An Approach to ICT Enabled Solution Architecture for Critical Social Security Issues and Challenges for e-Governance

W. Jeberson, Gurmit Singh and T. Mohanadhas

Abstract*— *Across the globe, countries have recognized Information and Communication Technology (ICT) as an effective tool in catalyzing the public services activity for efficient governance, and in developing human resources. There is a lot of growing recognition of the newer and wider possibilities that technology presents before society in the modern times. ICT has brought about unprecedented changes in the way people communicate; conduct business, pleasure and interact socially. The evolution of new technologies and e-Forms of applications makes the lives of the people better and more comfortable in several ways. With the emergence of ICT, technology is totally utilised as a tool for good governance, sustainable development, globalization of the economy and social empowerment. Information is also a key element of democracy. This paper attempts to provide a total solution architectural framework which enhances the potential for e-Governance in tackling some of the social security issues and challenges, which are hindering the growth process for extension of e-Governance activity, if not eliminate the entire present problems.

***Keywords*— ICT (Information and Communication Technologies), e-Governance, Security, Digital Divide.**

1. INTRODUCTION

With the advent of IT, it has become possible for the common person to access global information. Now, villagers can access information in their local language, thanks to Unicode, local language technologies, semantic technologies and related products and tools. The Internet has become the network for bridging the gap between citizens and governments while the Intranet bridges all central governmental organisations. However, the security of the Internet and Intranet based applications has not improved to reflect its use as a mission-critical infrastructure component. It is clear that Internet enabled applications are essential for delivering services to civil society with infrastructural capability even to tackle disaster and crises effectively.Various approaches are applied in support of privacy, security and trust in e-Governance for enhancing the G2C service delivery mechanism. These are public key cryptography (PKC) and public key infrastructure (PKI) including digital signatures developed for secure G2C transactions.

There are various reasons for the lack of e-Governance progress. To some extent, these may be due to technical issues, regulatory issues and economic issues that are very hard to eliminate. Lack of e-Learning tools and translation of contents affect the penetration of e-Governance to rural areas. Government departments have not fully attempted to computerize their back-offices to throw open the service deliveries to public. Many a times, departments are offering front-end services, which are more error-prone and problematic. Government Process Re-engineering and related reforms and regulatory frameworks are yet to mature enough to allow true e-Governance in place.

This paper discusses various issues pertaining to the hindering growth process of e-governance. Some of the issues discussed are related to e-government initiatives, organisational barriers, technological barriers, socio-cultural barriers, data and information barriers, privacy and security barriers, social security issues in e-government, identity theft and identity fraud, fraud in online payments and disparities in access of information systems.

2. ISSUES IN E-GOVERNMENT INITIATIVES

Almost all countries are facing lot of barriers [1] and security issues, which hinders the growth process of effective e-governance initiatives. Let us explore some of the areas where there are barriers.

2.1. Organisational Barriers

Since e-governance is a client-centered approach, it has to face lot of critical organizational challenges. The e-governance is purely for the citizens and government employees. It works in different way comparable to traditional service delivery mechanism by which the services are delivered to the citizens with the help of Information and Communication Technologies (ICT)[3].

The delivery of electronic services forces governments to change their organisation. The external objective of e-government is to satisfactorily fulfill the public's needs and expectations on the front office side, by simplifying their interaction with various on-line services. In the back-office, the objective of e-government is to facilitate a speedy, transparent, accountable, efficient and effective process for performing government administration activities. Real cost of the e-governance is only realised when there is a true integration between the front-end and the back office systems. Achieving this end-to-end

W. Jeberson (corresponding author) and Gurmit Singh are with Dept. of Computer Science & Information Technology, AAI-DU, Allahabad, India -211007. Phone: +91-9452248375; E-mail: jeberson@rediffmail.com, gurmitsingh3@rediffmail.com.

T. Mohanadhas is with National Informatics Center (NIC), Bangalore, India. Email: tmdhas@gmail.com.

integration requires administrative reforms, development of new skills, and redesign of traditional processes. Implementing the necessary changes is a complex process for governments with transparency.

