage the policies well by providing security and adoptability.
7. Systems Integration and Legacy Software – Applications that are already deployed and providing services are to be moved to the cloud, and that are integrate with applications deployed in the cloud. The Information Technology helps to co-relating the data across applications and pass messages across different systems to provide faster services to the end users. Cloud is built on SOA principles and can offer excellent solutions for integration of various applications. Also, applications can be seamlessly easily moved into cloud.
8. Migration to New Technologies – Technology migration is the biggest challenge. Moving to different versions of software, applying application and security patches is the key to maintaining a secure data center for E-Governance. Cloud architecture efficiently enables these kinds of requirements, by co-existing and co-locating different versions and releases of the software at the same time. Once these applications are tested, they can be migrated into production with ease.

3. SECURITY ISSUES

E-Governance will become more popular around the world in next few years. Most of the countries are in the early stage of development of E-Governance system. Security is the one of the crucial issue in E-Governance system. As the number of services provided by the E-Governance system to the users increases a high level of E-Government security is required.

There are several security issues concerned with E-Governance. Some of them are

1. Identification of security requirements.
2. Data protection and Data base security.
3. Physical and personal security.
4. Certification / Authentication.
5. Risk analysis and metric for E-Governance.
6. Privacy.
7. Identity management.
8. Availability.

Security of information is concerned with the properties like confidentiality, integrity, authentication, availability and reliability. Authentication of information identifies the actual author of the information. Secure electronic authentication is important in an E-Government system. Different authentication methods are available ranges from software solutions like use of passwords to hardware solutions like use of smartcards. Confidentiality of information means the information is to be confidential, only the authorized person can view the information. Confidentiality is the prevention of unauthorized information disclosure. Integrity of information means unauthorized person cannot alter or tamper the message stream of the information. Information should be available at all time and there is no delay or denial of service attacks.

In an E-Governance system databases contain all the government information so that they should keep very confidential. Databases connected to the web contain critical and private information. So that there are different threats occurs, someone can masquerade as a legitimate user and reveal private and costly information.

Privacy is another important security aspect. Different people consider different data as public or private. There are different levels of privacy; some data require no privacy while some others require high level of privacy. From everyday transactions Government collect different information from citizens, so that protecting the privacy of citizens' information like personal data, financial and medical data is an important issue. The databases are uploaded to the storage facility provided by the cloud service provider, who has higher priority to access the data. Since data are exposed to a third party, several security threats may occur. For ensuring confidentiality of government data they are encrypted before storing in to cloud.

4. ENSURING CONFIDENTIALITY OF DATA IN CLOUD

The implementation of Cloud based governance needs strong security mechanism because the sensitive data goes beyond the boundary of Government organization. Government organization would adopt Cloud based governance only if it is capable to provide them enough assurance regarding the safety of their sensitive data because they go beyond their organization boundary and stores the storage space provided by the cloud service provider.

The scenario for explaining my proposed work is how to obtain a water supply connection from the water supply department [18]. The proposed architecture of my system is shown in figure 1.

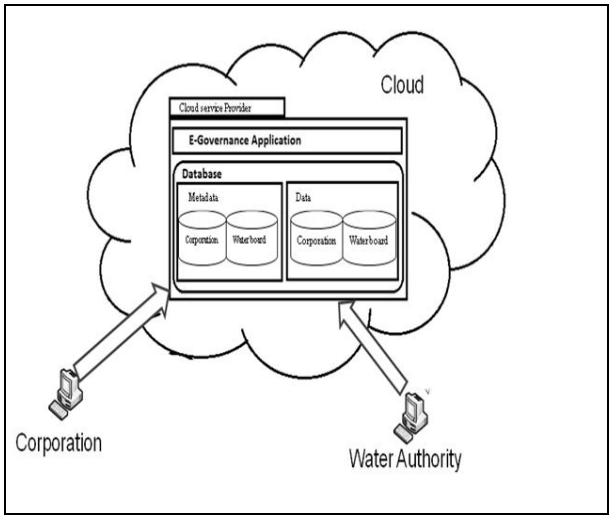

Fig 1: Architecture of e-governance application

The E-application and the databases for corporation and the water supply department are stored in cloud. The stages in obtaining a water-connection are:

- The citizens can submit an e-application for anew water-connection.
- The water supply server checks whether the Survey Field Number (SF number) of the land belonging to the applicant has been regularized by the municipal corporation.

