TUTA/IOE/PCU

Journal of the Institute of Engineering
July 2019, Vol. ***15 (No. 2):*** *218-224*

E-government Use in Nepal: Issues of Database Management and Data Security

Shailendra Giri[1], Subarna Shakya[2]
[1]Personnel Training Academy, Bagdol, Lalitpur, Nepal
[2]Pulchowk Campus, Institute of Engineering, Tribhuvan University, Kathmandu, Nepal
Corresponding author: [2]*drss@ioe.edu.np* and [1]*edpta.sg@gmail.com*

Received: *March 12, 2019* **Revised:** *April 25, 2019* **Accepted:** *April 28, 2019*

Abstract: E-government uses information and communication technologies (ICTs) tools and systems to provide better public services. Database Management System (DBMS) is a very significant part in e-governance activities and process in the nation. Security of the data is a main concern of the organizations and private. Proper database management and data security are the major issues in present era. The aim of the paper is to try analyzing necessity of database management and data security. The author used survey methods during research to collect the data and analyze it. This paper concludes that the data backup is key profession while using computer in an institute or people. Hard disk, external hard disk, pen drive, memory card, server and open drive are the major storage Medias. People and employees don't create backup of data due to lack of knowledge, device and don't know about importance. The authors conclude that using Antivirus on computer, password on file and computer system, data and information backup, firewall, encryption and decryption technology are the data security tools. Data security protect against the unauthorized use, disclosure, access, destruction, modification and loss of data. Confidential password security and regular monitoring on password are very necessary to secure data. An online security system, as well as manual security systems, should be managed attentively.

Keywords: e-Governance, data security, communication technology, database management

1. Introduction

E-government uses information and communication technologies (ICTs) tools and systems to provide better public services to government agencies and facilitate their daily administration, citizens, and businesses to improve the quality of services. It provides greater opportunities for citizens to participate in democratic institutions and political processes [8]. The government of Nepal has been working towards a holistic e-government transformation to provide enhanced service to citizens, improve transparency and to work towards the knowledge based society [9, 26]. World Bank defines e-Government as utilized by government agencies of information technologies that have the ability to transform relations with citizens, businesses, and other arms of government [24]. The EU has advanced e-Government strategies than rest of the world, hence their definition

of e-Governance and the implications of ICT resources associated. ICTs are already widely used by government bodies but e-Government involves much more than just the tools [6]. The term “e-government" focuses on the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. The Internet and related technologies has the potential to transform the structures and operation of government [14]. The major operations of e-Government of Nepal are government portal, national ID, e-Education, infrastructure, enterprise architecture, Public Key, Integrated Data, Training Center and groupware [26]. The importance and application of e-government are well summarized in a document from the White House [27] are citizen-centered, not bureaucracy-centered; result-centered; and market-centered, actively promoting innovation.

Nepal is facing some challenges during e-Government implementation are information transparency, legal issues, resource availability, infrastructure including connectivity in rural areas, capacity and awareness, political will and government action, assessment of local needs and customizing e-governance solutions [10]. Nepal’s e-Government mission is to improve the quality of citizen’s life by providing value added quality services using ICT [15]. To realize the vision and mission, the consulting team worked out strategies and selected 33 projects in sectors comprising G2C, G2B, G2G and infrastructure. All the projects are vital for Nepal, but there is a limitation of time, budget, human resource and capability of implementing such projects. The priority has given by considering the availability of technologies, institutional readiness, emergency handling capacity as well as environmental impact [13]. Database management for e-governance, data security concern and e-government law are discussed in this paper. This paper also explores the importance of database management system and security.

2. Literature Review

2.1. Database Management for e-Governance

Database Management System (DBMS) is a very significant part in e-governance activities and process. The collection of data, processing, storage, and access are four factors in DBMS. Collection of data needs to be managed meticulously so that the information should be true [2]. The huge volume of data needs timely for decision making process [28]. The e-governance administrators can use this discovered knowledge to improve the quality of service. The government institutions are analyzing a large amount of current and historical data to identify new and useful patterns from the large dataset now [2]. The automated electronic system needs back up security; password security and power back up security for smooth operation, maintenance and protection and keep away from the threat, theft, damage or loss of software and database [16].

