International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 5, September – October 2013 ISSN 2278-6856

Identity Management in E-Governance

Aparajita Pandey [1], **Dr. Jatinderkumar R. Saini**[2]

[1]Assistant Professor, Department of EEE,
BIT(MESRA), Jaipur Campus, Jaipur, Rajasthan, India

[2]Associate Professor & I/C Director,
Narmada College of Computer Application, Bharuch, Gujarat, India

Abstract*: From the beginning of modern governance and structured commerce, both public and private service agencies across the country typically require proof of identity before providing services to individuals. In this paper the problems that arise when governments turn to e-governance and use identity management to provide online services are discussed.*

Keywords: E-Governance**,** Identity Management, Internet Security, Privacy

1 INTRODUCTION

Around the world, Governments are strengthening their Identity management Systems. One of the reasons is to use the online environment to deliver and improve services; another is the increase in criminal activities in like spoofing and phishing. Governments are also concerned about terrorism, including the use of money laundering to finance it. This paper deals with the issues that arise when governments turn to e-government to provide online services. Government approach to Identity Management should take into account the cultural backgrounds. Social policy can be as important as technology in determining the approach to Identity Management.

Identity Management can be described as the policies, rules and processes and systems involved in ensuring that only known, authorized identities gain access to networks and systems and the information contained therein.[11].

2 DIFFERENCES BETWEEN GOVERNMENT & PRIVATE IDENTITY MANAGEMENT SYSTEMS

The people who use Identity Management Systems (IDM) may think that there is not much difference between Government and private IDMs because of the increased partnerships and cooperation between government and private sectors. However there are some key differences in the approaches to IDMs in both the sectors.

1. : The first difference is that government must look into broader issues like social inclusion, consistency and interoperability. A private company might target a particular segment but the government programs must serve the entire population that includes a large range in terms of age, language, technical, physical and mental abilities.
2. The second difference is that even in democratic structure, Government has the power of legal compulsion. The citizens have a little choice if they don't like the way they receive an essential service or how they are required to interact with the government. Their main way to respond is through general elections held every five years which is a very limited form of marketplace test. This is why citizens find it difficult to accept government initiated IDMs like AADHAR .The people also expect stringent accountabilities or greater transparency about security and privacy.
3. The key reason for having a strong IDM system is convenient, efficient and accountable online service delivery. Other reasons include law enforcement and national security where accurate tracking a person or linking information about them to help them in their investigations. This difference in the goals presents another challenge to Governments when they attempt to apply one IDM system to more than one use. Rather than try to meet all policy goals with one solution. Government might need several IDM solutions.

3 DIFFERENCES BETWEEN ONLINE AND OFFLINE IDENTITY MANAGEMENT SYSTEMS

In the online world large amount of information is collected and interconnected as compared to offline mode. This benefits the government and the citizens but it creates several risks that did not exist in paper based systems. For example, governments can track and monitor citizens' behavior and use this information which may result in discrimination or inaccurate presumptions that could be damaging and difficult to correct. In commercial market, citizens have the option to walk away from a service if they feel that the risk of using a particular IDM system is high but they don't have an option about in the case of IDM in Government systems. Therefore it becomes the responsibility of the government to ensure the security and privacy of the citizens using the IDM systems of the government.

In E-governance the accountabilities and responsibilities are not clear; this makes it difficult for the citizens to receive compensation. For example if a government online portal provides single sign on (SSO) services for

several agencies, it is not clear about which agency is responsible if the system fails. Responsibilities and accountability can fall under several parts of government hierarchy, the ministers responsible for a particular agency, the web –masters who designed the portal and the officials who approve or administer it.

Because of the direct marketplace pressures there is less incentive for the government to be responsive to citizens concerns. Even when they implement measures to address online concerns, they tend to manage their own risks first. Governments IDM systems usually take great care to provide information benefits and services to the wrong person but don't take equal measures to ensure that the citizens are interacting with legitimate government agencies. As now governments are now moving away from providing static information like office address to more significant services like filling tax return online, filling of online application forms for jobs and passport services etc. Therefore there is a need for a stronger IDM system so that the risks for the citizens of interacting with the wrong person should be managed.

