International Journal of
Engineering in Computer Science

E-ISSN: 2663-3590
P-ISSN: 2663-3582
www.computersciencejournals.com/ijecs
IJECS 2025; 7(1): 52-59
Received: 10-01-2025
Accepted: 19-01-2025

Aditya Sethi
Department of Computer Science, University of Delhi, Delhi, India

Parmod Kumar Sethi
Professor, Department of Physical Education and Sports Sciences, P.G.D.A.V College (E). University of Delhi, Delhi, India

Corresponding Author:
Aditya Sethi
Department of Computer Science, University of Delhi, Delhi, India

Addressing security challenges in the digital transformation of higher education: Strategies and solutions

Aditya Sethi and Parmod Kumar Sethi

DOI: https://doi.org/10.33545/26633582.2025.v7.i1a.158

Abstract
Higher Education Institutions (HEIs) are going through a massive digital transformation, be it Online education framework, administrative processes or Library Access, they all are vulnerable to certain cyber-attacks. Therefore, in the hurry to put up all the processes online and facilitate faculty and Students with e governed services, security factors should not be compromised. The study is undertaken to determine what security challenges Higher Educational Institutes (HEI's) face and what effective solutions can be provided to overcome the vulnerabilities of attacks. Research done in the paper highlights the issues and challenges that HEI's can face while adopting efficient e-governed frameworks. The study also provides insight on the new technology trends HEIs must adapt and adopt, the security challenges faced, and how to deal with them.

Keywords: Technology in academia, privacy concerns, cybersecurity, higher education, policy, digital transformation, e-governance

Introduction

Cyber security is considered as an essential aspect when it comes to e-Governance. e-Governance in higher education involves the use of electronic and digital technologies to enhance online learning, reform administrative operations, streamline service delivery, and support decision-making processes within educational institutions. There are five core NIST Cyber Security frameworks as follows:

- Identify - Establish a comprehensive organizational understanding to manage cybersecurity risk across systems, personnel, assets, data, and capabilities.
- Protect - Develop and execute suitable safeguards to ensure the uninterrupted delivery of critical services.
- Detect – Develop and implement appropriate measures to promptly identify any cybersecurity events that may occur.
- Respond - Implement and execute suitable measures to respond promptly and effectively to any detected cybersecurity incidents.
- Recover - Develop and execute plans to ensure resilience and restore impaired capabilities or services following a cybersecurity incident [Eko Yon Handri *et al.*,] [18].

Cybersecurity is crucial in e-Governance as it ensures protection of sensitive data, maintains the integrity of online services, and fosters public trust. As global connectivity increases, the use of e-government services is expanding, requiring the effective use and protection of data [Imdad Ali Shah *et al.*,] [12]. With advancing technology, data security systems must be developed to address emerging vulnerabilities. With the emerging trend of shifting tasks performed at higher educational institutions from offline to online, tasks that include admissions, registration, fee payments, student portals, e-library portal etc needs monitoring on a regular basis.

A. Importance

E-Governance in higher education refers to applying digital technologies to improve administrative processes, service delivery, and decision-making within educational institutions. It includes various activities, including online registration and admission processes, digital learning management systems, e-library services, online assessment and examination systems, digital student information management, and many more. As higher educational institutes are increasingly adopting digital platforms to provide services and manage information, they become more vulnerable to cyberattacks, which can compromise critical infrastructure, disrupt student services, and expose confidential information. One of the key advantages of digital transformation in higher education is its ability to foster innovation and creativity [Manoj KS Chhangani and Sofia I Hussain, [14]. Adopting robust Cybersecurity measures can help in safeguarding institutions against these threats by implementing measures such as securing networks, preventing unauthorized access, and ensuring the continuity of operations.

B. Objective

As individuals are becoming more connected, focused, and engaged in the virtual world, there is an increasing need for advanced cybersecurity solutions. Objective of this study is to explore the Security Challenges in the Digital Transformation of Higher Education and formulate possible ways to overcome these challenges. Aim of the study is to delve into the digital transformation of higher education in India, with a specific focus on the importance of Security in facilitating this transformation.

Digital transformation of E governance

Digital transformation in higher education refers to integrating digital technologies and innovative strategies to enhance educational institutions' teaching, learning, and administrative processes [Leal Filho, Walter] [22]. Digital transformation in higher education is not only limited to the classroom but embraces various areas such as admissions, student support services, learning management systems, and assessment methods. Digital transformation of higher education improves operational efficiency, student services, and the overall educational experience of students.