2.2. Technological Barriers

To develop a technological infrastructure first there is a need to design and implement the technical components that are necessary to realise the architecture. In introducing an adequate technological infrastructure, governments should aim at a full ICT alignment to all the government entities, which integrate national level, state level and local level governments. Some of the technological divides are as follows:

- The environment of the government departments and private departments are heterogeneous.
  - Multiple operating systems such as Windows/Linux /Macintosh
  - RDBMS such as Oracle/Sybase/DB2/SQL Server
  - Front ends such as VB/FoxPro/VC++
- The environment in the State/Central data centers are unified architecture so not possible to integrate all the information systems from various state governments.
- Some government departments have legacy systems that are not in a situation to obey the Data center standards.
- Network systems are poor in the sense of performance and bandwidth to enable latest technology infrastructure to the entire public in the nuke and corner of the country.

Therefore, throughout the country all the governments should co-ordinate to have a unified technological architecture.

2.3. Socio-Cultural Barriers

Cultural resistance is the greatest obstacle to integrated on-line public services. There are bureaucratic procedures, which hinders the implementation process of e-Governance. Indeed the most perplexing problems are usually created because of the political affairs and customary restrictions in the country. If these issues get the kind of consideration among public, then implementing e-government programs will be a much-complicated exercise[8].

2.4. Data And Information Barriers

Citizens, employers and the employees tend to see the public sector as one single institution. However, this view changes when they have to provide different government institutions with the same information. E.g. For the case of passport and driving license, separate application forms with almost same information are to be given. This problem is caused by the fact that public institutions do not share their data to one another. Another case in point is the different databases created and used by Central Election Commission and State Election Commission.

All the state governments use their own languages for the user interfaces and the way they are stored in database. If there is a need of reference of this data by other state government, it is not easy to translate to the respective local languages. Citizens face difficulties like in the case of a Ration Card transfer from one state to another state with each state making it mandatory to have their data in respective local languages.

Therefore, there is a need of a new kind of infrastructure to integrate data, one that conforms less to existing government boundaries.

2.5. Privacy and Security Barriers

E-government will only succeed if the customers have full trust in all the backend processes of e-governance. Without trust, e-government will never reach its full potential.

The privacy and security issues are at the core of a trusting relationship between governments and citizens. This is understandable and known the importance and sensitivity of the information governments collect from citizens.

Privacy and security issues drive or drag the information economy. Without sufficient protections, there will be no consumer-confidence in e-government. Governments need to reassure the public that e-government is safe and secure for users. The credibility for e-government is certainly more if there is more consistency in violation of security and privacy policies by information systems.

3. SOCIAL SECURITY ISSUES IN E-GOVERNMENT

E-government changes the face of social security [1] in an immense way. Citizens and employers will receive information with confidence from the government if the new services delivery mechanism developed with reputation and credibility of the social security of an organisation[7]. That may of course increase the standard operations cost. It introduces radical changes in the processing of claims for benefits, the assessment of workers' entitlements and the payments of benefits, all of which will be administrated by the new information systems designed to strengthen the processes requiring client attention while, at the same time, reducing the paper work to complete these processes[8]. Few of the security issues discussed below

3.1. Identity Theft and Identity Fraud

Identity theft and identity fraud are emerging issues that arise both in the security and in the economic crime context. Identity theft and identity fraud have flourished in recent years. Public is in fear of economic and other risks prompted by this problem. A search for new security features on identification cards and other smartcards, which provide the basis for many commercial transactions and interactions with government. Identity and confidential information given to the governmental organizations by public oozes in the hands of frauds or criminals, which may leads to destructive effects to public and less confidence of government ICT based services among public.

