Cyber Security and Data Privacy in the Era of E-Governance

Md. Asaad Raza
Department of Public Administration, Arignar Anna Government Arts and Science College,
Karaikal (UT of Puducherry), India

Corresponding Author: asaadraza@gmail.com

Received: 05-12-2023 Revised: 18-12-2023 Accepted: 02-01-2024

ABSTRACT
E-Governance is known as electronic governance which is based on information and communication technologies (ICTs) at various levels of the government and the public sector using Internet and other related electronic device. It is an efforts made by the governments to improve relations with their citizens. However, there are various concerns that are related with it. A cyber security and data privacy are the major challenges in this regards. The Cyber Security is known as the security of information by communicating channels using computing devices. These devices may be computer network, smartphones and other related equipment. The Data privacy is termed as concern of the information privacy of a person shared with others with proper handling of sensitive data. These data can be personal data*, confidential data of various sectors, government data, intellectual property data, etc. In order to execute good governance using E-Governance, there is a need for information security best practices. Data should be protected against cyber attracts. National and international framework should be work for concerns related to e-governance. There is a need for implement existing law and seeks to remedy that concern with cyber security. In this paper factors related to cyber security and data privacy for e-Governance have been addressed with administration and enforcement process, legal framework and national and international considerations.*

Keywords: *cyber security, data privacy, e-governance, digital personal data, cyber attack*

I. INTRODUCTION

Over the year, e-Governance is has been taken as an administrative tools for the governments to improve relations and working with their citizens. It brings government with an environment of transparency and openness and ease of doing business more closely to their citizens. The e-Governance covers a larger framework for the implementation of government policies. With changing the working methods, it is mapping various administrative work of society. It has various advantages in the field of health, education, finance, agriculture, law, justice, defence, power sectors, transport, science and technology, tourism, public distribution system, etc. Thee-Governance is function by using the Information and Communication Technology (ICT) in their operations[1-3].

Information Technology has transformed working methods global and connected people beyond imagination. It is gaining every day a milestone in field of e-Governance across the world by experimenting the innovative ideas for development and inclusive growth. In order to communicate and conduct of polices, it has migrated world's population towards Cyberspace. There are the provisions of confidentiality, privacy and security of information. It has created new opportunities and vulnerabilities also. The cyber security threats emanate themselves in disruptive activities by targeting individuals, businesses, Governments. There is a significant risk for globally linked economy, national security and public safety. As is a virtual space anywhere, it may the cause of disruption that attributes the use of Information Technology for disruptive works. Cyber security is a complex issue which address multiple domains of multi-dimensional. The cyber security threats pose the most serious challenges for economic and national security. It has given a challenge for governments in the world.

Data privacy that referred as information privacy which concerns the proper handling of sensitive data. These data may be *personal data*, confidential data of various sectors such as financial data, intellectual property data, etc. It meet requirements for protecting the confidentiality of the data. The personal information that shared with others need to determine the privacy of the data. The personal information may be name, contact information, location and real-world behaviour. Data privacy is the relationship among the collection and dissemination of data, contextual information norms and legal and political issues based data. The data privacy can be protected in various types of data protection. Security is an important element for privacy and data protection from external and internal threats. It also determining to digitally stored data can be shared to the securely. The data to whom is shares should have au authentication over it. Usually, data privacy related to the control process around sharing the information to third parties. It also required to how and where the data is shared and stored. This is followed by the specific regulations which regulated these processes. Now a day's all countries in the world have taken account of such data privacy and cyber security. They have introduced various form of legislation that concerning the data privacy in order to secure the information of the large section of the population. These data need to be protected using cyber security for the better e-Governance. In this paper Cyber Security and Data Privacy in the e-Governance is studied [4-6].

II. DEFINITIONS

E-Governance: e-Governance is known for an electronic governance which is based on information and communication technologies (ICTs) at various levels of the government and the public sector using Wide Area Networks, Internet, mobile and other related electronic device for enhancing the governance. The e-Governance has various example of governance in the field of Digital India initiative, Aadhaar, National Portal of India, online payment, digital management systems, electronic communication, online studies and entrance test, etc. It is aimed to simplify the governance processes for all including government, citizens, businesses, etc. Its implication of governance is to bring framework for easy, responsive, moral, accountable and transparent governance at National, State and local levels.