4 APPROACHES TO IDENTITY MANAGEMENT SYSTEMS

Management of online identity is a major concern for governments and private sectors alike. Both have something to learn from each other. Earlier efforts have either attracted major controversies or have been withdrawn. For example Microsoft PASSPORT service was criticized because it gave the company too much control over users' personal information [1]. UK's entitlement card lost support from the users once they came to know the extent to which government controlled it.[12] But a notable outcome of these approaches of IDM systems is an increased debate about the overall approach to IDMs which is moving beyond the concerns of privacy as an abstract concept to a more concrete analysis of what actually concerns to those who object to IDM systems. Now referential frameworks are being developed by government and private sector which aims at providing consistency in designing security and privacy in IDM systems and hence they are gaining more community acceptance. The Australian government, for example, recently developed the Australian Government Authentication Framework for Individuals (AGAF).[11].New Zealand started its "all of government authentication program"[22]. In International context, London School of Economics has developed a set of best practices criteria.[14]. Europe's Prime project is working on a published set of principles.[15].Microsoft's Kim Kameron has developed the laws of Identity.

None of these approaches focus on compliance with privacy or data protection law. Recent research findings [9] understanding and management of risks associated with the online tool can be a determining factor in the acceptance of stronger IDM systems. The IDM systems should address the real concerns of individuals have about what happens to their personal information in an IDM system and regard user control as important to achieving a solution that gains user trust, usage and acceptance.

5 IDENTITY MANAGEMENT IN INDIA

India is one of the leading IT services providers to the businesses across the world with US$60 billion outsourcing industry [9]. It has experienced considerable growth in the domestic sector, which emerged as a vital IT investor. The predicted increase in the IT spending in the country is 16.3% (US$ 43.57 billion in 2012), as reported by IDCs report Indian IT Market Overview Report-2012 [17]. According to the report, expected IT spending in Small and Medium Enterprises (SME) would grow by 43% by 2015. These developments have attracted huge Government investments into IT enabled sectors. Government agencies are spending more than USD 10 billion in several of e-Governance projects [16]. Celnet's report [18] `Payment in India is going e-way', mentioned 30% of the total transaction are e-transactions and 75% of the total payment to be in the form of electronic payments. India was ranked 6th in the world with 61.338 million Internet users in 2009 [19], and is predicted to have the 3rd largest Internet user base by 2013 (Forrester's Research) [3]. Internet penetration is at about 7.1% but is marked to be rising exponentially. With the increase in the number of Internet users and increased penetration of technology in modern India's individual, the exposure to the e-threats and privacy breach has increased as well. These threats can cause potential damages to financial, social, and personal interests of the individuals, e.g. targeted advertising. The commercialization with e-facilities has lead to development of a large sector involved in targeted advertising. Realizing the frustration and annoyance caused by such services and to protect the users, schemes e.g. National Do Not Call registry and regulatory guidelines for banking industry, were introduced. This got some respite for the users but was not of much significance. The scope of consumer privacy in the country changed with proposed amendments in IT Act, getting privacy to the table of discussion among various fraternities e.g. legislation, social communities in the country. The last few years also witnessed conceptualization of countrywide projects such as UID (Aadhar) and NATGRID (National Intelligence Grid).

India, world's largest democracy, has witnessed enormous development in information technology over past few years. It has become a necessity to share personal information for every service, from getting a mobile phone connection to registering for online banking. India being a collectivist society has different expectations of privacy than other developed nations. Recent developments in the Indian scenario e.g. privacy bill, UID