[M AlRousan *et al.*, [5] in their paper, highlighted the growing usage of smartphones and tablets that has significantly impacted e-government services, which supports the fact that there is a need to remain up to date with technologies in order to create smooth transition of e governed services. [Paudyal *et al.*, [6] claimed that migrating e governed systems to a cloud governance framework and adoption of distributed cloud computing operations can ensure effective implementation of e governed services. [M. Kemal Oktem *et al.*, [2] focussed on student's internet usage experience. They evaluated user activities, conditions and various others factors affecting student's usage of e governance applications. Authors emphasized on the need for institutions to implement strategies that enhance user experience and maximizes the benefits of e governance in higher education. [Serkan *et al.*,] [11] in their paper highlighted the critical role of cyber governance in ensuring cyber security. Authors pointed out several challenges such as Balancing security needs with operational requirements, Managing the complexity of cyber threats, ensuring compliance with evolving regulations and proposed several strategies to enhance cyber security in e governance. [Mijwil *et al.*, [19] in their paper emphasized on the critical role of cyber security governance in the digital transformation of public services. Authors in the paper threw light on integrating computer-based technologies into public services further enhancing efficiency and accessibility of services. [Stephanie Ness and Tushar Khinvasara, [20] in their research paper provided an overview of recent developments in cyber security, highlighting both the progress made and the emerging challenges. Authors discussed novel attack vectors and increasing sophistication of cyber-attacks. Along with that, authors discussed various solutions to overcome these challenges that included Enhancing cyber security awareness and training among personnel, Implementing advanced threat detection and response systems, developing comprehensive national cyber security policies and fostering international collaboration to combat cyber-crime. [Duggineni and Sasidhar, [17] focussed on critical role of data integrity in information systems and the effectiveness of various controls in maintaining it. Authors identified several threats to data integrity including unauthorized access, data manipulation, and system vulnerabilities. [Prakoso *et al.*, [21] suggested that while technology, training, and management support are vital for enhancing system performance, personal technical skills also play a significant role as previously believed. The paper emphasizes the need for comprehensive strategies that integrate these elements to improve financial information systems' effectiveness in businesses.

E-governance plays a crucial role in ensuring smooth management of information databases, facilitating the exchange of essential resources, and strengthening data analytics, all while promoting transparency and continuity across educational institutions. By leveraging ICT and IT tools, the government can efficiently handle various tasks such as policy drafting, accounting, and the implementation of educational principles. E-governance also enables the publication of rankings like the NIRF (National Institutional Ranking Framework), NAAC reports, MGNREGA details, and updated PFMS information [Pritam Das and Chandan Adhikary, [9].

Security challenges in digital transformation

The digital transformation of higher education brings various security challenges that institutions must look into in order to protect sensitive data and maintain system integrity. With the increased use of online platforms for teaching, learning, and administration, educational institutions are more vulnerable to cyberattacks such as data breaches, phishing, and ransomware. There are several major challenges faced by institutions of higher education few of which are discussed in detail: Infrastructure as a challenge, Human errors, Distributed Access and allocation of resources, Weak Institutional Policies, Weak Authentication Mechanisms, Using Automated tools.

A. Infrastructure

A significant challenge lies in ensuring that the infrastructure and connectivity is needed to support e-governance. In many developing countries, the lack of widespread internet access and limited technological resources impede the effective implementation of e-governance in higher education institutions (HEIs) [Manoj KS Chhangani and Sofia I Hussain, [14]. Data security and privacy are vital components of e-governance and are required for safeguarding sensitive information and maintaining citizen trust. A significant challenge lies in the infrastructure of higher education institutions. As institutions increasingly rely on digital platforms, the underlying IT infrastructure, including servers, networks, and data centres, becomes a critical target for cyberattacks. For e-governance to be effectively implemented in higher education, it is essential to build a strong infrastructure that supports the digital transformation of administrative processes and service delivery.

Weak or outdated infrastructure can lead to disruptions in service, data loss, and unauthorized access to sensitive information. To mitigate these risks, institutions must invest in upgrading their IT infrastructure, implementing advanced security measures like encryption and firewalls, and ensuring regular system maintenance and updates to fortify against evolving threats. Ensuring a secure and resilient infrastructure is essential for protecting institutional data and maintaining the continuity of digital services in the evolving landscape of higher education.

