INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Security ambiguity and vulnerability in G2C eGovernance system: Empirical evidences from Indian higher education

Sumeet Gill[1], **Priya Vij**[2]*

1 Supervisor, Department of Mathematics, MDU, Rohtak, India
2 Scholar, Department of Computer Sciences and Applications, MDU, Rohtak, Tel.: 9896727273

OPEN ACCESS

Received: 18-08-2020
Accepted: 09-09-2020
Published: 16-09-2020

Editor: Dr. Natarajan Gajendran

Citation: Gill S, Vij P (2020) Security ambiguity and vulnerability in G2C eGovernance system: Empirical evidences from Indian higher education. Indian Journal of Science and Technology 13(34): 3515-3520. https://doi.org/10.17485/IJST/v13i34.1373

***Corresponding author**.

Tel: 9896727273
pvij40@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

The Higher Education Institutions (HEIs) in India enhanced dependency on Information Communication Technology (ICT) based on G2C eGovernance applications persistently raised apprehension regarding cyber-attacks and breach of security. **Objectives**:The present study assesses the status of ambiguity and vulnerability pertaining to security aspects of HEIs G2C eGovernance web portals. **Methods**:Five prominent central and state HEIs i.e. Malaviya National Institute of Technology - Jaipur (MNIT), National Institute of Technology - Kurukshetra (NITK), Guru Nanak Dev University -Amritsar (GNDU), Maharshi Dayanand University – Rohtak (MDU), and Bhagat Phool Singh Mahila Vishwavidyalaya – Sonipat (BPSMV) were included in the study and Grey Box penetration testing method through open-source software's Whois.sc, Yougetsignal.com, Kali Linux, Builtwith.com, NMAP, and Google Hacking Database (GHDB), etc. along with social engineering testing through external penetration strategy was applied to assess the ambiguity and vulnerability of HEIs. **Findings**:The analysis revealed that login IDs and passwords related to web portals, eResources, networks, etc. are freely available and shared without any authorization which is a major cause of security breach. The vulnerability test depicted unencrypted communication between the HEIs portals and servers and the absence of well-articulated security and privacy. **Novelty**: The study exhibits the lenient view of HEIs administration towards security aspects of G2C eGovernance projects and the outcome would enable the HEIs of India to develop a comprehensive security policy for enriching and securing the G2C eGovernance System.

Keywords: eGovernance; security; ambiguity; vulnerability; privacy policy; social engineering testing

1 Introduction

The conception of eGovernance is barely few decades old but its significance is well evident the way G2C eGovernance applications facilitate government processes expeditiously and with enhanced transparency and accountability to evolve

into eSociety. Research outcomes endorse the use of ICTs and Web2.0 as a means of supporting Planning, eSociety, and eParticipation [1]. Gov2.0, as a strategic digital facilitator supports, the establishments to empower and enhance the citizen participation digitally [2]. Nations across the globe are determined towards the transformation of governance into eGovernance, to enhance connect with citizens to understand the real needs and works for the welfare of the society and also to empower the citizens to participate actively in policy making and implementation. However, the issue related to secure transactions in G2C eGovernance always remains crucial [3].

Cloud computing also evolved as web-based technology work in collaborations with various channel partners support facilities viz. eGovernance, eLearning, cloud-based ERP but security is a major concern [4]. Incidents of sensitive and crucial information leaks on web urged towards security control critical in G2C eGovernance network design [5]. Considering the vulnerabilities and security threats clear gap was evident while tracking and validating transactions. Blockchain Technology (BCT) can address the issues related to public services especially related to corruption and public data management [6]. The use of RSA based multi-server authenticated common login credential to access diverse G2C eGovernance services offered by various government agencies is also proposed [7] however, articulating consensus between diverse government agencies operating at national, state and district level is a challenging task and social and political factors also play a considerable role in it.

Along with the advent of ultramodern technology, the complexity of the G2C eGovernance systems has also been augmented and elevated novel challenges related to data privacy and security (Figure 1). Lack of vision and absence of security and privacy policy have occurred as the biggest hindrances that demand benchmarking of G2C eGovernance systems to acquire the trust of the stakeholders by identifying all possible threats and vulnerabilities in eGovernance Projects [8]. Studies acknowledged institutional trust substantial relationship with persistent intention to use and eWoM of eGovernance systems [9]. Disturbing privacy and security risks associated with eGovernance services ranging from eBanking to eEducation growing and serious concern amongst the stakeholders and the same needs to be addressed judiciously. Further, the need to sensitize citizens regarding perceived risks is also identified [10].