3.2. Fraud in Online Payments

A troubling aspect is that ICT and electronic commerce now becoming viewed as increasingly susceptible to misuse, especially in the case of online payments over the Internet. There appear to be mounting risks associated with data confidentially, availability, integrity, and Consumer & merchant authentication. Problems not only give rise to direct costs for firms and individuals, but also indirect costs associated with loss of flexibility, goodwill, market positions, strategic opportunities, etc. To a major extent, the issue boils down to a need for ensuring privacy and security, that leads to lingering subtle values of trust among public. Addressing these concerns is likely to be of great importance for the ability of the world community to realise the potential virtues of ICT. However, the risks stretch further because the opportunities for on-line transactions gradually enter in more area, which may accumulate tremendous power in destructive hands, and may undercut confidence in legislation as well as prevailing market forces in non-digital spheres as well. A case in point is the use of 128-bit encryption by most of the payment gateways in the country when it is known that such encryptions have been broken long back [8].

4. DISPARITIES IN ACCESS OF INFORMATION SYSTEMS

Another challenge for e-government is disparities in computer access. This challenge includes two policy issues: the often-described "digital divide" and accessibility for people with disabilities. In the case of the digital divide, not all citizens [1] currently have equal access to computers, whether due to a lack of financial resources or necessary skills. While the placement of Internet-enabled computers in schools and public libraries is helping address this issue, these efforts are still progressing. Some observers point out that much of what governments do involves interactions with people least likely to have access: the poor, the elderly, language-limited persons, and the less educated. Similarly, supporter for the disabled observe that computers can present new obstacles for citizens such as the blind or physically impaired, which may require costly hardware or software for their computers, such as screen readers or oral controls, to be able to access online information and services. Such peoples require the resources in such a manner that makes them accessible using these tools.

5. PROPOSED SOLUTION ARCHITECTURE

Various approaches applied in support of privacy, security and trust in the digital world. In particular, public key cryptography (PKC) and public key infrastructure (PKI), including digital signatures [6], which developed for, secure Internet enabled transactions. There are various reasons for the lack of progress. To some extent, these may be due to technical nature, regulatory issues and economic issues, which are very hard to eliminate in this area.

There appears to be a need for new ways of gaining trust. Digital certification is one of those areas where many actors are busy to develop proprietary solutions. According to a survey made by Deloitte Touche recently, shows that 45 % of firms have some sort of PKI solution in place. Digital certificates can be provided for applications that are given in table .1 below to enhance the security level, if not eliminate the present problems

Table 1. Services with the potential to gain from use of Digital Certificates

e-Governance	Tax authorities, tax report, tax forms e-procurement e-Tenders e-Voting e-District
Bank Transactions	Internet Bank ATM Applications for sending payments Credit applications Recharge of Cash Cards e-trade/e-commerce Cross border Payments
Other	Secure Communication Health Care Education/Exams Knowledge transfer Invoice applications Legally valid certificate like birth certificate position to represent

To fulfill the requirement of "non-repudiation", agreements must be clear and indisputable from the outset. For achieving global reach, the legal framework within each country, and the legal interpretation, need to be addressed. Many certificates are in place today because of various public and private initiatives. In most cases, however, they are primarily national in scope, and have limited geographical as well as sector-based validity. Most of the leading ICT adapting countries have still not adopted the use of digital certificates on a wide scale. Some of countries in Mekong Subregion (GMS), even though topper in technology development among other nations, an understanding of how to develop and implement solutions that rely on digital certificates is not fully developed for adopting it in e-governance. For digital certificates to be truly effective, they should work similar to a driver's license or passport, which is accepted wherever the person go. The certificate should be valid and easy to use.

A generalized multi purpose national framework for a national infrastructure that will enable strong authentication of users involved in electronic transactions [3]. A common bridge to enable the digital

certificate infrastructure to the entire country to link all central government organizations even to the global extent developed will satisfy one of the security requirements of "non-repudiation" in G2C service delivery models. Today, the issues are clearly a global one. The national infrastructure developed with highly available secured digital certificate management servers to serve the national framework throughout the country.