project signify a need for privacy awareness and understanding in Indian masses. It is also important for policy makers to comprehend sentiments and opinion of masses for structuring elective laws and policies for the citizens of India. Indian culture may play a significant role in shaping attitudes about privacy. Cultural values are known to affect a population's attitudes about privacy [4], [5], [6]. Hofstede developed a number of cultural values indices to measure cultural differences between societies. According to Hofstede, India is a collectivist society with lower Individualism Index (IDV) and higher Power Distance Index (PDI) compared to the US, which is an individualist society with higher IDV and lower PDI. Hofstede has shown that individuals in collectivist societies have more trust and faith in other people than individuals in individualist societies [7, [20]. Indians' tendency to trust that their personal information will not be misused can be found in recent Indian popular news media reports that Indians are largely unaware of the extent to which databases of personal information are sold and traded among companies. When informed of this practice, the news media reports that individuals are often shocked and outraged. News magazine India Today, featured a cover story titled \Privacy on Sale," illustrated with a cover photo of a man with a bar code stamped on his head [21]. The Times of India featured a special report on The Death of Privacy" [8]. Similar stories have been showing up in the Western press for several years, but have only recently appeared in India. The Indian joint family tradition, results in more routine sharing of personal information among a wider group of people than is typical in the US. Information that might typically be disclosed only to one's spouse or parents in the US is more frequently shared among uncles, aunts, and cousins in India. In addition, as it is common for Indian businesses to be owned and operated by large extended families, personal financial information is typically shared fairly widely among Indians. The urban cities in India support a large population base. Each year witnesses increased migration from rural to urban areas leading society towards urbanization. India originally is a collectivistic society, exhibiting a culture of joint families and life driven by rules and norms of the society, but the increased urbanization is influencing society towards individualism. An increase in the Individualism Index (IDV) marks the beginning of individualism in India Society and also accounts for the increased awareness about individual rights. In spite of large proportion of population being uneducated and illiterate, the government is making constant efforts to get all individuals under IT enabled services and projects e.g. UID, NATGRID. Mobile phones have come out as an evident tool for large communities and have hence become inevitable for the individuals not to use services on the mobile phones. Increasingly services such as banking, insurance, and telecom are introducing Information Technology (IT) enabled services increasing the purview of IT on life. Various studies in the past [9], [10] have shown Indian population to be less sensitive to the privacy in comparison to countries of the world, significantly because of the collectivistic nature of Indian society. However, increased exposure to technology could lead to change in this behavior. In 2009, the Government of Indian launched the national database, a Unique Identification number (UID),which aims at providing unique numbers to all individuals. The numbers are assigned based on the biometric information of the individuals e.g. iris, fingerprints, etc. The project rose concerns in the country regarding privacy of the data collected as it had major privacy challenges to handle e.g. De-duplication, maintaining a large centralized database against privacy breach, etc. Another aspiring project, NATGRID by the government faced significant opposition due to the involved threats to the privacy of the Indian individuals.

6 IDENTITY MANAGEMENT IMPLICATIONS

Governments are rapidly developing and transforming national policies for identity management. If done well the rewards are remarkable; if done poorly, policy failure will be slow but nearly certain. Comprehensive identity policies involve creating or adapting schemes for the collection and processing of individual–specific data that will be shared across services, both within and beyond government, often for a variety of purposes. The range of bodies involved in such policy developments is extensive, raising important issues both for the government led implementation of such policies and for academics to study and engage the policy deliberations as they take place. In an age of 'identity management', when government seeks to define and to control identity, and the individual is overwhelmed by fears of identity theft and the all-seeing, intrusive state

When citizen uncertainty about government trustworthiness is an issue, approaches to IDM that factor in user control and user-centric approaches to risk are more likely to achieve community acceptance. The risk associated with online identity management is sometimes unfairly shifted to the citizen, who isn't always in a good position to bear it and might not be willing to do so. This shifting of risk can take several forms. For example, the citizen might

- Suffer financial loss by interacting with a fraudulent entity;
- Experience major life disruption through the loss of identity credentials or fraudulent misuse of those credentials;
- Be unfairly discriminated against by inappropriate secondary use of data trails left in the identity management system; or
- Bear the burden of dealing with these failures, including attempting to gain redress and returning life to normal.

To counter these problems, several mechanisms give appropriate levels of user control and help manage risk, but none of them are likely to be sufficient on their own. The type of organization and the nature of the technology used and how it's deployed are important in deciding the right mix. Other key factors include

- Education about the risks involved in an identity management system;
- Law as a way for government to make promises to protect citizens and back up those promises;
- Technology as a way of designing in security, risk, and control mechanisms.

