International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 5
ISSN: 2454-4248
101 –108

Comparative Analysis of E-Governance Models

Ms. Vani Jain
Research Scholar
Suresh Gyan Vihar University

Dr. Devesh Bandil
Supervisior
Suresh Gyan Vihar University

Sachin Jain
JNU, Jaipur

Abstract:- Online working of a government or providing its services online to its citizens at their access is known as E-Governance. E-Governance is E-Commerce tool means online accessibility of government services. The technology and the methods used in E-Governance plan provide a roadmap for well-organized delivery of services at the door step. In today's time the development of any country depends on the uses of E-Governance and also their dispersion Development of any country can be reviewed by the extent of E-Governance in that country. Moreover, today's government has also full confidence in E-Governance and its widespread network across the world proves it.

E-government security is a key problem to confine the structure and development of E-government systems in any country over the world. E-Government security models are broadly used in the implementation and development of e-government systems. Due to the deference situation of the countries over the world there are diverse security models applied in each country. . Based on this analysis, the security requirements of the data and the applications have been formulated in the form of security parameters like confidentiality, integrity and availability as well the access requirements of the roles.

The overall aim of this research is to review the available existing E-governance security models, find out their merits and demerits and analysis of the available models with respect of security in E-Governance. This paper discusses about the possible threats and vulnerabilities for different data locations separately for different models. Here data are considered for four states: data in store, data in process, data in transit and data in destination.

Keywords: *e-governance, ICT, e-government, information, security, etc.*

*****

I. INTRODUCTION

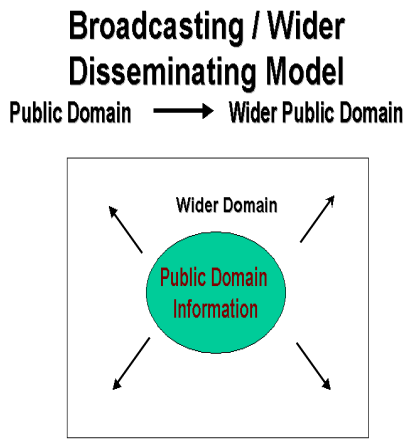
Models of e-governance are still evolving in developing countries. A few generic models have shaped up, which are finding greater recognition and are being replicated. These models are based on the inherent characteristics of ICT such as enabling equal access to information to anyone who is part of the digital network and de-concentration of information across the entire digital network, connecting all sources of information. In simpler terms, information does not reside at any one particular node in the Digital Governance models but flows equally across all the nodes. Hierarchy is inherent in the government departments. Therefore, appropriate administrative reforms and some re-engineering may be required before digital-governance may be really implemented. It needs to be noted here that these models of governance are fundamentally different from those which are popular in developed country due to differences in basic conditions, and perspectives and expectations from good governance. The five important models of e-governance, which can be used as a guide in designing e-government initiatives depending on the local situation and governance activities that are expected to be performed. These models are:

- The Broadcasting Model
- The Comparative Analysis Model
- The Critical Flow Model
- The E-Advocacy/Mobilization Model
- The Interactive-Service Model

1. Broadcasting model

- Broadcasting model is based on mass dissemination of governance-related information which is already available in the public domain into the wider public domain using ICTs.
- This raises awareness among the citizens about ongoing governance processes and government services that are available to them and how they can benefit from them.
- The application of this model using appropriate technologies could reduce the "information failure situations" where citizens are unaware of new and existing services being provided by the government. It can also provide as alternative channel to people to stay updated of governance related information and to validate information received from other sources.

 ISSN: 2454-4248
101 –108



Applications

- Putting governmental laws and legislations online
- Making available the names, contact addresses, emails, mobile numbers of local/ regional/ national government officials online.
- Make available information such as governmental plans, budgets, expenditures, and performance reports online.
- Putting key judicial decisions which are of value to general citizens and create a precedence for future actions online. viz. key environmental decisions, state vs. citizen decisions etc.

Merits

- It enhances 'access' and 'flow' of information to all segments of the society, which is essential to bringing good governance.
- Government can use this model to provide greater governance services to their constituencies, and to enhance the participation of citizens in governance processes.

