International Journal of Engineering and Technology Research (IJETR)
www.ijetr.com

A MULTI-LAYER STRUCTURE FOR INDIAN E-GOVERNANCE INFORMATION SECURITY

P.V.S.S.Gangadhar[1*], Dr.R.N.Behera[2]

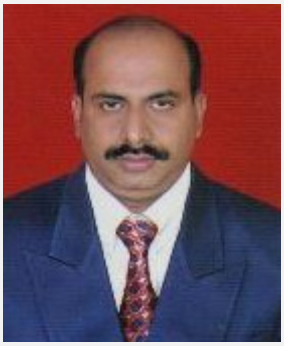
[1] Scientist"C", National Informatics Centre, Ministry Of Information Technology & Communication, Govt. of India, Rayagada (Dist.), Orissa.Pin 765001, India
[2] *Sceintist"E", Nationalinformatics Centre, Minsitry Of Information Technology & Communication,* Govt. of India, Rayagada (Dist.), Orissa.Pin 765001, India

ABSTRACT
To develop unique multi-layer security structure for e-governance services. The concept of e-governance system is to provide access to the government services to the citizens on any where at any time over open networks. This leads to issue of robust 'security' in the management of information systems. Security is closely related with availability, confidentiality, Integrity and authenticity in terms of e-services to the citizens and they are defined as Information is available and usable when required, and the systems that provide it can appropriately resists attacks and recover from failure is called Availability. Information is observed by or disclosed to only those who have right to know is called confidentiality. Information is protected against unauthorised modification is called as Integrity. Government transactions as well as information exchanges between departments can be trusted is called as authenticity and non-repudiation. In this research paper describes what are standard method are available and to be followed for better security model. In the ever-changing technological environment, security must keep pace with these changes to enable departments to create and operate in an environment of Trust and Confidence. It must be considered an integral part of the systems development life cycle process and explicitly addressed during each phase of the process. Security must be dealt with in a proactive and timely manner to be effective

Keywords: *e-governance, Security, (OWASP) Open Web application Security Model, COBIT (Control objectives for information and related technology), ISO17799.*

Available online on www.ijetr.com

Correspondence Author



P.V.S.S.Gangadhar

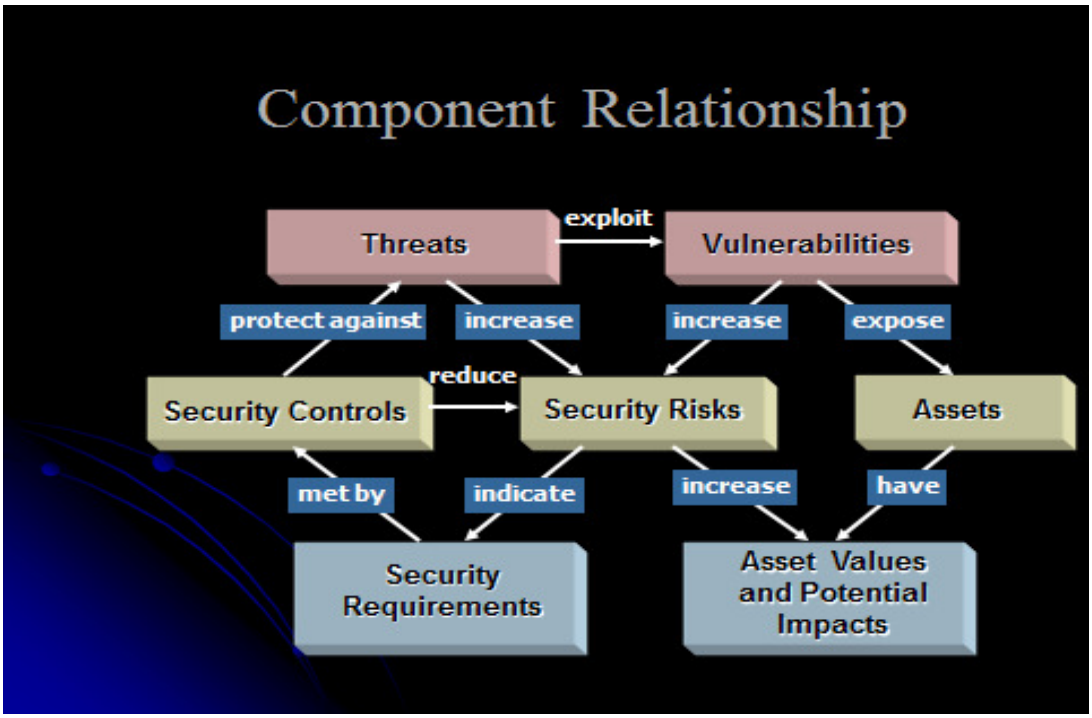
Scientist"C", National Informatics Centre, Ministry Of Information Technology & Communication, Govt. of India, Rayagada (Dist.), Orissa.Pin 765001, India