In the context of Nepal for the DBMS, the central government could manage the central data bank system and required data can be accessed from any corner of the country by the authorized person. If the system is authorized, the central government also could access the data if they need the data of the provincial and local government [3]. Three level of Government of Nepal must have a strategic vision of these problems. Heightening awareness of security issues must not be limited to promoting a culture of security. There should establish an information technology culture in daily life activities. The stakeholders must also be given the means to learn to manage the technological, operational and information-related risks they invite in using day to day coming new technologies [11] and steps must be taken to data security and to control the risk [1].

Most of the citizens and government personals are not making aware of the importance of the data protection and information security and effect of their loss. Few of the government employees have not knowledge and skill about data backup and recovery methods. Due to carelessness most of the people lose their data and information even though they have technical know-how [9]. Management must also consider the possible loss of reputation or competitive advantage, regularly and legal sanctions, and breach of contract if data falls into the wrong hands [16]. Development of ICT [22] is further creating problems from bad to a worse state, though it was originally used for the good purpose for the welfare of mankind. Data protection is the major concern of the people and they must duly contribute their quota as we all strive to restore peace, security, and stability in our nations. Nepal is lagging far behind, so, information security is weak in Nepal. If timely precaution is not taken to strengthen the situation could even be worst and people's trust in the e-governance may lose [23].

2.2 Data Security Concern and e-Government Law

Data security should protect against the unauthorized use, disclosure, access, destruction, modification and loss of data. Confidential password security and regular monitoring on password are very necessary. User and password security have not been maintained at a satisfactory level [17]. One of the preliminary steps in the assessment is to classify the data according to risk factors [16]. E-government system should be reliable and reliability can be maintained by sufficient existence and proper implementation of e-government law [7].

There is a need for information security best practices to protect e-government projects. Security policies, practices, and procedures must be in place as well as utilization of security technology. It helps to protect e-government system against attack, detect abnormal activities services and to have a proven contingency plan in place [20]. More than 3500 malicious websites are blocked per day and 89.4% mails are spam. The majority of the attacks (32%) are phishing followed by virus (29%) and network scanning/probing (18%) [4]. The comprehensive legal regulatory mechanism is needed to foster public trust and digital privacy and personal data protection has become an unavoidable provision for the specific form of e-government [7]. The e-government system should be supported by national laws and regulations for its legitimacy and legality [21]. Maintaining digital privacy and personal data protection scheme in e-government law is important to foster public trust [7]. The comprehensive legal regulatory mechanism is needed to promote public trust and digital privacy and personal data protection system has become an unavoidable provision for the specific form of e-government law [7].

The increased demand from society for the protection of privacy and personal data led several countries to develop their own privacy laws, for example the Australia Privacy Act, 1988, Finish Personal Data Act, 1999 and Open Government Data Guide Book, 2010, Korean Electronic Transaction Act, 1999 Consumer Protection Act on Electronic Transaction Act, 1998, Swedish Personal Data Act, 1985 [7]. In Nepal, there are several legal instruments created to develop IT sector for augmenting e-governance as IT Policy 2000, IT Policy 2004, Electronic Transaction Act 2004, Telecommunication Policy 2004, e-Governance Master Plan II, IT commitments in different plan periods, Electoral Transaction and Digital Signature Act 2000, Copyright Act 2000, Telecommunication Act and Regulation 1997, National Communication Policy 1992 and National Strategy Paper on ICT [18].

3. Methods

Data security is not only play the vital role in government organization but also in private organization too. Without database management and data security, the government could not move ahead securely. The researcher applied data survey method to collect data, analyze it and conduct the research. Government employees involve in survey at different part of the country. Books, journals, survey reports, government policy reports, acts and law are other references of research.

