Information and Network Security Aspects in E-governance Framework Some Issues and Recommendations

Durgesh[1] and M.K. Sharma[2]

***Abstract* --The role of ICT in the public sector has changed dramatically over the past decade. The evolution of e-governance started with governments putting information into portals. e-governance strategies has changed in last 10 years with the new trends like some governments adopting Private Public Partnership (PPP) arrangements as is the case of Hong Kong ESDlife. e-governance has evolved to the point where governments are not only providing information directly to citizens, businesses and other governments; they are also Usertrust is a key factor for e-government projects. Any ICT infrastructure must be secure because citizen and business transactions contain significant confidential information. Secure network and identity authentication and verification technology must be in place together with privacy laws and governance to ensure privacy and confidentiality is protected. Finally, the ICT infrastructure must be reliable. The network, applications and processes must be reliable to ensure availability and integrity of the e-government services. Network and Information security is a major concern.involved in implementing e-governance projects. problems in ICT like hacking, virus, spamming, invasion, privacy issues can evolve from lack of security measures. Governments need to provide secure access to information, applications and services via networks. In this paper we will discuss various security needs of electronic systems like e-governance and e-commerce. We would discuss in detail various security mechanisms to address various threats. In this paper we will discuss about some intelligent security system based on mobile agents and forecasting mechanism. We will also discuss a few products existing in the market. There are many security related issues when we talk about e-governance. E-governance projects handle sensitive and important data. In e-governance there is a trade off between security and availability. Security rules are too harsh or too soft and tuning it as per the demand is necessary. We will also consider various options that can lead to better and secured e-governance. In this paper we will cover need and tools of forecasting security needs and rule setting for the same and how it can contribute in resolving security issues in e-governance.**

***Keywords*--e-governance E-voting Informationsecurity Mycad Securenetwork Securitythreats**
1

I. Introduction

ICT is a significant enabler of successful e-governance projects, and can be a new approach for touching the lives of the common man anywhere, any time. We need the technology and strategies for better e-governance initiatives that are benefiting the masses. 2

The Indian central and various state governments are no strangers to the benefits of using ICT for e-governance. Many state governments and government based agencies have realized that ICT can add substantial value by surmounting the usual challenges of distance, slow speed of operations, and lack of accuracy of information. 3

The Department of Revenue (Karnataka), National Crime Records Bureau, National Highways Authority of India, Konkan Railways, IRCTC and the governments of West Bengal, Punjab, Haryana and Uttarakhand have been using ICT to empower their activities .

India has 600,000 villages. 70 percent of Indians live in villages, and 95 percent do not speak English. Therefore, e-governance models which do not support the rural delivery system will not contribute much for a good governance. Therefore the goal of e-governance should be in a direction, which can benefit rural India and should act as bridge to fill the gap of urban and rural India.

A. What is e-governance ?

Ravi Kant, Special Secretary, IT, Government of West Bengal, likes to describe e-governance as the use of information and communication technology (ICT) to enhance information access and the delivery of government services for the benefit of citizens, business partners, organizations and government functionaries.

“e-governance, however, is not really the use of IT in governance but as a tool to ensure good governance. e-governance does not mean proliferation of computers and accessories; it is basically a political decision which calls for discipline, attitudinal change in officers and employees, and massive government process re-engineering,”

The Indian Government has about 60 departments such as Agriculture, Industries, Health, Education, Social Welfare, Employment, Taxation, Finance, Pensions, etc. Thus, we

[1] Dr. Durgesh, Reader and Head , Department of Computer Science , Kumoun University , Nainitaal (Uttarakhand)

[2] M.K. Sharma Senior Lecturer , in Department of Computer Science , Amrapali Institute Haldwani (Uttarakhand).

can see that applying ICT processes, to improve the efficiency, speed and transparency, ease of use and lowering of the costs providing anywhere, any time services to the citizens and the businesses is very much essential but not an easy task. e-governance therefore is a very complex mission.[2]

B. e-governance models

Some popular e-governance models are :

1. Broadcasting/Wider Dissemination model
2. Critical Flow model
3. Comparative Analysis model
4. Mobilization and Lobbying model, and
5. Interactive Services model

II. Why Securing e-Governance?

As India adopts e-governance with a vengeance, the need for Network and Information security measures to protect vital data will be a major part of e-governance framework .

To design an e-governance framework, security has become a key issue that needs to be addressed. Like any other on-line project, an e-governance project needs a network to execute, but the major difference is that in an e-governance project considerable amount of critical information could be involved. Hence the need for securing such information is must.