Cyber Security: A Cyber Security is termed as the security of information by communicating channels using computing devices such as computer network, smartphones and other related devices. This may be applied though internet for private and public networks. It covers all possible processes and mechanisms that are executed by computer-based equipment. The information and services are protected from unauthorized person. The access of data in cyber security covers the protection of unwanted events including natural disasters.

Data Privacy: Data privacy is defined as concern of the information privacy of a person shared with or communicated to others proper handling of sensitive data. These information can be *personal data*, confidential data of various sectors, government data, intellectual property data, etc. It is based on the information of a person in terms of name, location, contact information, etc. If a data is shared with others need to determine the privacy of the data and it is required to protect the confidentiality of the data. Majorly, data are classified in four categories. These are the data belong to public, confidential, internal-only and restricted data. The example of data privacy can be found in the ensuring sensitive data of medical records of a person that only accessed by authorized personnel. The data privacy can be observed through access control measures. These measures are login through usernames and passwords or biometric authentication. Other example of data privacy is encrypting the data under controlled authentication [7-8].

III. CYBER ATTACKS AND DATA BREACHES

Recently, it is observed that several cyber security breaches have been taken place. These may be cause of the cyber attack. A cyber attack is termed as any malicious attempt of unauthorized access to the electronic devices such as computer, computing system or computer network. Its objective is to disable, disrupt and control computer systems. Within these systems cyber attacks alter, block, delete or manipulate the data. It has open a new challenge in the governance followed by the e-Governance.

It is noticed that in India it has reportedly seen that cyber-attacks cases has raised 10% in 2018 with respect to approximately 53,000 cases reported the year before. It has caused significant financial loss of approximately USD 500,000 within one year to Indian companies. It has been found that only 5% of such cyber-attacks are traced by authorities. This can be seen that Cosmos Bank got a major cyber-attack in India where the hackers launched a malware attack and transferring the money USD13151300 to a bank account in Hong Kong. In other case, offenders used SIM cards and hacked almost 30 individual bank accounts and approximately USD550000 money has transferred to some ones. Recently, Canara Bank ATM servers have been hacked by hackers stole of almost USD30000 from 50 different bank accounts. Furthermore, several website nearly 20,000 have been hacked including many government websites also.

The cyber attack is associated with the data breach. It is known as any security incident in which unauthorized parties’ access confidential information or data. This information may be personal data related to social security data, bank account numbers, healthcare data etc. Other information can also be incorporated in these category are corporate data such as customer data records, intellectual property, financial information etc. The data braches is seen in the stolen of passwords or other credentials with third parties. It includes human error also like an email attachment having personal data being sent to the incorrect recipient.

The data breach can be done by several steps. These are done by cracking the preventive measure of the stored data. Beaching the protected data can be followed by assessing the gathered facts including potential harm to affected individuals. There are several action can be taken to minimise the data breaches. This includes notification by individuals if its entity has been breached. Regular reviews required to see the incident and action to be considered immediate to prevent future breaches. It also in such a way that at any time, individual entities should take remedial action so that it limits the impact of the breach of concern individual. The action should be taken immediately to contain, assess and remediate the incident. Some case breaches may initially seem immaterial and it may become significant when their full information’s are assessed. In some situation it may be notify to individuals immediately as soon as containment or assessment of the breach occurs. There should mechanism to respond on a case-by-case basis. Depending on the breach an entity may take additional steps to specific the nature of the breach [9].

IV. THE INDIAN CYBERSPACE

A cyberspace is a complex interaction among the various sectors such as people to people, software and services which is supported by worldwide distribution of information and communication devices and networks. In this regards the government of India has made a framework to look it. Indian government has set up a National Informatics Centre (NIC) as early as 1975. It has the goal of providing IT solutions to the government. Between 1986 and 1988, there was three more set up made namely INDONET, NICNET and ERNET. INDONET had aim to connecting the IBM mainframe installations that made up India's computer infrastructure. NICNET is an NIC Network that being a nationwide very small aperture terminal for public sector organisations. It has also connected to the central government with state governments and district administrations. The ERNET (Education and Research Network) has ability to serve the academic and research communities.

In the year 1998 the policies such as the New Internet Policy had made to pave the way for multiple Internet service providers. This has further found that the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003. It has observed that by 2012 the Internet users in India were approx. 12.5% of the total population of the world. As per the data presented by Internet and Mobile Association of India (IAMAI), by the 2014, the internet user base in India is 243 million with a year-on-year growth of 28%. Such growth is again expected to continue in forthcoming years. It will have more and more people accessibility to the web. This accessibility can be done through mobile phones, tablets and other devices. The government is also making a push to increase broadband speed up to more than 4mbps. In this continuation a National e-Governance Plan (NGeP) has launched by government of India to make an environment of increasing thrust on e-governance. This may leads as a cost-effective way of taking public services among the various sectors across the country [7, 10].