6. PROPOSED APPROACH TO ESTABLISH SECURITY INFRASTRUCTURE FOR E-GOVERNANCE

- All State government should follow a Common Security Infrastructure (CSI). Current State Wide Area Networks (SWAN) should be modernised of not to be developed to maintain the common security standards to satisfy the minimum needs of CSI.
- Digital Certificates are maintained and controlled within the National Cyber Security Authority (NCSA), which is a body formed for national security under ministry of defense. Other country and third party participation duly avoided in case of digital certificate.
- Public Key Infrastructure (PKI) should be implemented from the top level to the lower level of freedom in the e-Governance system infrastructure. The digital certificates should have adequate length to avoid frauds
- Unicode concept implemented using firewall protected Unicode servers, which should bridge in between national and state level infrastructure.
- National and state level datacenter enabled with digital signature, firewall and 24x7 availability with distributed database facility.
- Information superhighway (backbone network channel) for national level network should be developed for the communication of information with future ready large capacity bandwidth, which should support to at least next 100 years. (Statistical principles should be applied to find out future demand of bandwidth)
- Security priority levels developed by identifying the sectors with high-level risk to low-level risk and classified as higher, medium and low level. i.e. Defense, police, finance, will be classified under higher level. Business, Universities, Hospitals will come under medium level. Library, warehouse etc. will come under lower level. Based on the classification contingency planes should be developed for disaster management.
- Smart card should be given to citizens with integrated biometric identity (Technology should be developed to minimize the expense). Smart card issued to citizens in co-ordination with NCSA and the database should be centralised.
- NCSA appoints a high power rapid-action research and development group to analyse every day security threat and to take the contingency plan quickly to resolve the problem.
- NCSA develop an independent certification authority for the interoperability of PKI and facility developed for every department and agency to entertain the PKI facility.
- The proposed model of security infrastructure will interconnects all the critical infrastructure services at international, national, state level and local level through the security infrastructure enabled by authorization policy and security technologies.

7. SOLUTION ARCHITECTURE MODEL FOR E-GOVERNANCE IN GREATER MEKONG SUBREGION (GMS)

The solution architecture is a generalized architecture provides all the basic information about how the Information and Communication Technologies (ICT) utilised to enable the technology framework for e-Governance integrating all the levels for Governance to provide services to citizens with security. Fig. 1.0 explains the solution architecture for secured e-Governance. All the state governments are insisted strictly follow the norms of generalized architecture and standards to make the integration of state government with central government to fill the gap of information divide so that the services to the citizens can be delivered to their doorsteps without any inconvenience.

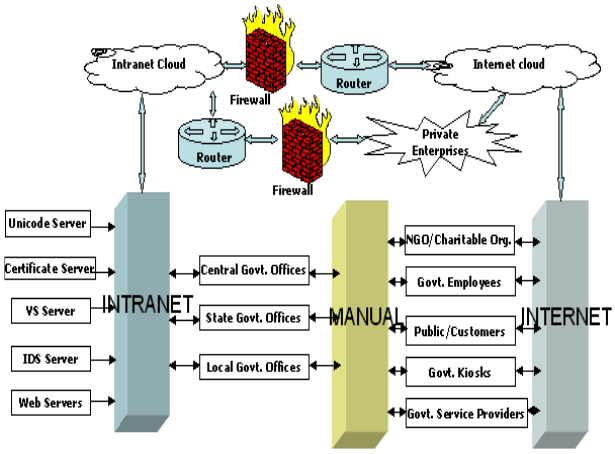
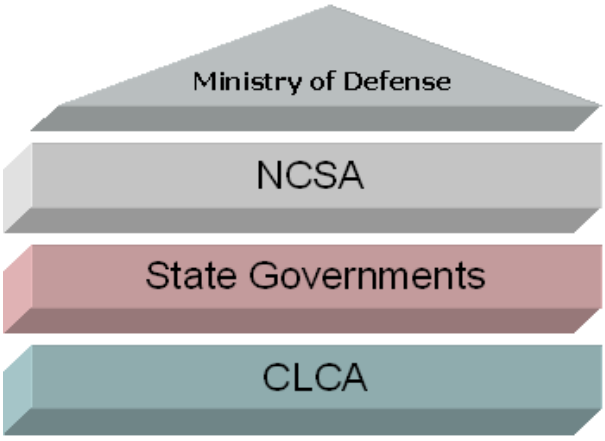


Fig.1.0 Solution architecture for e-Governance

- Central, State government offices and organizations were interlinked [3] by an intranet through security layer which will act as the backbone information superhighway for the entire Thailand.
- Central, State and Local government may do some activities manually or partial electronically e.g. Electricity, water spot billing. Data collected during manual operations are transferred to the Local Area Network (LAN) based systems, which are directly stored in remote databases under intranet framework for further processing. Some of the services were delivered to the customers/Government employees / public manually by the government offices (e.g. Universities send the mark list, degree through post) but at the same time services were available through internet also e.g. Result, marks of exams were available in internet or by voice response system or VOIP through telephone system.