Security is critical in e-governance to safeguard the confidentiality of transactions and information on the network. Government documents and other important material such as birth and death registration, motor vehicle license, land records, all of which have legal and legislative nuances have to be protected from unauthorized users in case of e-governance projects. Hence, security is critical for their successful implementation. [3]

A. Where Securing e-Governance

Security measures are required wherever ‘authenticity,’ ‘validity,’ and ‘legal rights’ of digital content have to be protected from repudiation. All digital content in form of applications that need protection from tampering, vandalism, decay and accident need security .

The role of network or information security is vital in every application, which collects or stores data, interacts with an outsider, carries some confidential information and other applications online and the best example of having most of such qualities and requirements are e-governance projects.

In some online application we need transition of money, such as banking, shopping, gambling and gaming. In e-governance framework central government can transfer a huge fund to state government online. With the Information Technology (IT) Act, 2000 coming into effect from October 18, 2000, transactions on the Internet have got legal validity in India [4]. This allows users to pay their bills for utilities on the Web, at least on paper. All these applications handle money transactions whether it is transferring money through the online bank or using credit cards. Either way, they’re interesting targets for criminals. It may be either through phishing scams, trying to fool the users to give away financial and personal information or it may be through Distributed Denial of Service (DoS) attacks. Either way, online transactions and their users are at a higher risk of getting targeted by digital attacks.

III. Security Threats

The complex network and large size e-governance framework make it most vulnerable for the virus, spam and Trojan attacks. A lot of intrusion attempts can be there to crack the security, in that network and information security is a greater challenge. With out having a proper security architecture the e-governance framework will face many security threats of a diverse nature.

In such a complex environment like e-governance project we need complete information security architecture. The architecture need to be further complemented with proper tools and solutions to keep itself away from any threat both at the network level and at the host level.

Once a virus attack is detected, everything comes to a standstill. Until the entire thing is cleaned up, work doesn’t move further. “When there was an intrusion at network or host level, it took a long time to cure and a huge loss of money can be there. There were some inherent vulnerabilities like Web defacements, stealing of information etc.

Table 1: Financial cost of downtime of network because of security threats per hour

Industry	**Application**	**Average cost per hour of downtime (US$)**
Financial	Brokerage operations	$7,840,000
Financial	Credit card sales	$3,160,000
Retail	Home shopping (TV)	$137,000
Transportation	Airline reservations	$108,000
Entertainment	Tele-ticket sales	$83,000
Shipping	Package shipping	$34,000
Financial	ATM fees	$18,000

Source : Contingency Planning Research, 2002

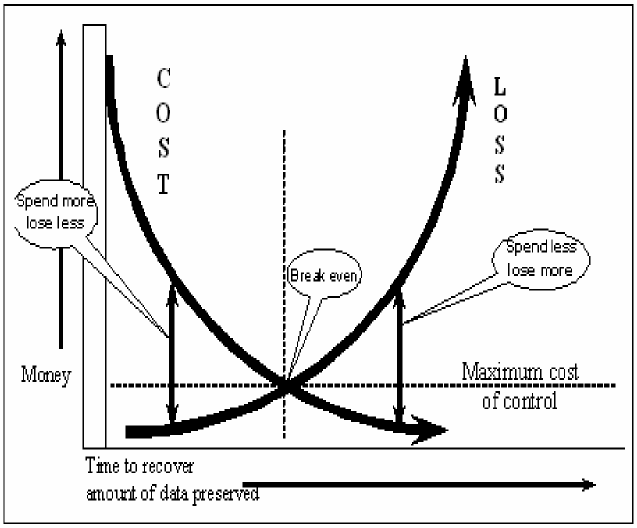

Figure 1 : Comparison curves for cost paid for security measures Vs Loss

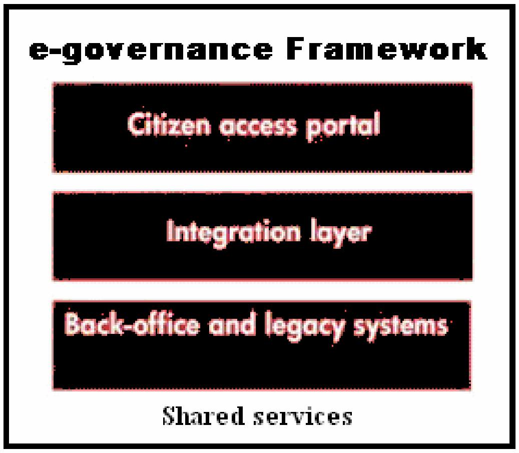

Figure 2 : e-governance Framework

IV. E-GOVERNANCE FRAMEWORK

One of the pillars of the e-governance framework is a set of shared services that allow agencies to share key parts of their infrastructure, applications and business processes within the agency, with other branches of government and with citizens. Shared services may include improved security features for e-mail, geographical information systems, electronic funds transfers, government directories, citizen databases, disaster databases, business databases and large data centers.

