A PUBLICATION OF MOTHERHOOD UNIVERSITY, ROORKEE

(Recognized by the UGC with the right to award degrees u/s 22(1) of the UGC act 1956 andestablished under Uttarakhand Government Act No. 05 of 2015)

Motherhood International Journal of Multidisciplinary Research & Development

A Peer Reviewed Refereed International Research Journal

Volume II, Issue I, July 2017, pp. 01-09

ONLINE ISSN-2456-2831

Issues, Challenges and Reasons for Privacy Threats in E-Governance in INDIA

Dr. Anil K Kapil[1] & Mr Sachin Kumar[2]
[1]Professor & [2]Assistant Professor
Faculty of Mathematics and Computer Sciences
Motherhood University, Roorkee, Uttarakhand

Abstract

This Paper highlights some of the issues, challenges and reason for privacy threats in E-governance. We also suggest some of the point that keeps in mind while privacy technology is adopted. E-governance performs various communications directly from the government to the people in which there is high level of transparency and accuracy. Four major interaction targeted in e-Governance Government to Customer (G2C) Government to Business (G2B) Government to Employees (G2E) Government to Government (G2G) . The first and foremost reason is the low security for the data; this covers the improper collection and storage of the personal data of an individual. Secondly the way of collecting the data also has a vital role. When any data is to be collected from the citizens for entering in to the e-governance project, most of the data will be transferred from the existing records and some of the latest and important information will be collected in person, thus this way of collecting the information will become insecure when the person who is recording uses it in a wrong manner. The next privacy threat that most of the developing countries face is due to the lack of knowledge. The persons who are not well versed in providing their information seeks some external private agencies for help and again from those agencies if there is leakage of information, privacy issue starts there.

Keywords: e-Governance, G2C, G2B, G2E, G2G

Introduction

Overview to e-Governance

E-governance, otherwise called electronic governance is the most significant application in the field of information communication technologies (ICTs) to the government in order to make the administration easy and efficient. In this busy society, every human is bounded by his/her day to day work nevertheless they also need to be communicated with the government for various issues. In this case, gone are the days where people used to stand in queue to get their work finished, and in these cases e-governance plays a vital role in the betterment of the society

and to decrease the human effort. E-governance performs various communications directly from the government to the people in which there is high level of transparency and accuracy. Four major interaction targeted in e-Governance Government to Customer (G2C) Government to Business (G2B) Government to Employees (G2E) Government to Government (G2G).

Privacy Issues

Even though e-governance has merits, the privacy and the security threats is one of the challenging drawbacks of it. Drawback in essence, it is not the direct impacts but still some of the important information regarding a person remain unsecure. Any e-governance initiative will become invalid to maintain the privacy when the privacy policy is not articulated properly. The privacy policy is the milestone of the information security effectiveness. Great importance is given to the privacy issues in e-governance indicates that there are various unauthorized agencies who are waiting for the secure information of an individual to use it for illegal reasons. 3. Privacy Laws and E-Governance. There are certain privacy laws provided by the government that monitor the privacy threats in the society, but pessimistically e-governance involves in all these privacy law issues and the data acts as a source for many external agencies to do malpractices. Online privacy laws Health privacy laws Information privacy laws financial privacy laws Privacy in one's home Communication privacy laws.

Aadhaar Data Exploitation in India

Aadhaar card is a mandatory in India, in which the unique identity of an individual is registered. An IIT Kharagpur graduate who has been caught of hacking into the central identities data repository of the unique identification development authority of India's (UIDAI) aadhaar project gained access to the repository through the digital India e-hospital initiative of the ministry of electronics and information technology. The app called 'ekyc' delivered demographic data like name, address, phone number of individuals from the central identities data depository of aadhaar to authenticate unique identity numbers. It was placed on Google play store with the issue that it was framed by an entity called mygov linked to the start-up qarth technologies, and then all the information were shared. The details of aadhaar-enabled e-hospital system created under the digital India project of the government of India to access all the central identities data that are repository of uidai for the verification of aadhaar numbers for his 'ekyc verification' app.

