Study of Current Cyber Security Threats to Information & Operational Technology (IOT) and Their Effect on E-Governance in Nepal

Article *in* Journal of UTEC Engineering Management · January 2023

DOI: 10.36344/utecem.2023.v01i01.005

1 author:

Chandan Bhagat
SOE Madan Bhandari Memorial Academy
5 PUBLICATIONS **53** CITATIONS

JUEM
Research across Technical Disciplines

Journal of UTEC Engineering Management
Volume 01, Issue 01, 2023, Pg. No. 41-50
OPEN ACCESS

Research Article https://doi.org/10.36344/utecem.2023.v01i01.005

Study of Current Cybersecurity Threats to Information & Operational Technology (IOT) and their Effect on e-Governance in Nepal

Chandan Kumar Bhagat

Assistant Professor, School of Engineering, Madan Bhandari Memorial Academy Nepal (Urlabari), Pokhara University, Nepal.

INFO

Corresponding Author
Chandan Kumar Bhagat
Assistant Professor, School of Engineering, MBMAN, Urlabari Morang, Pokhara University

E-mail
c.bhagat03@gmail.com

Orcid
https://orcid.org/0009-0009-3699-3247

Date of Submission
February 12, 2023

Date of Acceptance
June 5, 2023

ABSTRACT

As the development of digitalization process spreads worldwide, daily necessity and dependability on World Wide Web is increasing. Now after global pandemic of Coronavirus disease (COVID-19), digitalization has become compulsory process in the world. The process of digitization in Nepal is also increasing. Along with the process of digitization in Nepal, there is also a huge possibilities of cyber security threat.

Today, the information security system must be set up to counter emerging vulnerabilities that may additionally arise as a result of technological development and advancement. In the complex and dynamic arena of Internet, the challenges inherent in protecting Information infrastructure is significantly increasing, maybe as an influence of the global existence of services etc. Depending on these networks. These network links are unprotected to cyber-attacks due to more than a few flaws in the system. Therefore, it is necessary to accelerate on the protection that covers the software and infrastructure to provide the governance fruitful interconnection besides any probable hazard of being arranged. This research tries to find out the cyber security problems in the present concern as technological innovation is moving each and every sphere of existence so as e-Governance applications. Research additionally emphases on how e-Governance is made more protected and what type of security and protection mechanism to be implemented, have to be safe, tightly closed and dependable surroundings via numerous technologies in digital Governance functions i.e. cloud computing, e-commerce, social networking, e-Banking/Internet Banking system, e-Payment and also outline here in what way to reduce the Online crimes through strengthening the safety components of e-Governance systems.

Keywords: Cybercrime, Cybersecurity, Cyber Threats, e-Governance, IOT, NITC, Information Communication Technology, Security Breaches, G2C

How to cite this article: Bhagat C.K.., (2023). Study of Current Cyber Security Threats to Information & Operational Technology (IOT) and Their Effect on E-Governance in Nepal., JUEM 1(1), 41-50. https://doi.org/10.5281/zenodo.8116802

INTRODUCTION

As said by Richard Heeks, e-Government is the application and use of information technology (IT) by public sector organization i.e. government. E-Government is thus not just about the internet technology. The expansion of new information and communication technologies (ICTs) has significantly enhanced our capabilities to collect, process, and distribute information (Bhagat et.al, 2021). About all developing countries regard ICTs as an important factor while preparing their national development plans.

The increasing digitization of organizations and the associated networking of almost all regions are generating remarkable commercial potential. At the same time the improved networking is giving upsurge to new threats that need a quick and rigorous reaction. The constant increase in the figure of cyber-attacks (Bhagat et. al., 2021) in recent years has urged policymakers to make conforming procedures and protocols for cybersecurity. The aim of these requirements is to safeguard critical infrastructures in order to guarantee continuous services to citizens and strength to the country. Cybersecurity implies to the capability of controlled access to network, systems and the data they have. Digital infrastructure is considered a reliable and trustable cyberspace where cybersecurity measures are effective. The scope of cybersecurity covers the security of IT systems within the organization, the digital systems upon which they rely including critical infrastructures and cyberspace. Cybersecurity impacts the development of Information Technology and Internet services to a great extent. It is essential to improve cybersecurity to have protected critical information infrastructure for country's security and commercial viability (Bhagat et. al 2021). Dependency on Information Technology of the public has increased in all areas of human activities such as e-commerce, finance, health care, energy, entertainment, media, and national security (Dahal, 2017).