Education, law, and technology on their own aren't enough to have a major impact on citizen privacy and life control—it also requires mechanisms that can demonstrate that the measures in place are actually effective. Good governance is essential to ensure that an organization spells out clearly what it will do in terms of control and allocation of risk, and very importantly, to prove that it does what it said it would do. Governance mechanisms should start with internal management metrics and feedback and extend to outward-facing mechanisms, such as reports to ministers, external audits, regulators, and any other continuous disclosure obligations. In particular circumstances, they can extend even further, to investigation and enforcement action.

7 CHALLENGES IN IMPLEMENTATION OF E-GOVERNANCE

7.1 Trust

The user must be confident, comfortable and trusting of the tool or technology with which they will interact. The user must also trust the government. There has to be a balance between ensuring that a system prevents fraudulent transactions and the burden that extensive checks can take place on people who are honest. Trust, along with financial security, are two critical factors limiting the adoption of e-government services.

7.2 Resistance to Change

The resistant to change phenomenon can explain much of the hesitation that occurs on the part of citizens in moving from a paper based to a Web-based system for interacting with government. Citizens, employees and businesses can all have their biases with respect to how transactions should be processed. However, government entities and public policy administrators cannot ignore the changes that occur as a result of the implementation of information and communication technology (ICT). Education about the value of the new systems is one step toward reducing some of the existing resistance.

7.3 Digital Divide

The digital divide refers to the separation that exists between individuals, communities, and businesses that have access to information technology and those that do not have such access. Social, economic, infrastructural and linguistic indicators provide explanations for the presence of the digital divide. Economic poverty is closely related to limited information technology resources. An individual living below poverty line does not afford a computer for him to harness the benefits of e-government and other online services. As the digital divide narrows, broader adoption of e-government in the public domain becomes possible. Economic poverty is not the only cause of digital divide. It can also be caused by the lack of awareness among the people. Even some of the economic stable people don't know about the scope of e-governance. Awareness can only help to bring users to that service delivery channel once. It cannot guarantee sustained use of the system unless the system is also designed in such a way as to deliver satisfactory outcome. Procedures need to be simplified to deliver concrete benefits and clear guidelines provided to encourage their use by the actual end users and reduce users' dependence on intermediaries.

7.4 Cost

Cost is one of the most important prohibiting factor that comes in the path of e-governance implementation particularly in the developing countries like India where most of the people living below the poverty line.

7.5 Privacy & Security

There are three basic levels of access exists for e-government stakeholders: no access to a Web service; limited access to a Web-service or full-access to a Web service, however when personal sensitive data exists the formation of the security access policy is a much more complex process with legal consideration .

With the implementation of e-government projects, effective measures must be taken to protect sensitive personal information. A lack of clear security standards and protocols can limit the development of projects that contain sensitive information such as income, medical history.

8 Tackling the Issues in Implementation of IDM in E-Governance in India

Some suggestions are for tackling the challenges in implementing IDM in E-Governance are

8.1 Enhancing Citizen Awareness

Citizen awareness about the potential of ICT should be enhanced. Citizen access to government information/services must increased rather than further divide the digital divide.

8.2 Upgrading Skills

There is urgent need to upgrade the IT skills of government employees. Employees must be effectively

trained before introducing desired changes in work process in government departments. Above all it must be ensured that trained specialists are on hand to provide support for users of ICT-based systems and services. A major cultural change is required among employees in government- citizen dealings.

8.3 Common Standards

All states/ union territories must be adopt common standards to ensure creation and optimum utilization of government databases for nationwide citizen-related service

.

8.4 Experience Sharing

Continuous experience sharing between state and union territory governments on projects so as to avoid reinventing the wheel.

8.5 Security

Transactional security must be given priority to ensure that internet use is safe, seamless and crisis free.

8.6 Reliable Infrastructures

Sufficient resources must be allocated to build a reliable ICT infrastructure to avoid breakdown of services. Cementing public-private partnerships to supplement government efforts must be considered.