As a highly qualified technical expert, the IIT graduate had a deep interest in hacking the information's from the registered data. This action created a great issue in India and all the individuals were in a doubt that their personal details would have been hacked by these kinds of people when they linked in the e-governance.

Fraud detection and security measures taken by UIDAI

UIDAI lodged criminal complaints against Axis Bank, Suvidha Infoserve, eMudhra for illegally storing and using Aadhaar data to impersonate people and carry out transactions. Allegedly, Suvidhaa Infoserve and e-sign provider eMudhra had conducted multiple transactions using the same fingerprint, which implied that organisations are illegally storing biometric data on their servers.

Reasons for Privacy Threats in E-Governance

Even though e-governance projects are well planned by the experts and by the government, there are various reasons that are left behind the privacy issues in e-governance. The first and foremost reason is the low security for the data; this covers the improper collection and storage of the personal data of an individual. Secondly the way of collecting the data also has a vital role. When any data is to be collected from the citizens for entering in to the e-governance project, most of the data will be transferred from the existing records and some of the latest and important information will be collected in person, thus this way of collecting the information will become insecure when the person who is recording uses it in a wrong manner. The next privacy threat that most of the developing countries face is due to the lack of knowledge. The persons who are not well versed in providing their information seeks some external private agencies for help and again from those agencies if there is leakage of information, privacy issue starts there.

Privacy Technology

The governments which are planning for e-governance must have a high level privacy policy through which the intruders cannot hack the government systems and to protect the important information to be transferred for illegal usage, and to detect the unusual behavior in e-governance at its early stage.

Operational technology

Intruders those who are aiming for the personal information of the individual seek plenty of ways to access the networks that are connected through e-governance, provided with the excellent knowledge about the social techniques and by various operations that extract the information's and administrate the system infiltration. The system administrators are not able to provide detailed information about the persons due to the fear of intruders and they result in providing minimum information's. On the other side, services always make system administrators to get compromised by hackers nevertheless they can develop he operational technology in order to decrease the attack of intruders.

Analysis tools

In the society of increased intruders for public data, the e-governance is in need of effective analysis tools that monitor the vulnerability present in the applications that are used frequently. There are various types of tools that are used in e-governance in which they have their own pros and cons in dealing with data security. Critics too claim that these tools that are freely accessible are very useful in notifying the issues and the illegal activities executed by the external unofficial sources, thus through the usage of analysis tools there is a great chance of blocking the data.

Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is a very useful method to encrypt the message sent, that contains high security information's, with the motto of providing the barrier for the intruders and the administrator systems. The main advantage for the intruders in which they succeed is that, they can hack the data and transfer the same that are in the format of reading and compiling, so when this becomes impossible we can provide high security to the information's. As thousands of information's and details are shared through the internet daily, the users and system administrators are not aware that their data will be visible to many unintended recourses through the world. The person who interrupted the public data can transfer the data to various unofficial organizations through which they can use it for illegal activities. One key to this issue is the usage of cryptography, through which the readers will not able to

understand the information they accessed. The security to the information can be given by incorporating digital signatures and passwords. Only the person who placed the authenticated signature can access and transfer the data in future, and this process of digitalizing the privacy process sounds good in many countries**.**

Conclusion

It can be clearly understood that privacy issue is one of the major governing factor for any e -governance project by deciding the success of the same. In a wide range of data collection the administrators should not compromise the work load that deals with the privacy protection. The privacy threats also deals with the low security for the wealth of the citizen through bank account intruders and due importance must be given by the administrators and the citizens to minimize the privacy issue in e -governance.

References

1. S. Balakrishnan, D. Deva, (2017), Issues and Challenges in E-Governance Caused by Privacy Threats, CSI Communications, Volume No. 41, Issue No. 7.
2. www.searchsoftwarequality.techtarget.com › Internet Security › Network security.
3. https://www.quora.com/What-are-the-privacy-issues-with-Aadhaar.
4. http://www.aadhaarnews.com/aadhaar-data-hack-iit-kharagpur-graduate-arrested-earns-rs-40-lakh-year-ola/