In March 2018, over 300 Universities worldwide were affected because of cyber-attack and more than 100,000 professors' email accounts were targeted and about 8,000 of them were finally compromised and 31 terabytes of "valuable intellectual property and data" was exposed [11] [12]. The chances for external as well as internal cyber threats have been augmented because of enhanced level and the spectrum of vulnerability in the institutions due to lack or misuse of appropriate controls [13].

India has the third-largest higher education system in the world, after the US and China, comprising 21825 Colleges and 911 Universities [14]also significantly exploiting utilities of G2C eGovernance applications to provide end-to-end transparent services to all the stakeholders i.e. students, citizens, educational institutions, employees, etc. Moreover, National Education Policy 2020 of India emphasizes upon expansion of eServices in education. The growing concern about privacy and security towards G2C eGovernance and allied digitized services offered by HEIs have also emerged as a matter of great concern.

The way personal data has been handled and used can raise concerns regarding privacy and security of information [15]. Internet security and trust survey 2019 conducted by the Centre for International Governance Innovation (CIGI) and IPSOS, in collaboration with UNCTAD and the Internet Society, depicts that 78 percent of web users in 25 countries were concerned regarding their online privacy. In case of India, the proportion was 90 percent or higher. Furthermore, only 57 percent of internet users were aware of data protection and privacy rules [16].

The conflicting research outcomes related to G2C eGovernance system vulnerability and security issues make it imperative to conduct an empirical study to address this issue. Surprisingly, only a few studies have examined the vulnerability and security issues concerning HEIs G2C eGovernance initiatives in India. Moreover, the assessment of security weak points of G2C eGovernance has been done by ample researchers from development and applications perspective which needs to be addressed through the user's perspective also [17]. An efficient cyber security mechanism is not enough and awareness among the users is equally significant [18]. The present study shall bridge the gap identified in the review and suggest the measures to eliminate loopholes. The broad objective of the present study was as under:

To assess the status of ambiguity and vulnerability pertaining to security aspects of HEIs G2C eGovernance Web Portals.

2 Materials and Methods

2.1 Statistical analysis

The current study was experimental and causal in nature. Web portals of five prominent higher educational institutions of India established by Central/State Government NITK, MDU, GNDU, BPSMV, and MNIT have been selected as testing units.

Open source penetration software and web tools viz. Whois.sc, Yougetsignal.com, Kali Linux, Builtwith.com, NMAP, and Google Hacking Database (GHDB) etc. have been applied to assess the status of ambiguity and vulnerability of HEI G2C Web