Email: 1pvss.gagnadhar@nic.in

INTRODUCTION

Security refers to the protection of valuable assets against loss, misuse, disclosure or damage. In this way 'valuable assets' is the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. Protection arises from a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. These safeguards should address both threats and vulnerabilities in a balanced manner.

The emphasis on the value of time from the knowledge workers and citizens has driven governments towards the transformation to the electronic method in offering government services to the public. This underpinned the need of launching e-governance services worldwide. The inter-government integration, information sharing and collaboration is required to provide the citizens with well integrated services. The level of trust is one of the key factors for the integration and information sharing between the government departments. Information security contributes directly to the increased level of trust between government departments by providing an assurance of confidentiality, integrity, and availability of sensitive governmental information. The below diagram shows component relationship.



The research method proposed in this research paper tries to delivers a new model that can be used as tool to asses the level of security readiness of government departments, a checklist for the required security measures, and as a common reference for the security in the government

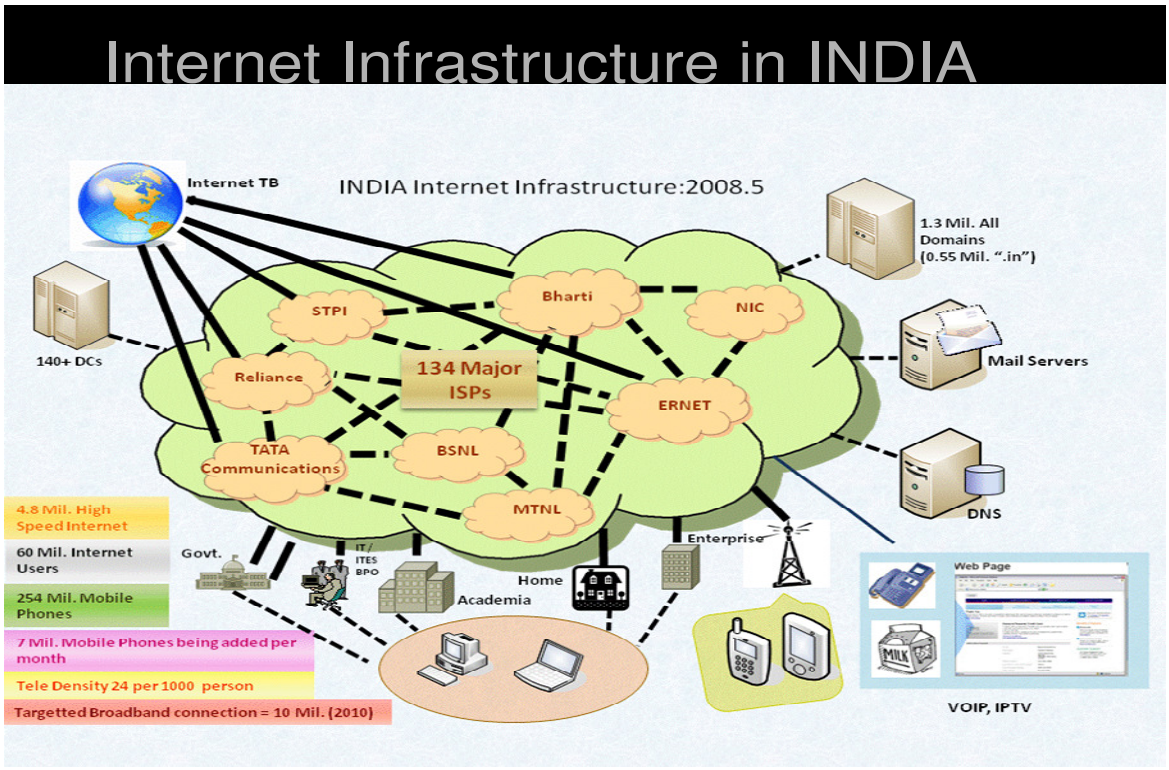
departments in India for implementing NeGP. Based on extensive literature research a new model is developed using a qualitative approach to build the overall structure and the number of layers in it. A quantitative approach is adopted during the research study to confirm the