9 CONCLUSION

As governments rush to develop new identity policies they fail too often in answering essential questions: are identity policies capable of addressing a diverse range of policy goals? Are the techniques we imagine to be necessary in fact helpful? *P*olicy makers remain fixated on expensive and biometrics and vast new centralized databases to solve problems they do not understand. Policy makers repeatedly commission identity schemes based on obsolete knowledge of modern technological capabilities. Policy making requires an understanding of technological issues as well as more traditional political and organizational concerns. As a result, policy makers can set about developing effective solutions that are citizen friendly and actually address pressing policy goals. The phases of planning, design, administration, and sustainability of identity management systems, are the key factors to enhance good governance, transparency, and accountability

References

[1] S. Pruitt, "Microsoft Ordered to Fix Problems." PC world, 8 August.2002;

[2] Godse, V. Policy paper: Privacy in India. DSCI (May 2010).

[3] Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. International Differences in Information privacy concerns: A global survey of consumers. The Information Society (2004)

[4] Boni, M. D., and Prigmore, M. Cultural Aspects of Internet Privacy. In Proceedings of the UKAIS 2002 Conference (2002).

[5] Fjetland, M. Global Commerce and The privacy clash. The Information Management Journal (January/February 2002).

[6] Hofstede, G. Cultural and Organizations - Software of the Mind – Intercultural Cooperation and its importance for survival

[7] Bhupta, M. Privacy on sale. India Today International.

[8] Ion, I., Sachdeva, N., Kumaraguru, P., and Capkun, S. Home is safer than the cloud! privacy concerns for consumer cloud storage. In Symposium on Usable Privacy and Security(SOUPS) (2011).

[9] Kumaraguru, P., and Cranor, L. Privacy in India: Attitudes and Awareness. In Proceed-ings of the 2005 Workshop on Privacy Enhancing Technologies (PET2005) (30 May - 1 June 2005).

[10] Kumaraguru, P., Cranor, L. F., and Newton, E. Privacy perceptions in india and the united states: An interview study. In The 33rd Research Conference on Communication, Information and Internet Policy (TPRC) (September 2005).

[11] www.agimo.gov.au/infrastructure/authentication/agaf/glossary/i#identitymanagement.

[12] http://is2.lse.ac.uk/idcard/

[13] https://www.prime-project.eu/prime_products/whitepaper/

[14] http://msdn2.microsoft.com/en-us/library/ms996456.aspx

[15] http://precog.iiitd.edu.in/research/privacyindia/PI_2012_Complete_Report.pdf

[16] http://articles.economictimes.indiatimes.com/2012-07-23/news/

[17] http://www.celent.com/reports/payments-india-going-e-way

[18] https://www.cia.gov/library/publications/the-world-factbook/geos/in.html

[19] Global online population to hit 2.2 billion by 2013. http:// www.pressreleasepoint.com/node/310679/pdf

[20] Hofstede, G. Geert Hofstede Analysis. Retrieved Oct 2, 2004., http://www.cyborlink.com/besite/hofstede.htm.

[21] Suraiya, J., and Vikas, S. The death of privacy. Times of India. http://timesofindia.indiatimes.com/articleshow/991395.cms

[22] A. McCue, "ID Card Support Collapses,"silicon.com,13 March 2006; agimo.gov.au/infrastructure/authentication/agaf_i),www.e.govt.nz/services/authentication

AUTHORS

Aparajita Pandey is an Assistant Professor at B.I.T.(MESRA),

Jaipur Campus. Her qualifications include B.E.(EEE) ,MBA. She is also a MCSE and has a diploma in Cyber law. She has teaching experience of about 10 years in the areas of Circuit Analysis, Data Communication and Computer Networks. She is also a member of IAENG and ISOC. Her research interests include Online Identity Management, Internet Trust,Privacy and Network Security.

Dr. Jatinderkumar R. Saini is Ph.D. from Veer Narmad South Gujarat University, Surat, Gujarat, India. He secured first rank in all three years of MCA in college and has been awarded gold medals for this. He is also a recipient of silver medal for B.Sc. (Computer Science).He is an IBM Certified Data Associate- DB2 as well as IBM certified Associate Developer- RAD. He has presented 14 papers in international and national conferences supported by agencies like IEEE, AICTE, IETE,ISTE, INNS etc. One of his papers has also won the 'Best Paper Award'.9 of his papers have been accepted for publication at international level and 13 papers have been accepted for national level publication. He is a chairman of many academic committees. He is also a member of numerous nation and international professional bodies and scientific research academies and organizations