Once the corporation server identifies that the SF number is a regularized one, the building plan is approved and the plan approval charges are calculated and levied.

Once all these are completed, the water supply server then approves the water-service connection, allots a water connection serial number and then calculates the appropriate water-connection charges.

This implementation needs strong security mechanism because the sensitive data goes beyond the boundary of Government organization. Encryption is a well established technology for protecting sensitive data [21]. So for ensuring confidentiality of government data, there is an encrypt/decrypt module which encrypt all data before storing into the cloud.

So we need a strong database encryption scheme. A good encrypted database system should meet the following requirements

- Sensitive data at rest are encrypted.
- The process of encryption or decryption is transparent to application.
- The storage after encrypting doesn't increase much.
- The download of performance processing encrypted data is tolerable.
- Safe key Management.

We adopt column-level encryption, which allows user to define which data stored in databases are sensitive and thereby focusing the protection only on the sensitive data, in turn minimizes the delays or burdens on the system. The second dimension is the choice of encryption algorithm. There are two types of it: the symmetric and the public key encryption. The symmetric algorithm is faster than public key encryption schemes hundred or thousand times, on the other hand, every time encryption is used, two different keys will be generated, safety of private key storage is also hard to guarantee in public key scheme. As to the database encryption case, the keys number will be much huge. Generally public key encryption schemes are not used for database encryption [23]. We use the Advanced Encryption Standard (AES) symmetric-key block cipher for encrypting the sensitive data which is intended to replace DES and 3DES [24]. All the government data is encrypted using this encryption scheme before storing into the cloud.

The Run time architecture of database encryption system is shown in figure 2. Every time a user sends a request the user inter interface accepts the request and put forwards a query to the query translator. The query translator translates the query using the encryption module and submits to the database server. After executing the query the query result filter receives the encrypted data with the help of the decryption module the query result filter decrypts the encrypted data and sends to the user interface.

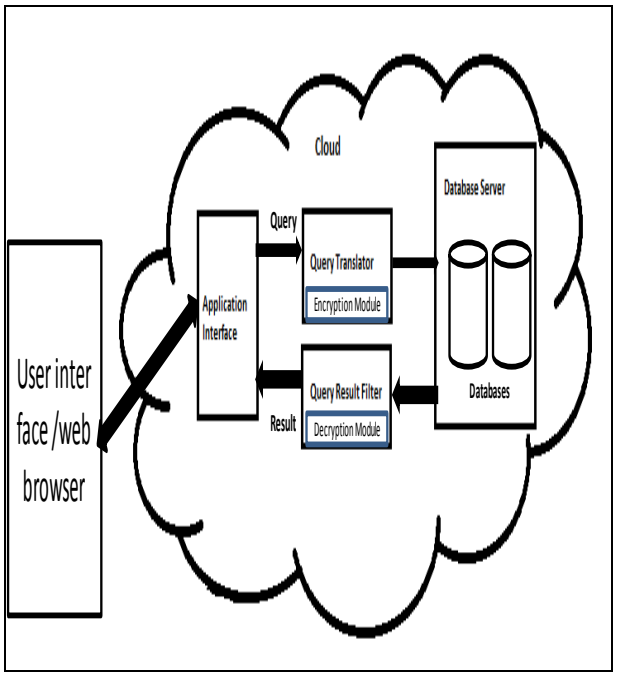

Fig 2: Run time architecture of database encryption system

The databases contain encrypted data so querying on it can greatly degrade the performance of database application system. Most of the cases, searching on an encrypted column will require the database to perform full scan over the table. So we need a mechanism to improve the query performance, which is rebuilding the SQL queries over encrypted relations using coarse index.

Each relation $R(A_1,..,A_m,\ldots A_n)$ of the original database are stored in the encrypted database of the form $R(A_1^E,..,A_m^E,..,A_n,A_1^s,..,A_m^s)$ with column from A_1 to A_m are encrypted. $A_1^s,...A_m^s$ are index columns used for locating the records, avoiding the full table scan and decryption at server. The creation of the column index will determine the query efficiency. So we use a better method. H.Hacigumus et al [22] uses a equi-width histogram to create partitioning of attributes, and then utilizes a collision-free hash function assigning an identifier to each partition. A value in the domain of attribute A_i will fall into a partition, in that way corresponding identifier will be stored in the encrypted table as a coarse index.