Demerits

- The model can lose its effectiveness in societies, where the free-flow of information is not possible. This can happen in countries where freedom of speech and expression, or political freedom is restricted, or there are tight governmental controls to censor information.
- The model also loses its effectiveness in situation of optimal ignorance. This happens when citizens are indifferent / not motivated to act upon information available to them, or when governments and decision-makers take wrong decisions, not because of absence of information, but complete disregard of available information.

In this model data are for public use. So main security concern is to maintain the integrity of data. With this data must be available. Keeping in mind about the four locations of data mentioned above, security aspects, threats and vulnerabilities have been discussed in Table 1.

Table 1. Threats & Vulnerabilities of Broadcasting Model.

DATA LOCATION	THREATS	VULNERABILITIES
Data in Store	• Encryption cracking • System failure • Corruption / loss or damage of back up media • Brute force attack	• No Password • Using the same key for a prolonged period of time • Inadequate back up facility • Non adherence to back up policy • Minimum length of the password has not been enforced
Data in Process	• Loss of decryption keys • Theft of credentials • Cross-site scripting • Query string manipulation	• Using the wrong algorithm or a key size that is too small • Password is guessable • Using application-only filters for malicious input • Using non-validated input used to generate SQL queries Relying on client side validation
Data in Transit	• Encryption cracking • Brute force attack	• Using the same key for a prolonged period of time • Distributing keys in an insecure manner • Passing sensitive data in clear text over network
Data in Destination	• Denial of service attacks • Misuse of privileges	• Lack of monitoring of services and activities

 ISSN: 2454-4248
101 –108

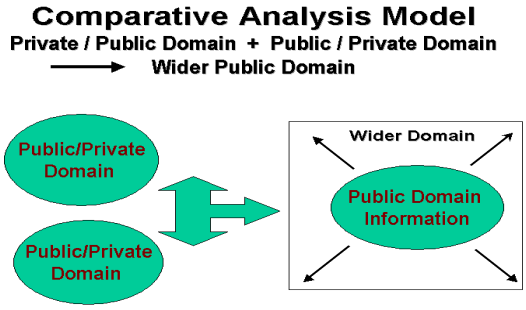
2. Comparative Analysis Model

Comparative Analysis Model is one of the least-used but a high potential e-governance model for developing countries. The model can be used to empower people by comparing cases of bad governance with those of good governance and identifying specific aspects of bad governance, the reasons and people behind them, and how the situation can be improved.

- The model is based on using immense capacity of ICT and social media tools to explore given information sets with comparable information available in the public or private domain.

- The model continuously assimilates "best practices" in different areas of governance and uses them as benchmark to evaluate other governance practices. It then uses the result to advocate positive changes or to influence 'public' opinion on existing governance practices. The comparison could be made over a time scale to get a snapshot of the past and the present situation or could be used to compare the effectiveness of an intervention by comparing two similar situations.

- The strength of this model lies in the infinite capacity of digital networks to store varied information and retrieve and transmit it instantly across all geographical and hierarchical barriers.



Applications

This model could be applied in the following possible ways:

- To learn from past policies and actions and derive learning lessons for future policy-making.
- To evaluate the effectiveness of the current policies and identify key learnings in terms of strengths and flaws in the policies.
- To effectively establish conditions of Precedence, especially in the case of Judicial or legal decision-making (example for resolving patent-related disputes, public goods ownership rights), and use it to influence/ advocate future decision-making.
- To enable informed decision-making at all levels by enhancing the background knowledge and also providing a rationale for action.
- To evaluate the performance and track-record of a particular decision-maker/ decision-making body.

Merits

- Developing countries could very effectively use this comparative model as ICT opens their access to the global and local knowledge products at a relatively low -cost.
- The model is very much based on the existing sets of information.
- There is a vast scope of application of this model for judicial advocacy as landmark/key judgments of the past could be used as precedence for influencing future decision- making. Further, watch-guard organizations and monitor-groups can use this model to continuously track the governance past record and performance and compare with different information sets.

Demerits

- The model requires the ability to analyse and bring out strong arguments which could then be used to catalyze existing efforts towards self governance.
- The model becomes ineffective in absence of a strong civil society interest and public memory which is essential to force decision-makers to improve existing governance practices.

In this model, data must reach to the targeted domain not to all. So confidentiality is great concern here. All possible security aspects, threats and vulnerabilities have been discussed in Table 2.

 ISSN: 2454-4248
101 –108

Table2. Threats&Vulnerabilities of Critical Flow Model.