B. Human Error

Human error and lack of awareness can also emerge as a security challenge when it comes to digital transformation in higher education institutions. Human error significantly contributes to cyber incidents in higher education and there is need for ongoing training to improve policy compliance and cybersecurity leadership among staff, ensuring better protection against cyberattacks [Eric CK Cheng and Tianchong Wang, [8]. Administration staff or faculty at higher educational institutions often lack sufficient training in cybersecurity protocols, which can lead to unintentional security breaches through practices such as weak password management, falling victim to phishing attacks, or mishandling sensitive data.

Cybercriminals are increasing their efforts to introduce new methods to attacks [Eric CK Cheng and Tianchong Wang, [8]. Faculty members and administrators many a times resist to adopt new digital tools and security measures that frequently leads to vulnerabilities.

C. Weak Institutional Policies

Weak institutional policies represent a significant security challenge in the digital transformation of higher education. When institutions lack robust and well-defined policies for managing cybersecurity, data protection, and user access, they expose themselves to increased risks of breaches and cyberattacks. To protect information assets, organizations need to communicate technical and behavioural solutions to their employees [Saleh AlDaajeh *et al*., [7]. Institutes of higher education comprises various departments that function simultaneously to achieve a particular goal. Security measures, strategies, and procedures to prevent information and computing security incidents are typically developed and executed by the IT department, often without input from top management or end-users. This separation of the information security team creates a significant communication gap, leading to non-compliance with established rules and regulations.

D. Distributed Access of Resources

Distributed access generally refers to the ability to access an institution’s data. It may be accessed from different locations which could be within the institution premises or outside the premises, resulting in significant increase in risk of data breach. Challenges such as insecure connection, end to end security, identity access management and Virtual Private Networks (VPN) can be faced by HEI while delivering services through E-Governed platforms. Moreover, with the advancement in technologies, new cyber-attacks are evolving that can infect an institution’s system. Many new and advanced mobile devices (such as, iPads, new Android phones, tablet devices and portable Internet access systems) are launched daily with upgraded versions of operating systems; these are ripe for infection and ready to infect a university’s network system [I Bandara, F Ioras, and K Maher, [1]. While Distributed and remote access provides a flexible, user friendly and a comfortable environment for students as well as faculty, but on the other hand it also significantly makes institution’s data vulnerable to Cyber-attacks.

E. Weak Authentication Mechanisms

In the sector of higher education, weak authentication mechanisms can lead to cyber security risk to students, faculty, and administration. Educational institutes tend to collect sensitive information from students as well as faculty such as financial details, personal records, medical records and academic records. Therefore, it is essential to develop and construct Strong Authentication Mechanisms in order to safeguard sensitive information. Many educational institutes use weak passwords for their official university accounts, that includes guessable combinations of name or birth date. Maintaining a predictable, Decipherable and obvious password could lead to high risk of cyber-attack. Apart from weak passwords there are other factors such as Lack of Multi factor Authentication, poorly managed access to third party systems, shared accounts and insecure storage of credentials that could lead to cyber-attacks. Higher education institutes can significantly reduce risk of cyber-attacks by addressing challenges posed by weak authentication mechanisms.

In HEIs, information security requirements are documented as information security policies and communicated to the end users through E-mails or by putting up on websites for information to all. These policies are not often delivered through reliable security education, training and awareness programs.

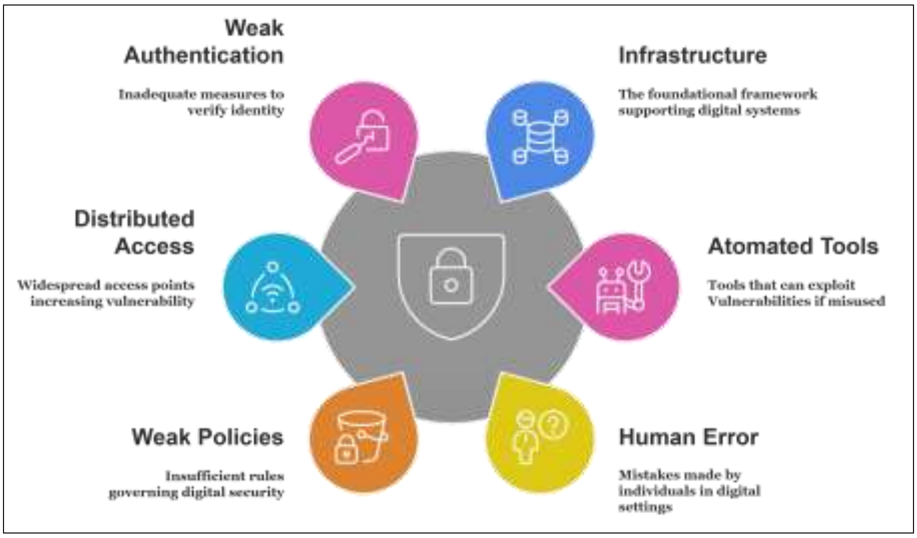
Weak Authentication
Inadequate measures to verify identity
Infrastructure
The foundational framework supporting digital systems
Distributed Access
Widespread access points increasing vulnerability
Atomated Tools
Tools that can exploit Vulnerabilities if misused
Weak Policies
Insufficient rules governing digital security
Human Error
Mistakes made by individuals in digital settings