importance of the modeled layers and sub layers. The applicability of the model is tested on different e-governance applications implemented by National Informatics Centre (NIC), which will be taken as case study to validate the model and its layers.

The research contributes to the theoretical knowledge of the information security modeling concept in four ways. First the literature review of existing security model and their coverage of security aspects. Second, the analysis of the security threats related to the e-services. Third, the construction of a new security model based on the academic research on the each layer. Four, the applicability of the model will be validated in the case study selection.

SCOPE

Currently most of the e-government services are accessed through different government department portals and not through the official e-government portal known as www.india.gov.in. The government portal acts as a catalogue of the government e-services and directs the citizens to the respective government portal once the e-service is selected. A citizen of India will have to access multiple portals to complete a cycle of a single e-service. The national e-governance (NeGP) plan is striving to achieve the goal of integration. The problem of integration of all the government departments has contributed factors including fear of security issues.



INTERNET INFASTRUCTURE INDIA

In this research document a new security model is developed for the e-government authority and its affiliated government departments. It is meant to be used as a reference and a standard for assessing the level of security in each department and as an assurance of government department's better security level.

The new security model will also assist in ascertaining the current level of security of each department, giving the confidence to other departments and serve as a mitigation action of the risks that may exist in the future.

METHODOLOGY

This research focuses on building a new security model for the e-governance of India. Initially the aim of the research is to build an information security model for any government organisation and it was then narrowed to address e-governance security issues

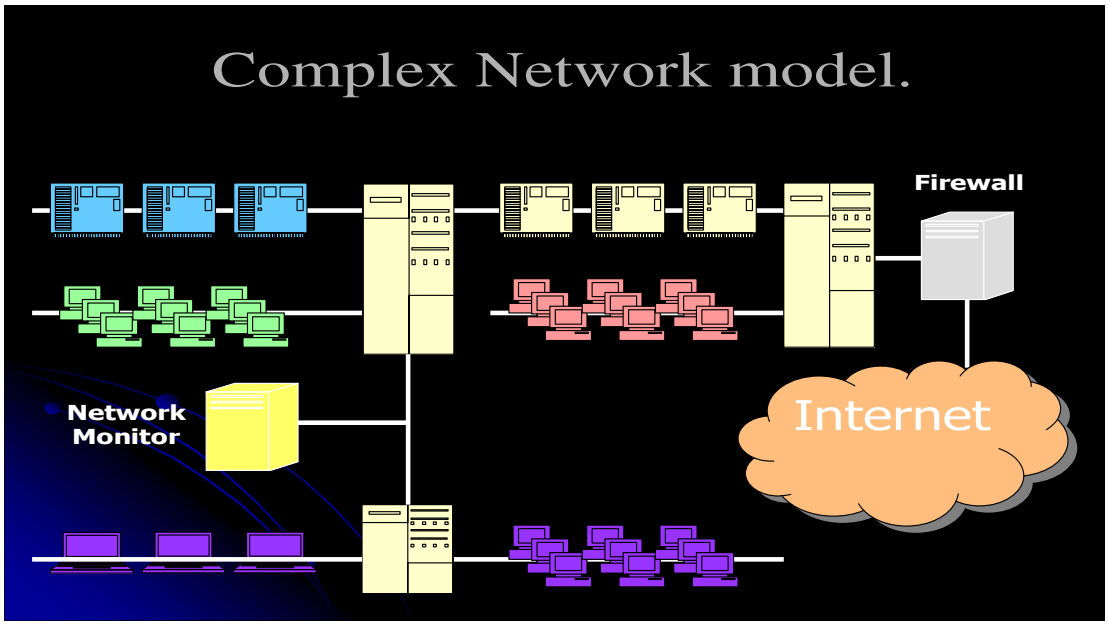
.