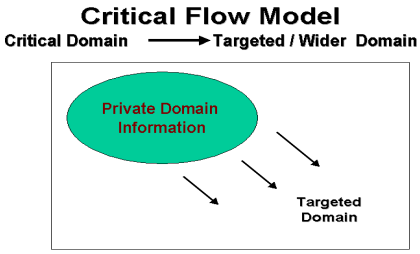
DATA LOCATION	THREATS	VULNERABILITIES
Data in Store	□ Loss of decryption keys □ Encryption cracking □ Denial of service attacks □ Misuse of privileges	□ Password is guessable □ Password sharing among the peer user □ Lack of monitoring of services and activities
Data in Process	□ System failure (Unavailability of information system) □ Corruption / loss or damage of back up media □ Brute force attack □ Impersonation □ Form field manipulation □ Cookie manipulation □ HTTP header manipulation	□ Failing to secure encryption keys □ Using the wrong algorithm or a key size that is too small □ Absence of back up policy □ Minimum length of the password has not been enforced □ Using non-validated input used to generate SQL queries Relying on client side validation □ Failing to validate input from all sources including cookies, query string parameters, HTTP headers, databases and network resources
Data in Transit Data in Destination	□ Loss of decryption keys □ Encryption cracking • Brute force attack • Impersonation • Network eavesdropping • Denial of service attacks □ Misuse of privileges	□ Using the same key for a prolonged period of time □ Distributing keys in an insecure manner □ Using the same key for a prolonged period of time □ Passing sensitive data in clear text over network □ Lack of monitoring of services and activities

3. Critical flow model

- The model is based on broadcasting information of 'critical' value (which by its very nature will not be disclosed by those involved with bad governance practices) to targeted audience using ICTs and other tools.

- Targeted audience may include media, affected parties, opposition parties, judicial bench, independent investigators or the general public.

- Those who would divulge such information could include upright officials and workers, whistleblowers, affected parties and those who were themselves involved in bad governance practices but have now changed their minds or may wish to trade such information for lenient punishments.



Applications

This model could be applied in the following possible ways:

- Making available corruption related data about a particular Ministry / Division/ Officials online to its electoral constituency or to the concerned regulatory body.
- Making available Research studies, Enquiry reports, Impact studies commissioned by the Government or Independent commissions to the affected parties.

 ISSN: 2454-4248
101 –108

- Making Human Rights Violations cases violations freely available to Judiciary, NGOs and concerned citizens.

Merits

- This model is more directed and evolved.
- Different organizations can use it differently depending on the aspect of governance they situation they want to address.
- The model corrects information failure, raising awareness about the bad governance practices.
- The model exerts indirect pressure on the concerned governance institution / policy-making body to move away from optimal ignorance attitude to reform, and take into cognizance the interest and opinion of the masses in decision-making processes.

Demerits

- The model may not work in cases where the governance mechanism does not allow public debates and opinions, and censures all information of critical nature. This model unlike the Broadcasting/ Wider-Dissemination model would be more effective in situations of Optimal Ignorance of the Government.

In this model, the analysis is done based on old records. So existing data validation is the main issue. All possible security aspects, threats and vulnerabilities have been discussed in Table 3.

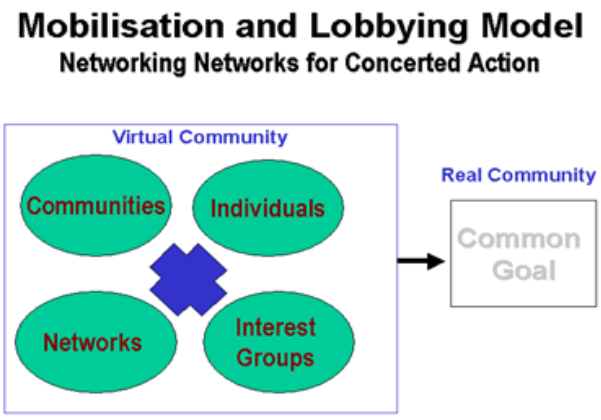
Table 3. Threats & Vulnerabilities of Comparative Analysis Model.