Now let's have a look at an example how the query translator translates the query. For this consider the water supply connection example which contain the relations

Application (aid, aname, address, sfnumber, buildingno)

Landdetails (lid, ownername, sfnumber, area, price, tax)

In which the columns address, sfnumber buildingno, area, price, and tax are sensitive because they contain confidential data of applicant like details of the land they owned. So these columns saved in encrypted form. The price column needs to have coarse index for comparison operations. Thus the

corresponding encrypted representation of the relations are

Application^{E}(aid, aname,addressE,sfnumberE,buildingnoE)

Landdetails^{E}(lid,ownername,sfnumber^{E},area^{E},price^{E},tax^{E}, price^{S})

Now the application wants to store records to the database posing a SQL request:

Insert into application values (1,'jhon','tvm',12,56)

Insert into landdetails values (101,'jhon', 12,5,55000,12)

The query translator will translate the query before submitting into database server. So we have to find the coarse index for price 55000. This is done by using the Map function , suppose the range of price of the form 0-500K and the map function is order preserving. We get Map (55000) = 2, then the insert query is translated into

Insert into application^{E} values

(1,jhon,encrypt(tvm), encrypt(12), encrypt(56))

Insert into landdetails^{E} values (101,jhon, encrypt (12),

encrypt (5), encrypt (55000), encrypt (12), 2)

In this way the query translator helps to insert all data into the encrypted database. The query result filter receives the result of query and decrypts the encrypted data in the result and then transmits them directly to the application.

The security of encrypted data depends on the security of keys at any extent .One easy solution is to store the keys in a restricted file, away from the encrypted data. So we embedded the key in the finger print image using DCT based image steganography techniques. The key is extracted only if this fingerprint matches with the fingerprint provided by the user who wants to decrypt data. This is done by using phase based image matching technique. When two images are similar, their Phase-Only Correlation (POC) function gives a distinct sharp peak.

5. EXPERIMENTAL SETUP AND RESULTS

To measure the proposed scheme's performance for administrator of the corporation and water supply server, evaluation process is carried out on 32 bit Intel Pentium laptop, Windows 7 with 2 GHz Dual Core Processor and 2 GB RAM. This cloud based e-governance application is developed by using the Windows azure emulators in visual studio 2010.We evaluate the proposed scheme on AES. To evaluate its performance on a cloud server we choose Microsoft Azure as a cloud service provider [25].

The performance is evaluated by changing different key sizes for AES encryption algorithm. In the case of AES three different key sizes is possible i.e., 128-bit, 192-bit and 256-bit keys. The Experimental result is shown in figure 3. It can be seen that higher key sizes give clear change in time consumption.

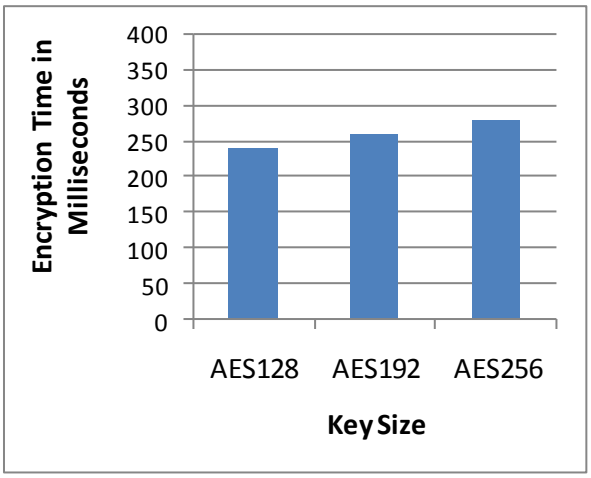

Fig 3: Time consumption for different key sizes for AES encryption

6. CONCLUSION

E-governance with cloud computing offers integration management with automated problem resolution, manages security end to end, and helps budget based on actual usage of data. At a global level, Cloud architectures can benefit government to reduce duplicate efforts and increase effective utilization of resources. This paper discusses the benefits provided by cloud computing to E-Governance. In an E-governance system databases contain all the government information so that it should keep very confidentially. The government databases deployed to the cloud contain critical and private information. The databases are uploaded to the storage facility provided by the cloud service provider, who has higher priority to access the data. Since data are exposed to a third party, several security threats may occur. For ensuring confidentiality of government data they are encrypted before storing in to cloud. By using the proposed encryption scheme the confidentiality of government data is achieved and in the same time we solve the problem of key storage to make key more secure.