OBJECTIVES

- To study cyber threat's cases and trends related to Information & Operational Technology (IOT).
- To analyze the problems, challenges and effect of cyber threats on e-governance in Nepal.

Review of the literature As a Research Method

The Literature Review method is used for the study. Several reports, national and international journals, Websites are the references materials for the study (Mishra, et.al., 2022). In relation to economic development smart village concept seems to be promoted here. (Mishra & Aithal, 2021; Pokhrel, et.al., 2021).

LITERATURE REVIEW

This paper discussed Cyber Laws and policies in Nepal, e-Government implementation in Nepal, E-government Implementation Issue in Nepal, Similarly, the most common threats, ICT and e-Governance, Applications of E-Governance in Nepal, Cybersecurity and E-Government, Effect of Cybersecurity Threats on E- Governance, Latest Trends: Cyber Crime, Global Cyber Crime Figures, Cyber Crime & Its Effect in Nepal, Finding & Conclusion

Cyber Laws and Policies in Nepal

Table 1: Cyber Related Laws & Policies in Nepal

SN	Name of the Document	Cyber Activity and Cyber Security Related Major Provisions
1.	Constitution of Nepal 2072	Article 19 says for the right to communication
		Article 27 says for the right to information as, a fundamental constitutional right..
2.	Electronic Transaction Act, 2063 (2006 AD) (ETA 2006)	There is the provision relating to electronic records and digital signature, provision relating to the computer network and network services providers, provision relating to computer related crimes and punishments etc.

SN	Name of the Document	Cyber Activity and Cyber Security Related Major Provisions
3.	Telecommunication Act, 2053 (1997 AD.)	It is an active legal instrument to regulate cyber related activity in Nepal
4.	Mobile Device Management Systems By laws 2075 (2018) (MDMS Bylaws)	It is an implementation of Equipment Identity Register (EIR) system to ensure national and consumer security,
		To detect the genuine mobile handsets and make the fake and non-genuine handsets in- operable in Nepal,
		According to this illegal mobile devices not registered in NTA are banned
5.	Online Child Safety Bylaws 2076	To make a secure internet for children that Internet Service Providers (ISPs) / Mobile Network Operators (MNOs) need to do, that families and communities need to do, and NTAs need to do.
		According to this, ISPs / MNOs are given instruction to show whether the available content on the Internet is suitable for the age group of children or not.
6.	Cyber security By laws 2077	This bylaw has agreed a check list for IS audit. This checklist contains 70 checklist questions. This includes questions related to 1) Standards and Prac tices, 2) Infrastructure/Network Security, 3) Core System Security, 4) Application Security, 5) Data Security/ Privacy, 6) IS Audit, 7) Cloud Security,8) CERT/Incident Response, 9) Security Operations Centre (SOC) 10) Cyber Security Awareness & Capacity Building and 11) Miscellaneous.
7.	Secure Password Practice	It has supplied to the employees working in various organizations of the Government of Nepal by compiling password security criteria and suggestions on what kind of password should be kept in office related work.
8.	National Information and Communication Technology Policy, 2015 (ICT Policy 2015)	ICT policy 2015 essentially focused on "Digital Nepal".
		Also mentioned is the establishment of a Computer Emergency Response Team (CERT) and a cyber-security cell in the ministry of communication and information technology. It is mentioned that the capacity building program will be conducted for law enforcement agencies and cyber security education programs for publics.
9.	Digital Nepal Frame work, 2076	The aims of this framework are to build the foundations of an information based society and digital economy, to achieve the goals of development and prosperity by making maximum use of digital technology, and to make public services available to the general public in a simple and easy way.
		In this agenda, 8 major areas have been selected ed. This includes digital foundations, agriculture, health, education, energy, tourism and finance and urban infrastructure. Under this, 80 initiatives have been identified.

SN	Name of the Document	Cyber Activity and Cyber Security Related Major Provisions
10.	National Security Policy, 2075	This contains some issues related to cyber space and cyber security. Policy No. 1.7.10 mentions the misuse of science, technology and modern equipment as an element affecting national security.
		Likewise, 1.9.2.4 of the policy mentions the misuse of modern technology in crimes under law and order related challenges and threats.