4. Results, Analysis and Discussion

Security of the data is a major concern of the organizations. Data security is the method of keeping data safe from accidental damage or other case. 86% of government employees concentrate on the security of data and information; this is stated in table 1. It claimed that the importance of data and security. Data Security focuses on protecting data rather than protecting the network where the data lives. Data security counter quantify helps guarantee the confidentiality, availability and honesty of information systems by preventing [12]. Due to awareness of data security and lack of Computer training many people and employees are unknown about database management and data security. So, they lose confidence.

Table 1: Security of data and information

No	20	14.0 %
Yes	120	86.0 %
Total	140	100.0 %

Source: Field work 2018

Civil servants have been using various methods to secure data in their organizations. With the help of table 2, we can say that how they secure data in government offices? Respondents answered: preferring antivirus software (70%), making a backup of all files (26.4%), using a password to protect computer (23.6%), and involving external technical to solve the problem (20%). Although, Antivirus software is dominating the market in the name of securing data but many duplicate Antivirus software are find in the market which are creating more problems to the computer users. Confidential password security and regular monitoring on password are very necessary [17]. Antivirus software, firewalls, digital signature, encryption and other technological tools support for protection data; computer networks are crucial for safe data but not sufficient to guarantee at all [12]. Data security should protect against the unauthorized use, disclosure, access, destruction, modification and loss of data. Hacker, crackers and thief are playing key role to get data by unauthorized access. World is losing huge amount of economy due to unsafely of data day to day. Future demands easy and smart new data security application and technology.

Table 2: Method of securing data:

Using antivirus software	98	70.0 %
Making backup of all files	37	26.4 %
Using password to protect computer	33	23.6 %
Involving external technical to solve the problem	28	20.0 %

Source: Fieldwork 2018

Data and information backup is major job of the civil servants in the organization. Table 3 showed that each organization backup their data and information, it is revealed by 77.9 % respondents. It is acknowledged that data and information back up is essential for future operation. People and employees don't create backup of data due to lack of knowledge, device, and negligence; and don't know about importance and impact of data loose. There are various data backup methods and devices are available in the market now.

Table 3: Is the information of your office secured and backed up?

No	31	22.1 %
Yes	109	77.9 %
Total	140	100.0 %

Source: Fieldwork 2018

Data and information are stored using different methods in government organizations. According to table 4, it is stated that the main way of backing up data is by using a hard drive (50.7%). Other methods are using pen drive (40%), putting the password in the workstation computer (35%), using external hard disk (27.9%), using servers (22.1%), using Google drive/ sky drive (6.4%). Cloud computing is being popular for data backup and access. Google drive and servers are not secure due to poor security concern in networking system and internet. Memory card, CD, USB, floppy disk may lose soon and loose data. At least two or three backup should create in an organization, individual and government offices. It is better to remain server in own country rather than others'.

Table 4: How information is backed up?

Using hard disk	71	50.7%
Using pen drive	56	40.0%
Using external hard disk	39	27.9%
Putting password in the workstation computer	49	35.0%
Using servers	31	22.1%
Using Google drive/ Sky drive	9	6.4%

Source: Fieldwork 2018

5. Conclusion

Database Management System (DBMS) is a very significant part in e-governance utilization and process. Security of the data is a major concern of the organizations and state. It declared that data backup is key profession while using computer in an organization or private. Hard disk, external hard disk, pen drive, memory card, server and open drive are the most important mass storage devices. It is acknowledged that data and information back up is essential for future operation. Few people and employees don't create backup of data due to lack of knowledge, device, and negligence and don't know about importance of data. Using Antivirus, fire wall, password, digital signature, encryption technology are major data and information security tools. The automated electronic system needs back up security; password security and power back up security, maintenance and

protection and keep away from the threat, theft, damage or loss of data and database. An online security system, as well as manual security systems, should be managed attentively. The further study should focus on innovate easy, smart and secure database management system as well as data security methods, application and technology.