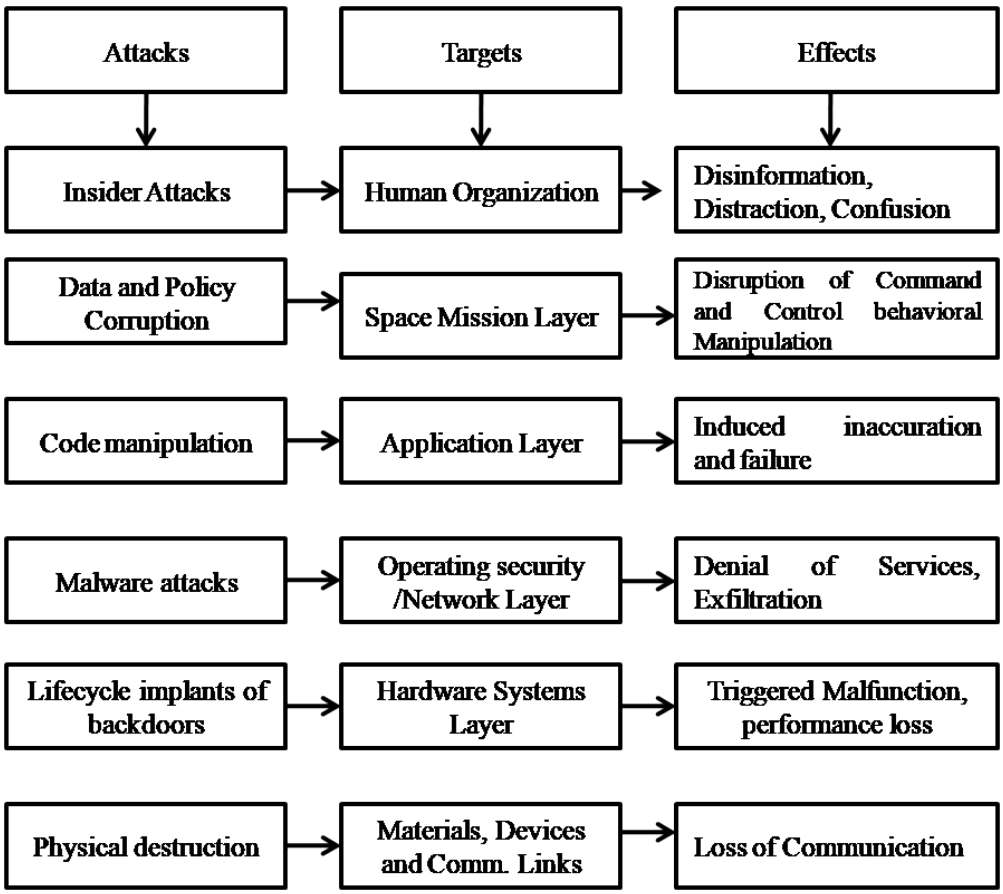

Fig 1. Cyber attacks vis-à-vis effects

Portals. Further, onsite observation and social engineering testing have been in accordance with standard security assessment guidelines to assess the structural gaps and level of social security. 100 employees, serving at different levels, of the select HEIs, have been personally interviewed for social engineering testing and respondents were approached through the snowball method during March 2019 to December 2019. The respondents were apprised regarding the objective of the research before starting the interview. Further, the respondents were assured that their identity shall not be revealed. The diversity of HEIs and respondents have been ensured for inclusive analysis.

2.1.1 Sample status

Out of 100 employees (Table 1), 52 (52.0%) were females and 48 (48.0%) were males; 46 (46.0%) were Post Graduates (25 females and 21 males), 29 (29.0%) were Ph. D. (12 females and 17 males) and remaining 25 (25.0%) were undergraduate (15 females and 10 males); 21 (21.0%) were serving as Assistant, 20 (20.0%) as Head of Department/Branch, 20 (20.0%) as Dean, 16 (16.0%) as Assistant Registrar, 14 (14.0%) as Superintendent and 9 (9.0%) as Deputy Registrar.

Table 1. Employee job position

HEI Name	Assistant	Superintendent	Assistant Registrar	Deputy Registrar	Head of Department	Dean	Total
BPSMV	3	3	2	1	5	6	20
GNDU	5	4	4	3	2	2	20
MNIT	5	3	2	1	4	5	20
NITK	5	2	4	2	4	3	20
MDU	3	2	4	2	5	4	20
Total	21	14	16	9	20	20	100

88 (88.0%) employees (Figure 2) affirmed that top-level management decides about G2C eGovernance technology purchase, G2C eGovernance technology purchase decision a group decision 58 (58.0%) and 92 (92.0%) confirmed that there was no involvement of end-user in G2C eGovernance technology purchase decision. Surprisingly, the outcome of the individual HEI analysis was found in accordance with overall results.