7. REFERENCES

[1] Mrinalini Shah,"E-Governance in India: Dream or reality?" , International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2007, Vol. 3, Issue 2, pp. 125-137..

[2] S. A Ashan Rajon and Ali Zaman, "Implementation of E-governance : only way to build a Corruption-Free Bangladesh, Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008), 25-27 December, 2008,

[3] Grossman, R. L. The case of cloud computing, proc. of IEEE ,Educational Activities Department, Piscataway, NJ, USA vol. 11, Issue 2, pp. 23-37, March, 2009.

[4] "Cloud Computing for E-Governance" A white paper, IIIT Hyderabad, India.

[5] M. Pokharel, and J. S. Park, "Cloud Computing: Future solution for e- Governance," Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance, ACM Press, New York, NY, 2009, pp. 409–410.

[6] K. Mukherjee, G.Sahoo, Cloud Computing: Future Framework for e-Governance, International Journal of Computer Applications (0975 – 8887) Volume 7– No.7, October 2010

[7] M.K.Sharma, M.P. Thapliyal G-cloud (e-Governance in cloud), Int J Engg Techsci Vol 2(2) 2011,134-137.

[8] W. Cellary, and S. Strykowski, "E-Government Based on Cloud Computing and Service-Oriented Architecture," Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance, ACM Press, New York, NY, 2009, pp. 5–10.

[9] Chihyi Yeh, Yiying Zhou, Hao Yu, Haiyan Wang, Analysis of E-Government Service Platform Based on Cloud Computing, 978-1-4244- 7618-3 /10/$26.00 ©2010 IEEE.

[10] Aprna Tripathi, Bhawana Parihar, "E-governance challenges and cloud benefits" , 978-1-4244-8728-8/11 ©2011 IEEE.

[11] Ajay Prasad ,Sandeep Chaurasia, Arjun Singh, Deepak Gour "Mapping Cloud Computing onto Useful e-Governance" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 5, 2010.

[12] Anttiroiko, A. V. (Ed.) Electronic Government: concepts,Methodologies, Tools, and Applications. Information Science Reference, Hershey, PA, 2008.

[13] Coursey, D. and Norris, D. "Models of e-Government; Are they correct? An empirical assessment" , Public Administration, Review, volume 68, Number 3, pp 523-536, 2008

[14] D.C. Wyld, The cloudy future of government it:Cloud computing and the public sector around the world, International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, January 2010.

[15] D.C. Wyld, Moving to the cloud: An introduction to cloud computing in government. Washington, DC: IBM Center for the Business of Government, November 2009.

[16] Grant, G., and Chau, D., "Developing a Generic Framework for E-Government", Journal of Global Information Management, Volume 13, Number 1, pp 1-30, year 2005

[17] R. Hicks, "The future of government in the cloud," FutureGov, 6(3), pp. 58-62, May 2009.

[18] P. Sumathi, Punithavalli M, "Constructing a grid simulation for e-governance applications using GridSim" Journal of Computer Science 4 (8): 674-679, 2008

[19] K. Mukherjee, G.Sahoo, "Security mechanism for C-Governance using Hadamard matrices" Proceedings of 2nd International Conference on Computer and Communication Technology (ICCCT), 2011

[20] Lianzhong Liu and Jingfen Gai, "A New Lightweight Database Encryption Scheme Transparent to Applications" , The IEEE international conference on Industrial Informatics ,DCC Daejeon, korea, july 2008

[21] R. Agrawal, J. Kiernan, R. Srikant, and Yirong Xu, "Order Preserving Encryption for Numeric Data," *In the Proceedings of the ACM SIGMOD*, pp. 563-574, 2004.

[22] H. Hacigumus, B. Iyer, Chen Li, and S. Mehrotra, "Executing SQL over encrypted data in the database service provider model," *In ACM SIGMOD Conference*, pp. 216-227, 2002.

[23] Tingjian. Ge and S. Zdonik, "Fast, Secure encryption for indexing in a column-oriented DBMS," IEEE 23rd International Conference on Data Engineering, pp. 676-685, 2007

[24] Jamil T, "The Rijndael algorithm" , potentials, IEEE Volume: 23, Issue :2, 2004.

[25] Microsoft windows Azure. Http://www.microsoft.com/azure/