A. information management life cycle in e-governance framework

We can offer and deliver many services using a e-governance framework, some of them are:

1. Single and Multiple department Transactions
2. Private correspondence of documents to Government
3. Change of Personal status
4. Employment Application
5. Information Search
6. Electronic voting
7. Interdepartmental requests
8. Granting permission to access services
9. Enrollment/ Revocation of Government employees
10. Fraud Investigation
11. Access to e-Government services under delegated
12. Government to citizen services

Before start to offer all that service we need to collect and process lot of information. For that a predefined system is required.

B. Information management life cycle

1) *Collection*

Gathering data on citizens, businesses and other entities.

2) *Storage*

Gathered data is stored for processing.

3) *Processing*

Processing takes place at many servers level.

4) *Communication*

Data collection and processing require a lot of Government to Citizen (G2C) and Government to Business (G2B) communication to happen.

In this life cycle, each stage above carries security risks and on each stage we need a security of network [4] as well as of information.

C. e-governance Service Attacks and Threats

- Unknown Outsider Attack
- User Fraud
- Insider Attack
- Privileged Insider Attack
- False Identity
- Impersonation
- Unauthorized Disclosure
- Revoked rights
- Theft of Access Tokens
- Duplication of Access Tokens
- Denial of Service Attacks
- Misinformation and Propaganda
- Breach of Anonymity
- Breach of Accountability
- Failure to Recover Business Information
- Theft on Monetary value

V. Security solutions market

Anti-virus (AV) and firewalls occupied the largest market share in the security appliances business. However, the concept of a self-defending and self-healing network increasingly brought intrusion detection and protection (IDP) solutions to the forefront. While anti-virus and firewalls are seen more as reactive security mechanisms, IDP solutions are more proactive and get activated as soon as any abnormal behavior is detected. Next table will help us to find the name of some vendors, from which we can get security solutions.

TABLE 2 : LEADING SECURITY PRODUCT VENDORS

Product Category	**Key vendors**

TABLE 3 : TOP MARKET LEADERS IN NETWORK SECURITY

Anti-virus	Trend Micro, Symantec, Network Associates, MacAfee
Firewalls	Cisco, Checkpoint, Juniper, Nokia

A. *Security monitoring tools*

If we look at the e-governance projects and the networks that are being rolled out for these, network or information security seems to be paramount. In an e-governance project, a substantial amount of documentation is being done like maintenance of land records, police records, court judgments and so on. Each department functions independently and has its own set of transactions to undertake. Hence having security measures in each department is critical so that only authorized people get into the network and access the information.[5]

The importance of security is high among industry and government, but the awareness is low. An understanding of the security technology and the need for its implementation is required for a safer and more secure IT environment in the country. Securing public data and ensuring security of the government Web sites are some applications where security solutions or monitoring tools are required. Some common processes of those tools are:

1) *Vulnerability Assessment*

Network and information security assessment services review all aspects of the data and voice networks and provide recommendations to maximize security, reliability, and availability. Following can be deliverables:

- Identification of vulnerabilities that need to be immediately addressed
- Verification of security products and features already in place
- Prioritize security projects for future implementation
- Assess the real-world threat to network assets

Rank	**Players**	**Revenue (Rs crore)**	
		2004-05	**2003-04**
1	HCL Comnet	16	8.5
2	Datacraft	12.5	8.4
3	Wipro Infotech	8.4	6.5
4	GTL	5	2.4
5	Secure Synergy	4	-
6	Ramco	2	-
7	Network Solutions	1.5	-
	Others	10.6	9.6
	Total	**60**	**35.4**

2) *Security Policy Development*

Any security policy must satisfy working objectives as well as the technical aspects of securing e-governance information. Part of developing a secure network is crafting a set of organizational security policies. These policies establish the rules and guidelines that system and network engineers can use when deploying solutions. This policy would then guide how network engineers install and configure firewalls, intrusion detection systems and other network equipment. Developing a useful, practical, and feasible network security policy document can be very time consuming, especially if you are unsure about all the possible technical and practical implications of certain decisions[6]. Some automated tools like Coleman Technologies, Inc. Managed Services tools can help any organization to develop and deploy a comprehensive security policy.