(Source: Study, 2021)

Active Organizations controlling cybersecurity in Nepal

Few of the remarkable organizations actively at work in cybersecurity are: Information Security Response Team Nepal, Center for Cyber Security Research and Innovation, One Cover Private Limited, CryptoGen Nepal (Source: Study, 2021)

E-government Implementation in Nepal

The main principle of good governance are accountability, transparency, responsiveness, and effectiveness and efficiency. These principles can be achieved through e-government (Cybercrime Statistics 2023:Femi Falana, 2008). In regard to these objectives of digital government, the government of Nepal has made e- government Master Plan (e-GMP) for e-government execution and transformation. Though there are some missing essentials in the master plan (e-GMP), it may lead to the fruitful implementation and the execution of e-government in Nepal. All plans are continuously progressed so that the e-GMP can be evaluated and updated for better result. Due to lack of Act, and Law, lack of proper monitoring, evaluation and coordination between government agencies and citizens, e-GMP seems not to be effective.

Cybersecurity & E-Government

As said by Adhikari, (2012) cybersecurity is generally concerned with information privacy, reliability and accessibility. It is also responsible to protect information, system and network infrastructure against cyber threats. These features strengthen services such as verification of manipulators and users, permission, accountability and reliability. While we talk about the wider perspective cybersecurity includes public and technologies both. Protocols of data and information security have been established through the expertise of leading hi-tech nations and are easily available in the open literature (Adhikari, 2007). For effective implementation of data and information security framework these protocols frame should have various policies and procedures (Gautam, 2007).

ICT and e-Governance

Information and Communication Technology (ICT) plays vital role for the successful implementation of digital government or e-Government. The four mail pillars of e-Government are connectivity, knowledge, data content and capital (Ghimire 2017, Giri et.al, 2018). Information and Communication Technology (ICT) is responsible for connectivity and data transmission and storage. Therefore, in the era of Science, Technology and Innovation, effective use of ICT is vital to encounter the ever-growing outlooks of citizens and businesses. From mere computerization, e-Governance is constantly developing to offer access, fairness & empowerment to masses. Nagaraja (2016) defined "E-Governance" as the use of ICT to convert the usefulness, efficiency, transparency and responsibility of transfer of data and transaction between government, between government organizations, between government and citizens, between government and business. Through e- governance, government services will be made available to citizens in a convenient, efficient and transparent manner. (Goswami, 2018). Four pillars of e-Governance are the Connectivity, knowledge, data content and capital (Goswami, 2018)

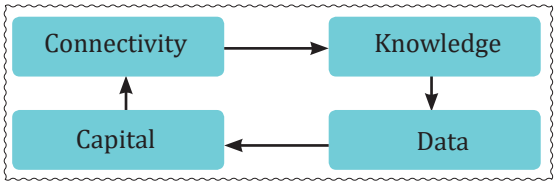

Figure 1: Four pillars of e-Governance

As per Nagaraja (2016) Via e-Governance with ICT , government services will be made available to citizens in a convenient, efficient and transparent manner (Goswami, 2018).

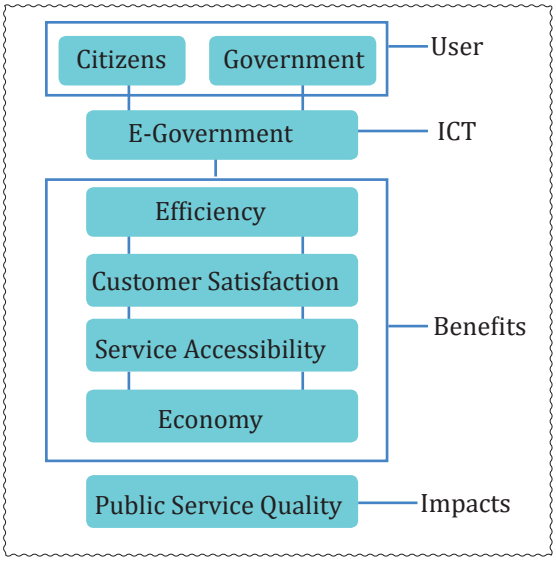

Figure 2: Activity Flow

Applications of E-Governance in Nepal

E-governance provides government services to citizens in a convenient, efficient and transparent manner. Few of them are enumerated below (Kumar and Panchanatham, 2015): G2C Services, PSC e-Services, Validate VAT/PAN, VAT registration, E-License, Internet Banking/E-Banking, National ID Card/ Nagrik App, E-Tender etc.