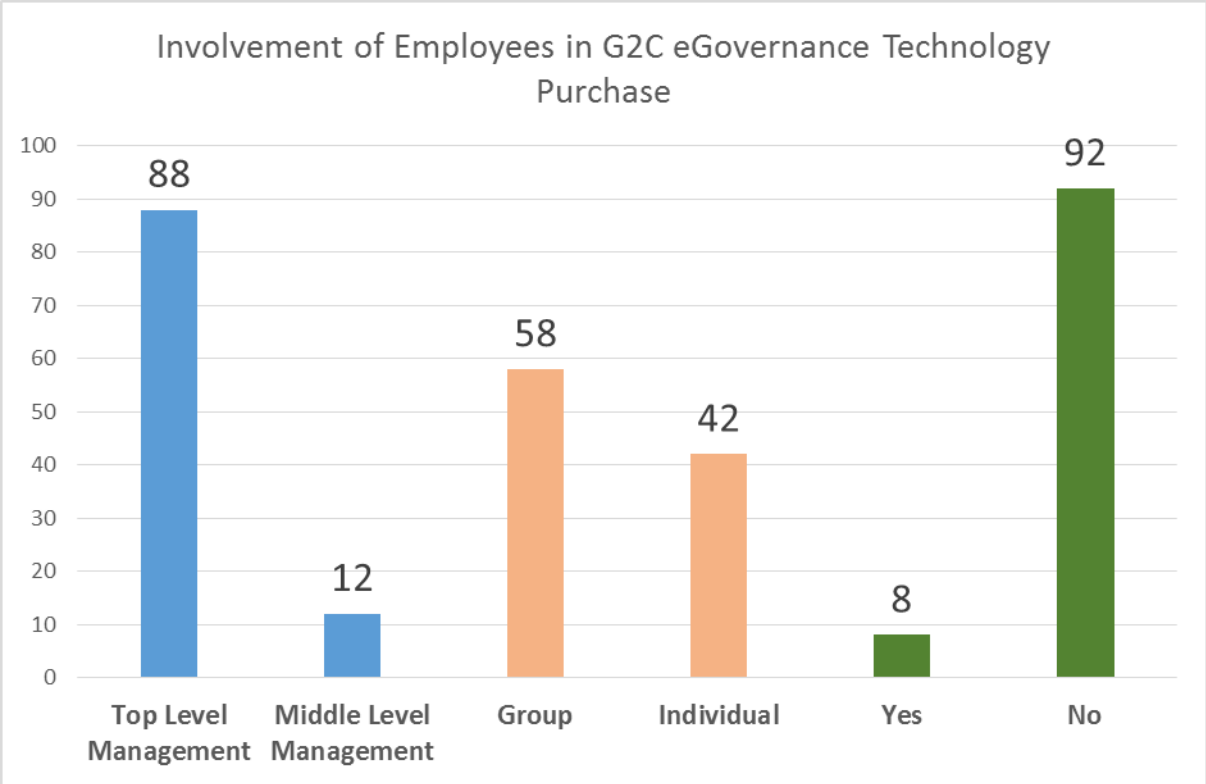

Fig 2.

3 Results and Discussion

The penetration testing initiated with information gathering viz. IP Address, Server details etc. related to HEIs followed by the selection of testing methods and tools and summarised with post penetration risk assessment and report generation. The researcher has applied Grey Box penetration testing method along with social engineering testing using external penetration strategy to assess the ambiguity and vulnerability of HEIs. The exhaustive analysis of penetration and social engineering testing of the HEIs has been presented under supplementary tables 1, 2, 3 and Table 2 .

Table 2. Broken / Dead Links

HEIs	WebPages Processed	Broken/dead Links	LINKs Processed	Links with issues
BPSMV	344	85	1417	188
GNDU	471	333	1500	134
MNIT	1156	30	–	–
NITK	1360	819	1500	478
MDU	383	28	1500	36

It was found that all the web portals were registered with ERNET and the IP location of only two HEIs i.e. NITK and MDU was found at their respective premises and remaining three HEIs IP was located at - BPSMV at Cyfuture Uttar Pradesh – Noida; GNDU at Secured Servers Llc, Phoenix – Arizona; and MNIT at Bharat Sanchar Nigam Limited, Jaipur, Rajasthan.

It was exposed that the GNDU, MNIT, and NITK web portal hosted on a dedicated server whereas in case of the BPSMV and MDU, Eight (8) and Five (5) other sites were hosted on the server, used by theses HEIs, respectively. The Reverse IP Lookup revealed that in the case of BPSMV, MDU, and NIT-K, Thirty Four (34), One (01) and Twenty (20) external domains not related to these HEIs were hosted on the same server. It was found that website of only three HEIs i.e. GNDU, MNIT and MDU were mobile compatible using Viewport Meta.