3) *Wireless Network Analysis*

Wireless networks are inexpensive, simple to deploy and very attractive for an increasingly mobile workforce and can be helpful to provide e-governance service in rural or remote areas. Unfortunately, wireless access points are designed for ease of use, not security. A thorough risk analysis provides an option for prioritizing and justifying future security expenditures. Depending on the scope of the risk analysis, the project may involve assessing sensitivity, criticality, threat, vulnerability, and susceptibility to penetration.

4) *Successful Identity Authentication*

Protecting access to electronic resources is not a simple process. Internet is a standard medium for conducting operations in e-governance framework, within and without organizations. At present, there is a need for secured identity authentication, verification, and protection technology within all industries. Tools like NIPP Secure ID™ [7]consists of a comprehensive set of proven biometrics technology compatible with various applications. This solution allows authentication and validation of any type of transaction in Government Agencies, Companies, Medical and Financial Institutions, Banks, and Judicial Levels of any other companies.

VI. Case Studies

A. E-voting

The ultimate test of e-governance security and privacy may be electronic voting. In contrast to the obstacles of paper-based elections, e-voting allows citizens to vote via mobile device or electronically at a polling station. In Madrid, HP and Scytl teamed up for two electronic referendums in 2004. Approximately 135,000 citizens of Madrid voted on local issues via the Internet and mobile phones in an event that became Europe’s largest e-participation experience to date.[8]

B. MyKad

Since 1999, the Malaysian government has begun gradually phasing in a multi-purpose national ID smart card, that it intends all Malaysians to adopt by 2005.[9] The card, known as **"MyKad**," incorporates both photo identification and fingerprint biometric technology and is designed with six main functions: identification, driver's license, passport information (although a passport is still required for travel overseas), health information (blood type, allergies, chronic diseases, etc.), and an e-cash function.[10] The card can also function as an ATM card, although it is MyKad's least attractive feature and banks have discouraged customers from using the card for such purpose. There are plans for adding additional applications for digital signatures for e-commerce transactions.

Fig 3 : MyKad

VII. Conclusion

Many citizen who have facility or infrastructure to access online information, want the convenience of interacting with governments online, but they also need reassurance that the personal information they share can be safely guarded. The viability of e-governance projects ultimately depends on trust.

The information systems security research should be one of the visions of e-governance to concentrate in the next few years to develop security techniques, security technologies and products to be used for facing new challenges using open media for transactions pertaining to Government, Industry and Business covering commercial, financial and administrative aspects. The security requirements are of dynamic phenomena and not a static phenomenon. The security management is no longer technology oriented but management oriented for effective implementation as well as, ascertaining information and systems as an asset of the organization. The information assurance involves people, processes and technology. It has to be customized for every organization based on various requirements which are static and dynamic and depending upon the risk and challenges they are facing is conducting, managing and transacting businesses within the country and across the globe.

VIII. References

[1] Security Aspects of e-Governance and Intelligent Security System , Dr. Parag Kulkarni, Capsilon Research Labs, India
[2] Progress of e-Governance – an overview ,C. S. R. Prabhu,, Sr. Technical Director , National Informatics Centre
[3] MCA 21 (a project by the Ministry of Company Affairs)
[4] Securing e-Governance, digitally , Express computer , www.expresscomputeronline.com
[5] Network and Information Security Standards for e-Governance- An Approach Paper-by: T.M.Rao, Senior Technical Director, NIC
[6] '20 million M'sians to get smartcards' ZDNet Asia, 6 September 2001
[7] 'PKI International Scan - April 2003' Public Works and Government Services, Canada, April 2003
[8] 'Malaysia's national smart card underused: Report', ZDNet Asia, 11 July 2003
[9] 'MyKad with 8 applications, but its full potential has yet to be explored' Jaring Internet Magazine, Malaysia, August 2003
[10] 'Malaysia to fingerprint all new-born children' The Register, 4 May 2005

IX. BIOGRAPHIES

Dr. Durgesh Pant is working as Reader and Head , Department of Computer Science , Kumoun University , Nainitaal (Uttarakhand) . He has guided several Ph.D students .He has published several research papers .He is convener , Computer science courses of Kumoun University as well as member of Board of studies of several Indian universities . His area of interest and research includes Data compression , Algorithm analysis , Data warehouse & mining etc.

Mahesh K. Sharma (M.Tech , pursuing his Ph.D) is working as Senior Lecturer , in Department of Computer Science , Amrapali Institute Haldwani (Uttarakhand). He has 10 years experience of academics and industry . He is coauthor of 5 books and published international and national research papers . He is content author for Chaudhary Devi Lal University , Sirsa and Uttarakhand Open University Uttarakhand . He is active member of Computer Society of India and Special Interest Group for E-Governance