The objectives of the research are as follows:

1. Establish the security requirements for e-governance application used by Govt. of India .
2. Collate state of the art approaches and methods for the e-governance security.
3. Develop model for evaluating the security level for inter-government information sharing.
4. Test the model in the India e-governance scenario.

Information security mainly deals with

(i) Confidential (ii) Integrity/Authenticity (iii)Availability (iv) Non-repudiation (v) Privacy.



COMPLEX NETWORK STRUCTURE.

RESEARCH PROCESS

The word "cyberspace" was coined by the science fiction author William Gibson, when he sought a name to describe his vision of a global computer network, linking all people, machines and sources of information in the world, and through which one could move or "navigate" as through a virtual space.

This research paper based on the research methodology mixing the quantitative and qualitative methods as explained by Creswell (Creswell, J. W., 2003). The questionnaires designed for collecting data from various departments has open-and-closed ended questions to obtain both quantitative and qualitative data for the analysis from departments experts and chief Information security Officers/ head of the network groups.

Presently e-governance in India follows

OWASP (Open Web Application Security Project) model. It has to satisfy the COBIT and ISO17799 standards. An extensive literature review of existing security models (i.e. OWASP, COBIT & ISO17799) was carried out. Information security models addressing information flow and sharing, e-commerce security, Internet optimization, e-governance services security, human behavioral effect on cybercrimes, networking security rating and other aspects of security, were to be studied and analysed. The reviewed models contributed to the information security field by addressing one or two aspects of security. The structure of these models is varied from mathematical structure, to pure graphical representations.

The review of strength and weaknesses of these models
assisted in building the conceptual design of the new model based. how the process of review of the existing models led to conceptualizing the new model.

- **Cyber security standards** are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.
- These guides provide general outlines as well as specific techniques for implementing cyber security.
- For certain specific standards, **cyber security certification** by an accredited body can be obtained.
- There are many advantages to obtaining certification including the ability to get cyber security insurance.

Cyber Security Standards:

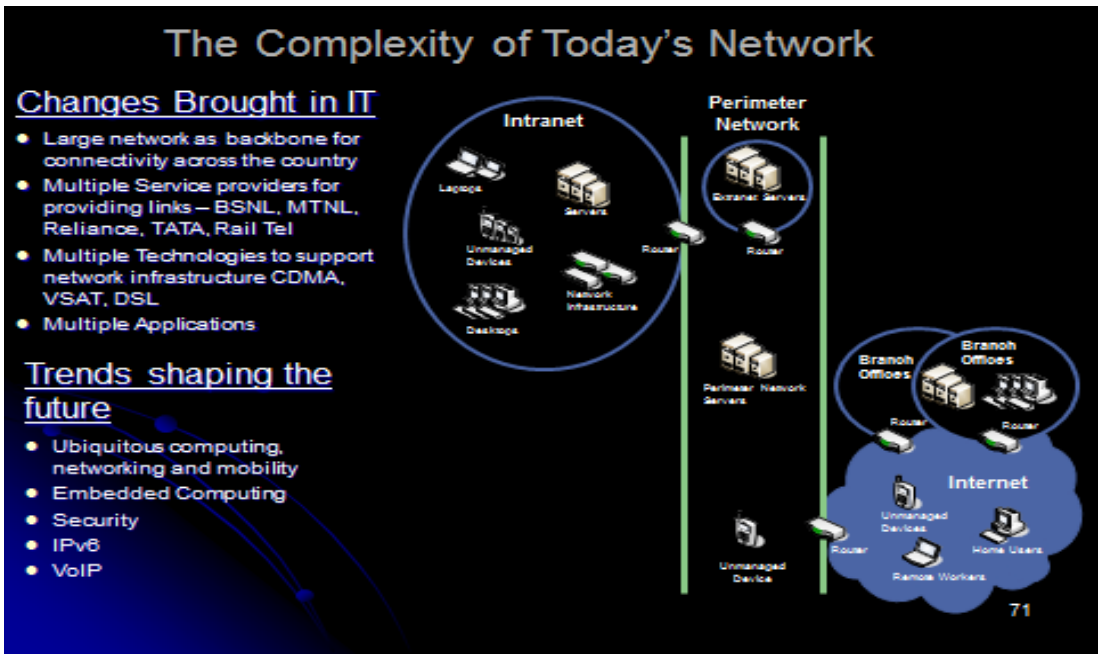
- ISO 27002 incorporates both parts of the BS 7799 standard.
- Sometimes ISO/IEC 27002 is referred to as BS 7799 part 1 and sometimes it refers to part 1 and part 2.
- BS 7799 part 1 provides an outline for cyber security policy
- BS 7799 part 2 provides a certification.
- The outline is a high level guide to cyber security.
- It is most beneficial for an organization to obtain a certification to be recognized as compliant with the standard.