DATA LOCATION	THREATS	VULNERABILITIES
Data in Store	• Encryption cracking • System failure • Corruption / loss or damage of back up media • Theft of credentials	• Failing to secure encryption keys • Using the wrong algorithm or a key size that is too small • Using the same key for a prolonged period of time • Absence of back up policy • No back up copy kept off-site • Use of weak cipher or • hash to make password non readable
Data in Process	• Brute force attack • Form field manipulation	• Inadequate back up facility • Non adherence to back up policy • Using input file names, URLs or user names for security decisions
Data in Transit	• Network Eavesdropping	• Passing sensitive data in clear text to network
Data in Destination	• Encryption cracking • Brute force attack	• Password is guessable • Minimum length of the password has not been enforced

 ISSN: 2454-4248
101 –108

4. E-Advocacy Model

- E-Advocacy / Mobilization and Lobbying Model is one of the most frequently used Digital Governance model and has often come to the aid of the global civil society to impact on global decision-making processes.
- The model is based on setting-up a planned, directed flow of information to build strong virtual allies to complement actions in the real world.
- Virtual communities are formed which share similar values and concerns, and these communities in turn link up with or support real-life groups/ activities for concerted action.
- The model builds the momentum of real-world processes by adding the opinions and concerns expressed by virtual communities.
- The strength of this model is in its diversity of the virtual community, and the ideas, expertise and resources accumulated through this virtual form of networking.
- The model is able to mobilize and leverage human resources and information beyond geographical, institutional and bureaucratic barriers, and use it for concerted action.



Applications

This model could be applied in the following possible ways:

- Fostering public debates on issue of larger concerns, namely on the themes of upcoming conferences, treaties etc.
- Formation of pressure groups on key issues to force decision-makers to take their concerns into cognizance.
- Making available opinions of suppressed groups who are not involved in the decision-making process into wider public domain.
- Catalyzing wider participation in decision-making processes.
- Building up global expertise on a particular theme in absence of localised information to aid decision-making.

Merits

The model enhances the scope of participation of individuals and communities in debates which affect them and help them build a global alliance.

- A community may no longer find itself isolated but may find an ally for mobilizing effective action through this model. It also creates an effective deterrent for governments and decision-making bodies who are responsive to people's opinion to provide better governance.
- The model could also be used favorably by the government in a positive manner to encourage public debates on issues where the opinion and expertise of civil society is of great importance and therefore could become a tool to enhance democratic practices and improve governance practices (especially in Developing Countries).

Demerits

- This model require a transition period before being adopted on a wider scale.
- It require familiarity of ICT among all the citizens benefited from this model.

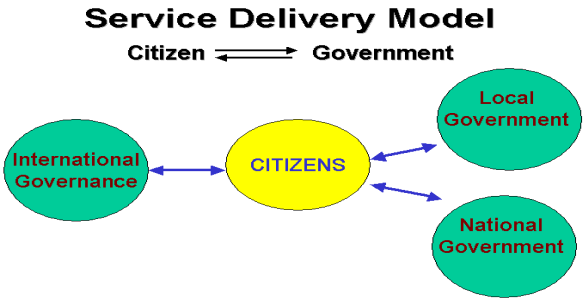
E-advocacy model has come to the aid of the global civil society to impact on global decision making process. Security aspects, threats and possible vulnerabilities for this model have been discussed in Table 4.

 ISSN: 2454-4248
101 –108

DATA LOCATION	THREATS	VULNERABILITIES
Data in Store	▪ Encryption cracking ▪ System failure ▪ Corruption / loss or damage of back up media ▪ Brute force attack ▪ Inability to identify actual user	▪ Failing to secure encryption keys ▪ Complexity of the password is not enforced ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Absence of back up policy ▪ No back up copy kept off-site ▪ Use of weak cipher or hash to make password non readable
Data in Process	▪ Http header manipulation ▪ Cookie manipulation	▪ Failing to validate input from all sources including cookies, query string parameters, http headers, database and network resources
Data in Transition	▪ Information disclosure ▪ Network eavesdropping	▪ Storing secrets when it is not needed ▪ Storing secrets in clear text ▪ Passing sensitive data in clear text over network
Data in Destination	▪ Theft of credentials ▪ Inability to identify to actual user	▪ Distributing keys in an insecure manner ▪ Complexity of the password is not enforced ▪ Use of weak cipher or hash to make password non readable

5. Interactive-Service model

- Interactive-Service model is a consolidation of the other digital governance models and opens up possibilities for one-to-one and self-serviced participation of individuals in governance processes.
- The participation is direct and not through representatives.
- It can bring greater objectivity and transparency in decision-making processes, and give a greater feeling of involvement and empowerment, provided that individuals are willing to engage in the governance processes.
- Under this model, the various services offered by the Government become directly available to its citizens in an interactive **Government to Consumer to Government (G2C2G)** channel in various aspects of governance.