V. ADMINISTRATION AND ENFORCEMENT PROCESS

The government of India has an approach for governance by using the cyber security and data protection criteria. There is a mechanism to enabling a legal framework on Cyber Security. It has a capability to make the policies that will compliance and assurance the e-governance process. Research and development are taken into account in the regards of Cyber Security. In the case of mal practices there is a early warning and response system named as National Cyber Alert System. It has also made a process with exchange of Information with International agencies. Various security training has been conducted with skill and competence development. These training include a domain specific training using cyber forensics, Network and System Secured Administration. It has taken into account to do administration with collaboration to the National and International agencies.

In the connection with Administration and Enforcement Process, a MeitY has been appointed the officials such as Secretary of the Department of Information Technology of each Indian State or Union Territories for look it. These are comes under the Information Technology Act (ITA) 2000. Any related person can make a written complaint to adjudicating officer based on the location of the computer system or the computer network along with a fee. Here the claim can be made for compensation also. After the complaint, the concerned officer will issues a notice to the parties notifying the date and time for further proceedings. Based on the evidence, the officer can decide whether to pass orders if the respondent pleads guilty, or it may to carry out an investigation. In the case when the concerned is convinced, the scope of the case extends to the punishment. It may be financial penalty and case will transfer to the Magistrate jurisdiction. There is an option of appeal also. The first appeal can be filed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and then appeal before the High Court. There is a maximum penalty for violation of the provisions of Personal Data Protection Bill 2018 (PDP Bill) is 15 crores rupees or it will be 4% of the total global turnover in the preceding year, whichever is higher is applicable. It is mentioned that an expert committee should give the report and central government need to establish an appellate tribunal to adjudicate on appeals [11].

VI. LEGAL FRAMEWORK FOR DATA PROTECTION

There is a legal framework for data protection. The general Data Protection Law in India is governed by the Information Technology Act, 2000 (IT Act). The specific rules are issued under Section 43A of the IT Act: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 known as Data Protection Rules. Under this Act, two categories of information are covered which are considered with respect to data protection. First is Personal Information (PI) which is termed as any information that relates to a natural person either directly or indirectly in combination with other information available with a body corporate which is capable of identifying such person. Second is Sensitive personal data or information (SPDI) which is related to personal information that consists of information relating to various factors. These may related to passwords, bank account, credit card or debit card or other payment instrument, health condition, sexual orientation, medical records and history and biometric information.

Here, the Data Protection Rules are mostly applicable to institutions and corporates that are related in the collection, receiving, possessing and dealing of SPDI using an electronic medium. This Data Protection Rules are applicable only to institutions and corporates which are located within India. Hence, if SPDI of any individual is collected, received, processed, dealt with and handled outside India, this may not be applicable. However, the IT Act is applicable to an offence committed outside Indian Territory with a condition that the act involves a computer or computer network located in India. But, the local data protection laws of the corresponding countries may apply. The draft of Personal Data Protection Bill, 2018 introduces about a 'Data Fiduciary' and a 'Data Processor'. Recently, the Department of Information Technology has issued a Clarification on the Data Protection Rules in 2011 known "2011 Clarification". In this clarification, it was clarified that those rules which are govern under collection and disclosure of SPDI will not be apply to any body which providing a services for collection, storage, dealing or handling of SPDI under a contractual obligation within or outside India. There are some penalties for offenders who providing services under a contract, have accessed PI with wrongful intent and discloses the PI. This disclosure would cause harm without authorization. In this section it is prescribed that there is a penalty of imprisonment up to three years or a fine up to 500000 rupees [3, 12].

VII. DIGITAL PERSONAL DATA PROTECTION BILL 2023

Recognizing privacy as fundamental right under the pursuance of the developments in Court, the Government of India has introducing an extensive data protection law in 2018. So far four drafts of proposed privacy legislation have been released. The latest draft of the proposed draft is Digital Personal Data Protection Bill, 2022 was released in 2022. This has comes in account by public consultation and inviting comments for stakeholder until January 2023. In the proposed Law it is prescribed the compliances for collection, storage and transfers of personal data. It corresponds to data of individual is collected, received, processed, dealt with and handled within India. This data may be collected from online or collected offline and then subsequently digitized [13].