CONCLUSIONS

The model is an betterment of the existing models in its comprehensive nature to address the variety of threats to information security to the departments. It has an adaptable structure that can be extended to new emerging threats. In addition, the model is easy to understand and used by non technical people with management responsibility for the e-governance security.

The new model presented in this research paper provides the authority and its affiliates a structured methodology to assess the security level in different government departments, a checklist of all the security elements required to build a robust security programme and architecture, and a mean to align the different views on the needed security levels for transparent information sharing. It can also be evolved to be an international framework for the government security architecture and a standard used by authorities worldwide. The new model addresses some of the main domains of ISO17799 by addressing policies and operational management, and the people capability maturity matrix (PCMM) through addressing the competency layer.

The below diagram shows how complexity of today network. What are ISP major role in india. And it is how connected back bone for Indian internet service.



COMPLEXITY OF TODAY'S NETWORK.

The new model developed through the research work of this research paper has four strong characteristics:

- This Security model is flexible and not biased to any technology, policy or any other security aspects: The sub layers presented in the model are academically researched independent from any industry or brand bias so that in future it will have wide impact.
- The new model is independent of any theory, threats, sector or architecture or framework and it can be placed as part of any government system architecture for any government department.
- This Security Architecture can be used for multiple purposes: The new model can be referred as a comprehensive security architecture which addresses more than the technological aspect. It can also be used as a checklist for what's implemented and what's in the future plan and can easily be turned into a measurement tool for the security level of the government departments. Finally, it can be used as a strong awareness tool for government executives to give them a holistic view of all the security aspects required by their organization.

REFERENCES

[1] Xiaohong Gan (2008) *"Research on Risk Aversion of E-government Network Security".* ieee research paper.

[2]WANG Jin-fu (2009) *"E-government Security Management: Key Factors and Countermeasures".* ieee research paper.

[3] Irfan Syamsuddin, Junseok Hwang Bertucci,(2010) *"A New Fuzzy MCDM Framework to Evaluate E-Government Security Strategy"* ieee research paper.

[4] "*INFORMATION SYSTEMS SECURITY COMPLIANCE IN E-GOVERNMENT"* (2009)

[5] Goncalves, M. (1999), Firewalls A Complete Guide, McGraw Hill, New York

[6] Hafedh AlShihi (2006) " *Critical Factors in the Adoption and Diffusion of E-government Initiatives in Oman"*.

[7] Sibal sarkar *"e-government adption and diffusion"* CSI, research paper.

[8] Zhiyuan Fang (2002), *"E-Government in Digital Era:*
Concept, Practice, and Development".

[9] *"ICT for Rural Development: An Inclusive Framework for e-Governance",* CSI paper.

*****