The researcher further analyzed the trustworthy reputation of the HEIs web portals using webrootbrightcloud threat intelligence web services and discovered that the web reputation of all the select HEIs was in Green Zone i.e. BPSMV (96), GNDU (92), MNIT (100), NITK (96) and MDU (88) out of hundred (100) meaning thereby the stakeholders considered G2C web portals of these HEIs trustworthy.

The in-depth social engineering penetration testing carried out through informal interaction with the employees revealed that the employees share Login IDs and Passwords related to web portals, eResources, networks, Wi-Fi etc. with their natives which is one of the major causes of the security breach. Shockingly it was also observed that employees share sensitive Login ID and Passwords with their subordinates so that the subordinate can complete the work on behalf of the senior officials. Moreover, it was also revealed that the same Login Id and Password were shared by employees during duty shifts. In all such cases if any cyber-attack takes place, it will be difficult to fix up the responsibility of the employee at fault.

The worst case was revealed at BPSMV where the department and faculty-specific password related to students admission to accomplishment i.e. admissions, examinations and other related phases were available with every employee whether authorized or unauthorized or regular or temporary and in some instances with students also.

The analysis of privacy policy exposed that only MNIT privacy policy was clearly visible on the portal. The vulnerability test depicted unencrypted communication between the HEIs portal and server. It was exposed that only NITK was using a secure private connection certified by K7 Web Proxy meaning thereby the sensitive and personal information viz. password, message, credit card, etc. shared by users via web portals of the BPSMV, GNDU, MNIT, and MDU can be seen by other people during transmission.

The Reverse IP Lookup (Supplementary table 3) revealed that Thirty Two (32), Eighteen (18) and one (01) other unrelated domains were hosted on the same web servers of BPSMV, NITK and MDU, respectively. The hosting of other unrelated domains on the same web server literally opens the gateway for the cyber attackers to gain access to other domains hosted on the same server and the risk associated with other unrelated domains may compromise the security of HEIs.

The broken/dead links of HEIs web portals were assessed through https://www.brokenlinkcheck.com/ and https://www.drlinkcheck.com/ (Table 2) and revealed that in case of NITK web portal, 819 broken/dead links along with 478 links with issues were identified; followed by GNDU web portal 333 broken/dead links along with 134 links with issues; BPSMV web portal 85 broken/dead links along with 188 links with issues; MNIT web portal 30 broken/dead links; and MDU web portal 28 broken/dead links along with 36 links with issues were ascertained. The broken/dead links/links with issues on the web portals contribute to a poor user experience along with signal of low quality to search engines.

4 Conclusion

The outcomes of the study are an eye-opener. The study proposes to use ample solutions to viz. two factor-based RSA, RSA cryptosystem, BAN logic model, AVISPA, RSA signature, block chain security solutions, and many more to minimize ambiguity and vulnerability related to the use of login IDs and passwords. One Time Password (OTP) Protocols regarding the use of IDs and passwords must be followed strictly. To eliminate loopholes, the study recommends that electronic gadgets must be authorized by the network administrator before accessing applications of HEIs. The use of HTTPs for communication over the private certified channels and privacy policy must be uploaded and clearly visible. The importance of security policy needs to be understood by the administrators of HEIs. Every eGovernance initiative will remain venerable to security breaches in the absence of a well-articulated security policy. It is highly recommended that HEIs shall host web portals on a dedicated server located at their own premises to keep spam, marketers, and data miners away. The cleaning up of broken links can add context to web portals, and HEIs may adopt a broken link building strategy to recreate the dead content to improve end-user experience.

The study concludes that the problem of ambiguity and vulnerability is not only related to technology but primarily related to human conduct. Accordingly, sensitizing the citizens, service providers, channel partners, and other stakeholders, etc. towards security and privacy protocols is the foundation of secure G2C eGovernance systems.

Acknowledgement

The research team acknowledges the help of open-source society for providing software access required for penetration testing of the web portals of HEIs. The team appreciates the HEIs for the necessary approval and support required for the study.