- The intranet backbone network linked with Local, Central and District level datacenter through security layer will work with 24x7 architecture.
- For exchange of data from state government to central government with multilingual compatibility Unicode server should be maintained for the interchange official language to any other desired language. Central government should form an authority for regulation of linguistics as Central Linguistics Control Authority (CLCA). All state level governments should take initiative steps to develop Unicode for their own language with the guidance from the CLCA.
- Storage Area Networks (SAN) developed with generalized security architecture to store centralized data are enabled with Intrusion Detection System. Data from State, Central and Local governments will be stored in various levels of datacenters. The datacenter should include security layer to protect intrusion of hackers and unauthorized users to access data. Certified and authenticated users only allowed fetching data. PKI implemented in SAN datacenters.
- For online financial transactions, digital certificate based security is enabled to have a smooth hassle free transactions.

The above said architecture hierarchy is pictorially explained in figure 3.



NCSA- National Cyber Security Authority
CLCA- Central Linguistics Control Authority

Fig. 3. National security flow hierarchy diagram

- For Disparities in access of information systems, there is a need of initiating awareness among the public by the joint effort with NGOs and education based governmental bodies. Improving the literacy rate will thrive lot of changes among public. Indeed this process is a time consuming process to implement. For peoples with disabilities government can initiate the respective welfare organisations (e.g. Blind Federation, Deaf Federation) by funding to start training programs to train such disabled peoples with special electronic accessibility devices specially designed to access the information systems for that types of peoples that may be enabled with voice recognition etc. for their need. Thus the gap of the digital divide can be reduced drastically to have a better future.

8. SECURITY INFRASTRUCTURE FRAMEWORK FOR GREATER MEKONG SUBREGION (GMS)

To enable improved security and privacy there is a need to secure the entire network of e-Governance with multilayered security model. This approach will cover the entire system, which provides security for every layer in OSI model so that consistency in security of entire network of e-Governance from physical layer to presentation layer is applied. To enable this multilayered security [2], the layers logically organized into three levels by grouping some of the layers in each logical group, which are named as follows:

The Network Security Layer provides security functions at OSI layers 1 to 3 (physical to network layers)[2].

The Network-Assisted Security Layer provides security functions at OSI layers 4 to 7 (transport to application layers) [2]

The Application Security Layer provides security in layer 7 of the OSI model [2]

Security functions such as VPN, VLAN (Virtual LANs), port security, IP security, encryption and secure dynamic routing operate purely at the Network Security Layer. Others such as fire walling, intrusion detection, SSL encryption, content filtering and virus scanning operate at either the Application security layer or Network-Assisted Security Layer. Thus by enabling the multilayered security in a structured fashion the security can be tightened overall in the e-Governance communication networks and in service delivery mechanisms.

The following general principles are to be followed to enable the security infrastructure for e-Governance in Greater Mekong Subregion (GMS) countries:

- Use a uniform access management system for entire network that enabled in central, state and local government level with the appropriate level of authentication and resource access authorization to meet the basic security standards.
- Use of e-Governance standards
- Use of Standards like Web 2.0, e-Forms etc.
- Use a **centralized authentication** mechanism to facilitate administration and remove the need for locally stored passwords. Figure 2 explains the model of centralized authentication system.

Authentication systems are used to ascertain identity. There are various types of authentication in present scenario they are (i) Single-factor authentication uses user ID /password combinations to prove identity.(ii) Two-factor authentication requires two components, usually a combination of something the user knows (such as a password) and something the user possesses (such as a physical token Secure ID card). (iii) Three-factor authentication adds a biometric, a measurement of a human body characteristic [4].