Most common threats

Network operation

- ***Packet sniffers:*** Data interception and analysis of traffic;
- ***Ping sweeps:*** Request for IP addresses of running machines;
- ***Port scanner:*** Scanning open TCP and UDP ports;
- ***Phishing:*** Technique of finding the necessary information directly from network users.
- ***SQL injection:*** To hack websites, data and programs that work with
- ***IP-spoofing:*** Via somebody else's sender's IP address to defraud the security system;
- ***DNS-spoofing:*** Altering domain name cache data
- ***DHCP-spoofing:*** Replacement of a default gateway.
- ***Password attacks:*** Password cracking and hacking;
- ***Spamming:*** Misuse of email capabilities.
- Technological advancement with Weak Security:
- Technological advancement is happening every day.

Most likely, new devices have Internet access in some form or other but no strategy for security.

This reveals a very severe threat – each unsafe connection means susceptibility. The fast growth of technology is evidence to researchers, yet safety lags critically [16].

Effect of Cybersecurity Threats on E-Governance

Digital Governance influences usage of digital techniques to transmit and ensuring data to citizens and entrepreneurs. Today, payment of ISP Bills, electricity, telephone and any other types of bills is done online. Everybody is dependent on internet and when peoples depend on internet services all that come in e-Governance and any effect on IOT will definitely affect e-governance as it uses ICT infrastructure.

E-Governance applications permit citizens and corporates to perform trade management online which could else need "a journey to business district". Organizations are benefited, too, by means of reduced administration, better

records, and improved efficiency (Kumar and Panchanatham, 2015). Information and ICT can boost the reformation of task principles by helping various sectors, providing improved governance facilities to people, better governance dealings with trade and commerce, enabling citizen accessibility of data and involvement for policymaking and further resourceful governance administration. ICT effectivity in governance is prudently related to capability of Governance to inculcate a perception shift environment in organizations which is essential for transparent working and creation of expertise and its exchange. E-Governance leverages usage of digital technics to transmit and ensuring data to citizens and entrepreneurs. Nowadays, payment of water, electricity, telephone and any other types of bills is done online. Everyone is reliant on internet and when peoples depend on internet services all that come in e- Governance and any impact on IOT will definitely affect e-governance as it uses IOT infrastructure.

The possible incidents an IOT network may face include the following:

- Choked or deferred movement of information through IOT networks (Information Security Form, 2018; Cybercrime Statistics, 2022), which in turn could delayed e-Governance services.
- Illegal modifications to commands, instructions, or alarm limits, that may harm, deactivate, or shutdown devices (Nagraja, 2016; Kumar & Best, 2006), generate ecological effects, and/or jeopardize human life.
- Incorrect data sent to system operators, either to mask illegal changes, or to act the operators to initiate unsuitable actions (Mark Jamison, 2016; Silwal et.al.2013), which could have numerous undesirable effects.
- Industrial control system (ICS) software or configuration settings altered, or ICS software diseased with malware (Pandey & Patel, 2017; Shachtman, 2017), which could have several adverse effects on services rendered to citizens through ICS setup.
- Intervention with the functioning of protection equipment (Mishra & Pokharel, 2023), that may jeopardize human life.

The possible Emerging incidents an IOT network may face include the following:

Criminal/illegal modifications, configuration settings altered, Intervention with the functioning of protection equipment (Kumar & Best, 2006; Silwal, 2013).

- ***Convergence of IOT:*** Integration of modern ICS with corporate LAN for remote monitoring and control and allowing remote access of ICS to vendors and support personnel, these rights of access to ICS invite many openings to breach security such as:
- ***Denial of Service (DoS) attacks:*** Invalidated sources and inadequate access rights permit attackers in harming OT systems to perform DoS attacks on vulnerable unpatched systems. ICS are open to usually known TCP/IP DoS attacks like SYN flooding, low-rate DoS (LDoS) attacks influencing TCP's retransmission time-out mechanisms, or buffer-overflow scenarios [18].
- ***Use of outdated and open source protocols:*** ICS operations normally use outdated, insecure protocols such as FTP and Telnet. Modbus/TCP, Ethernet/IP and DNP3 SCADA communication protocols of ICS for control devices normally do not need any validation to remotely execute commands on a control device, and no encryption replacements available (Mark Jmison, 2016).
- ***Absence of Basic access control implementation:*** Most devices need most basic access control isolating framework software mode versus application program mode. Server and terminal authentication is either not exist or entirely useless.