References

1) Falco E. Digital Community Planning. *International Journal of E-Planning Research*. 2016;5(2):1–22. Available from: https://dx.doi.org/10.4018/ijepr.2016040101.
2) Aladalah M, Cheung Y, Lee VCS. Winning Digital Citizens: A Model and Instrument. In: and others, editor. 20th Pacific Asia Conference on Information Systems (PACIS 2016). PACIS. 2016. Available from: https://aisel.aisnet.org/pacis2016/336/.
3) Deekue SN. A strategic framework for e-government security: the case in Nigeria. 2016. Available from: https://uobrep.openrepository.com/bitstream/handle/10547/622496/Deekue.pdf;jsessionid=45AAF5D7AD3DA1DF36E20D9B0DD442DA?sequence=1.
4) Chaudhary O, Siddique AS. Cloud Computing Application: Its Security Issues and Challenges Faced During Cloud Forensics and Investigation. *International Journal of Advanced Research in Computer Science*. 2017;8(2):12–15. Available from: http://www.ijarcs.info/index.php/Ijarcs/article/view/2916.
5) Hassan GR, Khalifa OO. E-Government - an Information Security Perspective. *International Journal of Computer Trends and Technology*. 2016;36(1):1–9. Available from: https://dx.doi.org/10.14445/22312803/ijctt-v36p101.
6) Páez R, Pérez M, Ramírez G, Montes J, Bouvarel L. An Architecture for Biometric Electronic Identification Document System Based on Blockchain †. *Future Internet*. 2020;12(1). Available from: https://dx.doi.org/10.3390/fi12010010.
7) Soni P, Pal AK, Khushboo K. A User Convenient Secure Authentication Scheme for Accessing e-Governance Services. In: 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India.. 2019;p. 1–7. Available from: https://doi.org/10.1109/ICCCNT45670.2019.8944393.
8) Saha S, Bhattacharyya D, Kim TH, Bandyopadhyay SK. Model based threat and vulnerability analysis of e-governance systems. *International Journal of u- and e-Service Science and Technology*. 2010;3(2):722–722. Available from: https://www.researchgate.net/publication/46157223_Model_Based_Threat_and_Vulnerability_Analysis_of_E-Governance_Systems.
9) Nulhusna R, Sandhyaduhita PI, Hidayanto AN, Phusavat K. The relation of e-government quality on public trust and its impact on public participation. *Transforming Government: People, Process and Policy*. 2017;11:393–418. Available from: https://dx.doi.org/10.1108/tg-01-2017-0004.
10) Bayaga A, Ophoff J. Determinants of e-government use in developing countries: the influence of privacy and security concerns. *IEEE*. 2018. Available from: 10.1109/NEXTCOMP.2019.8883653.
11) Higher Education Cyber Attacks History. EDGUARDS. 2018. Available from: https://edguards.com/pr/articles/higher-education-cyber-attacks-history/.
12) Lynn A. Cyber Attacks History in Higher Education. 2018. Available from: https://www.informationsecuritybuzz.com/articles/cyber-attacks-history-in-higher-education/.
13) Mishra S. Organizational objectives for information security governance: a value focused assessment. *Information and Computer Security*. 2015;23(2):122–144. Available from: https://doi.org/10.1108/ICS-02-2014-0016.
14) UGC Annual report. 2019. Available from: https://www.ugc.ac.in/pdfnews/3060779_UGC-ANNUAL-REPORT--ENGLISH--2018-19.pdf.
15) Digital Economy Report. In: and others, editor. Value Creation and Capture, Implications for Developing Countries United Nations Conference on Trade and Development. 2019. Available from: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf.
16) Cigi-Ipsos, Centre for International Governance Innovation, UNCTAD and the Internet Society. CIGI-Ipsos, UNCTAD and Internet Society. CIGI-Ipsos Global 2019Survey on Internet Security and Trust. . 2019. Available from: https://www.cigionline.org/internet-survey-2019.
17) Alsultanny AY. Assessment of E-Government Weak Points to Enhance Computer Network Security. *International Journal of Information Science*. 2014;4(1):13–20. Available from: https://doi.org/10.5923/j.ijis.20140401.03.
18) Joshi BS. Survey on need of cyber security and cyber awareness in e-governance plan in India. *Multidisciplinary International Research Journal of Gujarat Technological University*. 2019;1(1):15–20. Available from: http://www.researchjournal.gtu.ac.in/Combine/January%202019%20First%20Issue.pdf.