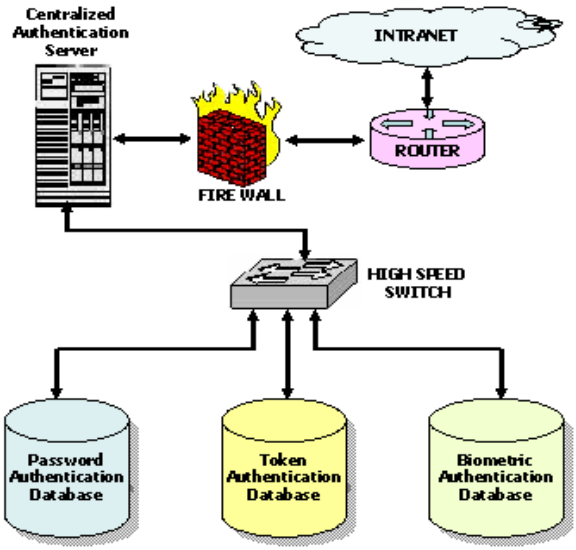


Fig. 2. Model of centralized authentication system

• Use a **centralized authorization system**, tightly coupled with authentication system, with appropriate granularity for the enterprise [3].

Once authenticated, authorization mechanisms control user access to appropriate system resources. Authorization can be categorized according to the granularity of control. Authorization is often "role based" whereby access to system resources is based on a person's assigned role in an organization. The System Administrator role may have highly privileged access to all system resources whereas the General User role would only have access to a subset of these resources. Authorization may also be "rules based" whereby access to system resources is based on specific rules associated with each user, independent of their role in the organization. For example, rules may be set up to allow Read Only access or Read/Write access all or certain files within a system, or access only during certain times or from certain devices.

• Enforce strong, complex rules for all passwords.

The Single Strong Password system enforces strict password rules. For example, passwords must contain at least eight characters, both upper and lowercase letters, and at least one number or symbol. Additionally, passwords must not contain dictionary words of four characters or longer, a previously used password, a password that matches an account name, contain a date or year, keyboard patterns, or repeating characters. Users are required to change passwords at predefined intervals.

• Securely store all passwords in encrypted standard format.

• Securely log or record authentication and authorization events for audit purposes.

9. CONCLUSION

The New approach and solutions would enable the true empowerment of both government employees and public of Greater Mekong Subregion (GMS) Countries best practices and the guidelines given will improve the credibility and reliability of the e-Governance service delivery mechanisms among the public. No system connected to the Internet is safe from attack but the solution architecture provided will reduce drastically the frequency of attacks in the network if not eliminate the entire attack and increase the confidentiality among the public. This paper gives a practical approach providing coverage for the multi-dimensional facets of e-Governance in terms of social security and challenges of Mekong Subregion (GMS) based countries. The solution architecture along with appropriate e-Governance standards for Meta Data, Security, Systems Development, language technologies, etc. would pave the way for new generation e-Governance practices.

REFERENCES

[1] Wikipedia, the free encyclopedia (2007). Information_Age. Retrieved on 03 September, 2007 from the World Wide Web: http://en.wikipedia.org/wiki/Information_Age#Information_Economy

[2] Nortel Networks, (2004). Unified Security Architecture for enterprise network security", June 2004.

[3] Mittal, P.A. et al. 2004. A framework for eGovernance solutions.

[4] Oxenhandler, D. 2003. Designing a Secure Local Area Network

[5] Zwahr, T. and Finger, M. 2006. Enhancing the e-Governance model: Enterprise Architecture as a potential methodology to build a holistic framework

[6] Wikipedia, the free encyclopedia (2007). Information_and Communication Technologys for development on 12 October, 2007 from the WorldWideWeb http://en.wikipedia.org/wiki/Information_and_Communication_for_Development_(ICD)

[7] Kabeer, N., Sharma, A. N. and Upendranadh, C. 2006. Social Security in South Asia: Issues and Perspectives.

[8] Verstraeten, J. 2000. International Conference on Information Technology in Social Security procedings.