Distinction of access rights among administrators and end users is usually absent or not employed (Mark Jamison, 2016).

- ***Man-In-The-Middle Attacks:*** Network intruders can influence in-transmission directions, commands, or alarms due to absence of encryption and mutual authentication of ICS. Reiteration attacks can activate automatic system reactions affecting in erratic malfunctions. Prompting system operators to take wrong and probably risky human intervention due to wrong monitoring data presented by spoofing bouts. Network sniffing may expose secret data to invisible seizure for governmental or industrial spying, radical attacks, or felonious chases (Mark Jamison, 2016; Silwal et. al 2013).
- Corrupted Control System Device-Control logic software is not secure and can be smoothly changed. Corrupted devices can end in system harm, disruption, or safety hazards. Firmware is not secure, making it possible to change configuration settings or push malicious code over Ethernet in many cases. Successive device failure or random functionality may result in DoS events (Information Security Forum, 2018).
- Technological Advancement with Weak Security: Technological advancement is happening every day. Most likely, new devices have Internet access in some form or other but no strategy for security. This reveals a very severe threat – each unsafe connection means susceptibility. The fast growth of technology is evidence to researchers, yet safety lags critically (Pandya & Patel, 2017).
- Insufficient Security Expertise – Spending in software that observes the safety of a system has become a rising movement in the enterprise space after 2014's lapses of information breaches. The software is programmed to provide alarms when invasion efforts happen, yet the alarms are only valued if somebody is accessible to resolve them. Businesses are trusting too greatly on machinery to entirely defend against bout when it is intended to be a managed technology.
- Mobile Malware: Security specialists have perceived threat to mobile device safety since the initial phases of their access to the Internet. The nominal mobile filthy act amid the long list of latest occurrences has users far less worried than they would be. As our culture's strong dependence on mobile phones and how slight cyber offenders have targeted them, it generates a shattering hazard.
- **Access through Third-party:** Cybercriminals desire the route of least resistance. Goal is the poster boy of a key set-up attack through third-party entry points. The international retailer's HVAC dealer was the unlucky supplier whose IDs were whipped and used to snip commercial data records for 70 million clients (Pandya & Patel, 2017).
- **Default Configuration:** Big data tools have the facility to be tailored to suit an organization's requirements. Firms remain to disregard the significance of correct security configuration settings. The New York Times became target to a data breach as a consequence of applying only one of the few, critical functionalities desired to totally shield the origination's information
- **Obsolete Security Software:** Updating security software is an elementary technology management exercise and a required move to protect massive data. Program is developed to protect against identified risks. That implies that any new wicked code that knockouts an old form of security software will go unnoticed (Pandya & Patel, 2017).

Others

Supply chain attacks, Internet of Things (IoT) devices, Social engineering, Phishing attacks Spoof website and enter credentials, or download malware, gives hackers the tools needed to escalate attacks.

- From there, serious threats like ransomware can be delivered.
- Cybercrime on social media
- Fake lottery scams in Nepal.

Global Cyber Crime Figures

- As per study, 2021, there were about 97 data breach victims each hour worldwide.
- It was seen that the ratio of attacks against organizations by continent in 2021 is as follows(Information Security Forum, 2018).

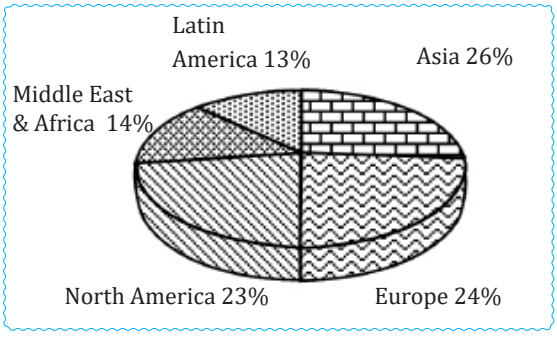

Figure 3: Percentage of Attacks Against Organizations in 2021

Cyber Crime in Asia

Cybercrime in Pakistan

Financial fraud, most of the Pakistani people have experienced cybercrime through social media like Facebook

Cybercrime in India

There have been most of the Indian websites hacked in recent years. It was found that, in 2018, about 17,560 sites were hacked. Similarly, in 2020, further about 26,121 sites were hacked. Besides of these crimes 78 % of Indian organizations experienced a ransomware attack in 2021 (Information Security Forum, 2018).