This Act provides the processing of digital Data of individual in such a way that the rights of the individuals to protect their Personal Data with lawful purposes. This Bill has passed in India's Rajya Sabha and Lok Sabha to curb misuse of personal data using online mode. There is a penalty of up to 250 crore rupees on entities or companies that are misusing or failing to protect personal digital data. This Act will look into the issues related to consumer protection, electronic contracts as well as the content moderation on social media. The Digital Personal Data Protection Act (DPDP Act) 2023 has come into account on 11th August 2023. The features of the bill are that it provides for the processing of digital personal data with the rights of the individuals for protecting their personal data as well as to process the personal data for lawful purposes. Thus the Digital Personal Data Protection Bill 2023 is helping for e-governance with Cyber Security and Data Privacy.

VIII. INTERNATIONAL CONSIDERATIONS

In order to global alignment and best practices in the field of digital landscape, India's working procedure for governance must be align with international standards. It is noticed that two top email providers named as Gmail and Yahoo had more than 34 million users registered from India. Out of these nearly 62% of Internet users in India use Gmail. The average Internet speed India is 1.3 mbps in the year 2013 which was the lowest among Asian countries. Now the internet speed has been increased to remarkable level. Reports shows that only 2.4% of India's Internet connections having the speeds of more than 4 Mbps. There must be some restrictions on International Data Issues for data transfer which is subject to certain restrictions like recipient entity ensuring the same level of data protection under comply with a lawful contract or prior consent. In this regards the MeitY guidelines for use of cloud services indicates that the service provider need to store the data within the country. In the case where the data is located in foreign countries, the conditions related to data location must be mentioned in an agreement with the service-provider. There must be mechanisms that apply to International Data Transfers. The transfer of data internationally would have to periodically notify under competent authority with proper contract. In addition, it is required that transfer entity must store at least one copy of the personal digital data. This can be done on a local server or data centre in country. For e-governance it required to share the technical details for various software code or algorithms with the government [13-15].

IX. CONCLUSION

The e-Governance based on the governance through electronic mode has been studied. It is ICT based governance at various levels of the government and the public sector using Internet and other related electronic device. It has been noticed that this has made the governance with improve relations with their citizens. It is noticed that cyber security and data privacy are the major challenges. The Cyber Security is related to security of information by communicating channels using computing devices. The Data privacy is also a major concern of the information privacy of a person shared with others. The shared data can be *personal data*, confidential data of various sectors, government data, intellectual property data, etc. To execute a good governance using E-Governance, data should be protected against cyber attracts. National and international framework should be made for such concerns. It is also required that existing law should implement and seeks to remedy related to cyber security.

REFERENCES

1. Kumar D, & Panchanatham N. (2014). Strategies rebooting the government in e-mode. *Global Journal for Research Analysis, 3*(8).
2. J. Satyanarayana. (2006). *E-government*. India: Prentice Hall.
3. Cyber Laws. (2013). http://indianrailways.gov.in.
4. E-Governance. (2013). http://en.wikipedia.org/wiki/E-Governance.
5. Holmes. (2003). *Solutions come to those who wait*. Times of India.
6. Kumar D, & Panchanatham. (2024). Strategies for effective e- governance management. *International Journal on Global Business Management & Research, 3*(1).
7. National Cyber Security Policy. (2013). http://deity.gov.in.
8. Saxena, K. B. C. (2004). Towards excellence in e-governance. in: *Towards E-Government: Management Challenges*, M P Gupta. (Ed.). India: Tata McGraw-Hill.
9. Yuchong Li, & Qinghui Liu. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186.
10. Kumar D, & Panchanatham N. (2015). Enforcing transparency in Indian e-governance through ICT. *International Journal of Business Management & Research*.
11. Kumar D, & Panchanatham N. (2015). A study on Cyber law in promoting e-governance. *International Journal of Multidisciplinary Research*.
12. Nir Kshetri. (2016). Cybercrime and cyber security in India: Causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313–338.
13. https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022. Last Accessed February 25, 2023.
14. Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, & Kamran Shaukat. (2023). A critical cyber security analysis and future research directions for the internet of things: A comprehensive review. *Sensors, 23*(8), 4117.
15. Peter Vrsansky, & Daniel Bednar. (2017) *Cyber security and the international law*. *Bratislava Law Review, 1*(2), 38-49.