Acknowledgement: I am thankful to my family and my staffs as well as Personnel Training Academy and Rapti Engineering College, Dang for their valuable support in my study.

References

[1] ARIR (2014), *Administration Reform Implementation Report,* High level administrative reform implementation and monitoring committee, Singhadarbar, Nepal.

[2] Arora RK and Gupta MK (2017), e-Governance using data warehousing and data mining, *International Journal of Computer Applications,* 0975–8887, **169(8):** 28-31.

[3] Baral C (2018), Electronic Government in Context of Nepal, *Journal of Personnel Training Academy,* Government of Nepal, **6(1):** 37-43.

[4] CAN (2010), National IT workforce survey-2005, *Computer Association of Nepal* (CAN), United Nation: E-Government Survey.

[5] e-Government Master Plan Consulting Report, Government of Nepal, http://www.nepal.gov.np/

[6] EU Digital Agenda, https://ec.europa.eu/digital-agenda/node/1033.

[7] Ghimire TB (2014), Data protection law and policy factor impact on public trust in e-government system in Nepal, *Journal of Personnel Training Academy,* **2(1):** 26-36.

[8] Giri S and Shakya S (2018), Effective service delivery using ICT for civil service in Nepal. *International Conference on Power, Energy, Signals and Automation,* 25-26 May, Chennai, India.

[9] Giri S and Shakya S (2018), ICT tools and service delivery: A case of Nepalese civil service, *Proceedings of Science Globe International Conference,* 10th June, Bengaluru, India.

[10] Giri S and Shrestha RL (2018), Reform of civil service of Nepal with e-government practice, *Journal of Personnel Training Academy,* **6(1):** 22-36.

[11] Giri S and Shakya S (2018), ICT and service delivery mechanisms in civil service of Nepal, *International Journal of Computer Science and Mobile Computing*, **7(4):** 47-52.

[12] Gurusamy V (2018), Cyber Security for Our Digital Life, *Proceeding: National Conference on Innovations in Computer Technology and its Applications, Guru Nanak College, Chennai.*

[13] http://ict4d.co/tag/egovernance/

[14] http://stats.oecd.org/glossary/detail.asp?ID=4752.

[15] http://www.doit.gov.np

[16] Kabir AH (2015), Data Centric Security, *National Security Institute J.,* Washington DC, **1(3):** 21-33.

[17] Kafle M (2017), E-government: practices in Nepal, *Journal of Personnel Training Academy*. Kathmandu: PTA, Nepal, **5(1):** 80-85.

[18] Kim YS (2007), *E-Governance Implementation Strategy in Least Developed Countries: A Nepalese Case,* Available at: http://delivery.acm.org (accessed 20 January 2019).

[19] KIPA (2006), Government of Nepal, e-Government Master Plan Consulting Report.

[20] Kumar D and Panchanatham N (2015), A case study on cyber security in E-governance, *International Research Journal of Engineering and Technology* (IRJET), **2(8):** 272-275.

[21] Pande RN (2017), E-governance and cyber security in Nepal, *Journal of Personnel Training*

Academy, Lalitpur: PTA, Nepal, **5(1)**: 30-38.
[22] Regmi M (2017), Strategies for e-government in Nepal's civil service, *Journal of Personnel Training Academy,* Lalitpur: PTA, Nepal, **5(1):** 86-101.
[23] Shrestha PS (2017), E-Government and its challenges in Nepal, *Journal* of *Personnel Training Academy,* **5(1):** 124-136.
[24] The World Bank "E-Government", http://go.worldbank.org/M1JHE0Z280.
[25] UNPAN Document, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf.
[26] Uns (2014), E-Governance: Nepal, United Nation's E-government Survey.
[27] White House, Office of Management and Budget 2002, The strategy of e-Government, Available at: http://www.whitehouse.gov/omb/inforeg/egovstrategy.pdf, Accessed on 24 February, 2019.
[28] Yildiz M (2007), E-government research: Reviewing the literature, limitations and ways forward, Government Information Quarterly, **24:** 646–665.