Cybercrime: Some Common Cases in Nepal

While in case of Nepal, Among the many cybercrime incidents reported recently. Some of the commonly reported incidents include: Bank ATM attacks, Ransomware, Spear phishing, Privacy leaks, Child pornography, Dissemination of mendacious information.

In 2017

- The authorized website of the Department of Passport became hacked by a team of Turkish hackers and defaced with threatening notes to expose the government's data.
- Similarly, SWIFT system of Nepal Industrial and Commercial Bank (NIC Asia Bank) was reportedly hacked by an unidentified hacker. They captured USD 4.4 million
- In 2019, when five Chinese people found hacking the Nepalese ATM server around Kathmandu Valley.
- The Hacker succeed to hack the ATM Machine after injecting the malware in the ATM machine. In this cybercrime, Chinese hackers robbed Rs 17.6 lakh in total. *(Source: Study, 2021)*

Other Case

- As per Kathmandu Post, 19 government departments' websites became hacked
- According to Nepal Police, there were 132 cases reported during 2017, and they reported just 53 cases of cybercrime in 2016. *(Source: Study, 2021)*

CONCLUSION

It is apparent from above literature review that cybersecurity is an integral element of each e- governance drive. Digital security, operational secrecy and availability of data online are vital. In e-governance programs, security of governance policies and related critical documentations is required from illegal users. Study indicates that cyber threat's cases and trends are in increasing order along with the technology's development. Above study also shows that e-governance combined with security setups delivering appropriate safety is

the prerequisite of any system design objective. Further, each government must spend additional on these initiatives to make governance useful, transparent, accessible and safer in order to boost public confidence in good representative e-governance.

Future Scope

Following are some of the questions identified for future study:

- Cyber Risk Assessment and its Mitigation aspects related to e-governance in Nepal.
- Effective Cybersecurity Framework in Nepal.

References

[1] Bhagat, Chandan and Sharma, Bharat and Mishra, A.K., Assessment of E Governance for National Development – A Case Study of Province 1 Nepal (2021). Chandan Bhagat et al; East African Scholars J Eng Comput Sci; Vol-4, Iss-4 (May, 2021): 46-52, https://ssrn.com/abstract=3857194

[2] Bhagat, Chandan and Sharma, Bharat and Mishra, A.K., (2021). Critical Success Factors for the Implementation of E-Governance -A Case Study of Province 1 Nepal. International Journal of Interdisciplinary Research in Arts and Humanities (IJIRAH), Volume 6, Issue 1, 2021, https://ssrn.com/abstract=3857190

[3] Bhagat, C., Mishra, A. K., & Aithal, P. S. (2022). Model for Implementation of e-Government Services in Developing Countries like Nepal. International Journal of Case Studies in Business, IT, and Education, 320–333. https://doi.org/10.47992/ijcsbe.2581.6942.0199

[4] Cyber Crime Statistics (2023). https://aag-it.com/the-latest-cyber-crime-statistics/

[5] Dahal, K. R. (2017). Utilization of experience civil servants. Public Service Journal, Kathmandu: Public Service Commission, Nepal. 1(1). Pp. 38-47

[6] Femi Falana, (2008). "Challenges of democratic transition in Africa | Pambazuka News," https://www.pambazuka.org/governance/challengesdemocratic-transition-africa.

[7] G. P. Adhikari, (2012). "Evaluation of e-Governance Projects of Nepal," Proc. 6th Int. Conf. Theory Pract. Electron. Gov., pp. 472–473,

[8] G. P. Adhikari, (2007). "Key issues in implementing e-governance in Nepal," in Proceedings of the 1st international conference on Theory and practice of electronic governance - ICEGOV '07, p. 243.

[9] Gautam B P, (2007). "Opportunities and Challenges of Tourism Financing A Study on Demand and Supply; Status, Structure, Composition and Effectiveness of Tourism Financing in Nepal", Florida USA 2008. ISBN-10: 1-59942-661-7.