Applications

This model could be applied in the following possible ways:

- To establish an interactive communication channels with key policy-makers and members of planning commissions.
- To conduct electronic ballots for the election of government officials and other office bearers.
- To conduct public debates / opinion polls on issues of wider concern before formulation of policies and legislative frameworks.
- Filing of grievances, feedback and reports by citizens with the concerned governmental body.
- Establishing decentralised forms of governance.
- Performing governance functions online such as revenue collection, filing of taxes, governmental procurement, payment transfer etc.

Merits

- It brings every individual into a digital network and enable interactive flow of information among them.
- The government services are directly become available to all the citizens in an interactive manner.

Demerits

- The model firmly relies on the interactive applications of ICT and therefore is a technology and cost - intensive model

 ISSN: 2454-4248
101 –108

- It would also require elemental familiarity of ICT among the citizens to fully benefit from this model.

In this model, information flows in two ways. So security concern is much higher than all other models. All possible threats and vulnerabilities for this model have been discussed in Table 5.

Table 5. Threats & Vulnerabilities of Interactive Service Model.

DATA LOCATION	THREATS	VULNERABILITIES
Data in Store	Encryption cracking Loss of decryption keys System failure Corruption / loss or damage of back up media Impersonation Denial of service attack Inability to identify actual user	Failing to secure encryption keys Complexity of the password is not enforced Using the wrong algorithm or a key size that is too small Using the same key for a prolonged period of time Absence of back up policy No back up copy kept off-site Distributed keys in an insecure manner
Data in Process	Theft of credentials Brute force attack Misuse of privileges	Use of weak cipher or hash to make password non-readable Lack
Data in Transition	Information disclosure Network eavesdropping	Storing secrets when it is not needed Storing secrets in clear text Passing sensitive data in clear text over network No password
Data in Destination	Theft of credentials Inability to identify to actual user	Distributing keys in an insecure manner Complexity of the password is not enforced

Conclusion

As the usage of Information Technology is growing very fast, Indian government is making many efforts to provide services to its citizens through e-Governance. Although Indian government is spending a lot of money on e-Governance projects but still these projects are not successful in all parts of India. Unawareness in people, local language of the people of a particular area, privacy for the personal data of the people etc. are main challenges which are responsible for the unsuccessful implementation of e-Governance in India. Government must take some actions to make the people aware about the e-Governance activities so that people may take full advantage of these activities and e-governance projects can be implemented successfully. The participation of people can play a vital role in implementation of e-Governance in India.

In summary, this paper presents a methodology to formulate the security architecture of the different G2C applications from their identified models. The methodology and the resulting security architectures can be used for the development, upgrade and audit of the G2C applications in a model-driven manner. Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. So access controls for different stakeholders for different data locations have been defined. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. In this paper, major contribution is the security requirement analysis of the overall G2C applications according to the models.

References

[1] Service excellence in e-governance issues: An Indian case study. D'Souza, Andrew Gilmore and Clare. 2006, JOAAG Vol. 1. No. 1, pp. 1-14

[2] E-Governance of Universities: A Proposal of Benchmarking Methodology. Raposo, Mario, Leit˜ao, Jo˜ao and Paco, Arminda. Oct 16, 2006, Munich Personal RePEc Archive.

[3] Students as e-Citizens - Deriving Future Needs of e-Services for Students. Staffan Lindell, Mikael Lind and Olov Forsgren. s.l.: University College of Borås, Sweden, 31 october 2006. international Workshop on E-Services in Public Administration (WESPA2006).

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

[5] 10. Vivek Sawant, Aatul Wadegaonkar. Digital University Framework. eGovernance : case studies. s.l.: CSI SIG on eGovernance, 2008, 19. 142

[6] 11. A Review of E-Government Readiness in India and the UAE. Farooquie, Jamal A. 1, Jan 2001, International Journal of Humanities and Social Science, Vol. 1.