[10] Ghimire Bishnu (2013). E-Governance and Its Role in Service Delivery", The Nepalese Journal of Public Administration. Ministry of General Administration.

[11] Giri, Shailendra, Shakya Subarna & Pandey Rose Nath. (2018). E-Governance Implementation: Challenges of Effective Service Delivery in Civil Service of Nepal. Global Journal of Computer Science and Technology: G Interdisciplinary, Volume 18 Issue 3 Version 1.0

[12] Goswami, A. (2018). Impact of Cyber Security in different Application of E-Governance. Journal of Advances and Scholarly Researches in Allied Education, 15(4), 65–70. https://doi.org/10.29070/15/57309

[13] https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline%20Cyber%20Crime%20Statistics&text=Data%20breaches%20cost%20businesses%20an,a%20cyber%20attack%20in%202022.

[14] Information Security Forum. (2018). Threat Horizon (2020). Information Security Forum.

[15] Kumar, D., & Panchanatham, N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.

[16] Kumar, D., & Panchanatham, N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology. https://www.irjet.net/archives/V2/i8/IRJET-V2I846.pdf

[17] Nagaraja, K. (2016). E-Governance in India: Issues and Challenges. IOSR Journal of Economics and Finance, 7(5), 50-54.

[18] Kumar, R. & Best, M. L. (2006). Impact and Sustainability of e-government services in developing countries: Lessons learned from Tamil Nadu, India. Information Society.22, I-12. (Available at: http://citeseerx.ist.psu.edu/ viewdoc/download?oi=10.1.1.162.1637&rep=rep1&type=pdf)

[19] MARK JAMISON, "ICT essentials for rebuilding fragile states," 25-Oct-2016. https://blogs.worldbank.org/ic4d/ict-essentials-rebuildingfragile-states?CID=ECR_TT_worldbank_EN_EXT. [Accessed: 16-Feb-2018].

[20] Mishra, A. K., Pokharel, R. (2023). Economic Feasibility Assessment of Smart Village Project: A Case of Sandakpur Rural Municipality, Ilam, Nepal. In P.K. Paul, S. Sharma, E. Roy Krishnan (Eds.), Advances in Business Informatics empowered by AI & Intelligent Systems (pp 138-160). CSMFL Publications. https://dx.doi.org/10.46679/978819573220310

[21] Mishra, A. K., Singh, M. K., Gautam, D., Bhagat, C. (2022). Assessment of Compact Minkowski Fractal Microstrip Filter for Band Applications. Journal of Emerging Technologies and Innovative Research (JETIR), 9(5), 423-428, https://zenodo.org/record/6538787

[22] Mishra, A. K., & Aithal P. S., (2021). Foreign Aid Contribution for the Development of Nepal. International Journal of Management, Technology, and Social Sciences (IJMTS), 6(1), 162-169. https://doi.org/10.5281/zenodo.4708643

[23] N. Silwal, T. C. Bruneau, and A. (2013), Federalism in Nepal: Divergent Perception and Convergent Requirement for Democratic Consolidation.

[24] Nagaraja, K. (2016). E-Governance in India: Issues and Challenges. IOSR Journal of Economics and Finance, 7(5), 50-54.

[25] Pandya, D. C., & Patel, D. N. J. (2017). Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. IOSR Journal of Computer Engineering, 19(01), 04–07. https://www.iosrjournals.org/iosr-jce/papers/Vol19-issue1/Version-4/B1901040407.pdf

[26] Pokharel, R., Mishra, A., K., & Aithal, P. S. (2021). Practicability Assessment of Smart Village Project: A Case of Sandakpur Rural Municipality, Ilam Nepal. International Journal of Management, Technology, and Social Sciences, 265–281. https://doi.org/10.47992/ijmts.2581.6012.0170

[27] Shachtman, N. (2017). Exclusive: Computer Virus Hits U.S. Drone Fleet. Retrieved from https://www.wired.com/2011/10/virus-hits-drone-fleet/

Abbreviations:

ICT: Information Communication Technology,
IOT: Information & Operational Technology,
NITC: National Information Technology Center,
PSC: Public Service Commission,
G2G: Government To Government,
G2C: Government To Consumers