Fig 1: Security Challenges in Digital Transformation

Security measures for higher educational institutions

There is a need to identify patterns that contribute to cybercrime vulnerability, validating the need for improved cybersecurity in higher education institutions. By using an information assurance risk analysis and categorizing information assets, the study seeks to enhance the security and usage of institutional technology. A thorough needs assessment must be carried out to pinpoint the specific requirements and challenges facing the institution. This evaluation should take into account the current infrastructure, technological capabilities, and the needs of different stakeholders, such as faculty, students, and administrative staff. The subsequent actions should be undertaken in order to avoid cyber security threats:

A. Planning and Execution

Successful implementation of e-governance in higher education requires careful planning and execution. It is essential to develop a strong technological infrastructure to support e-governance initiatives. This involves investing in dependable hardware and software systems or cloud infrastructure, establishing secure high-speed internet connectivity, and ensuring data security and privacy. A solid technological base is crucial for enabling smooth communication, data sharing, and collaboration among all stakeholders. Designing and maintaining a resilient network infrastructure with high-speed internet, redundant connections, and network segmentation can help in overcoming security threats.

B. minimizing human error

Minimizing human error can significantly reduce the vulnerabilities of cyber-attacks. Between 2014 and 2019, a study conducted by IBM reported that 95 percent of all security breaches were caused by human error. The cost of these incidents reached an estimated dollar 3.56 million US dollars. This research was gathered and organized by IBM based on 1000 clients in 133 countries. Hence there is a need to minimize human errors that could help higher education institutions overcome security challenges. Well-aware and trained employees minimise the occurrence of accidental and nondeliberate actions determining a violation of cybersecurity rules, and play a significant role in minimising information security risks and protecting the organisation's critical assets and valuable intellectual property [Alessandro Pollini *et al.*, [10]. In order to avoid cyber threats, institutions should prioritize hiring qualified practitioners to strengthen cybersecurity leadership and protect information assets. According to several models as studied by authors in [Alessandro Pollini *et al*, [10], it is possible to explain human errors and violations by studying the employees' attitudes toward cybersecurity-critical behaviours, since cybersecurity can be improved by predicting the actual behavioural intention of unsafe behaviours. Neglecting to do so could have negative consequences for future cyberattack prevention.

C. Strong Institutional Policies

Strong institutional policies along with regular audits can also minimize the risk of cyber-attack in higher educational institutes. Before a policy can be developed, several assessments must be performed and current policies must be examined. A steering committee composed of representatives from the student body, academic staff, and the institution's administration should be established. This committee should guide the creation of computing vision statements for Academic Computing, Library Computing, and Administrative Computing to help shape the development of security policies. Effective implementation of Information Security Management (ISM) and encompassing policies, processes and procedures along with organizational structures, and software and hardware functions is essential for managing and mitigating risks and threats [I Bandara, F Ioras, and K Maher, [1]. Creating strong institutional policies can help avoid overcoming security threats.

D. Management Strategies

Management Strategies plays an important role in overcoming risks of cyber-attacks. E - governance services significantly optimize services that are citizen centric by offering smooth functioning of digital platforms that ensure efficiency and transparency. In order to make these services continue to work efficiently, institutions must go beyond institutional policies and infrastructural development by formulating a versatile management strategy. These strategies would facilitate a smooth transition from traditional governance practices to e-governance, highlighting the importance of raising awareness and building capacity among stakeholders about benefits of e governed systems. By creating an ecosystem of cutting edge technologies and fostering a culture of security awareness, institutions can create a resilient system that can safeguard institution's data.

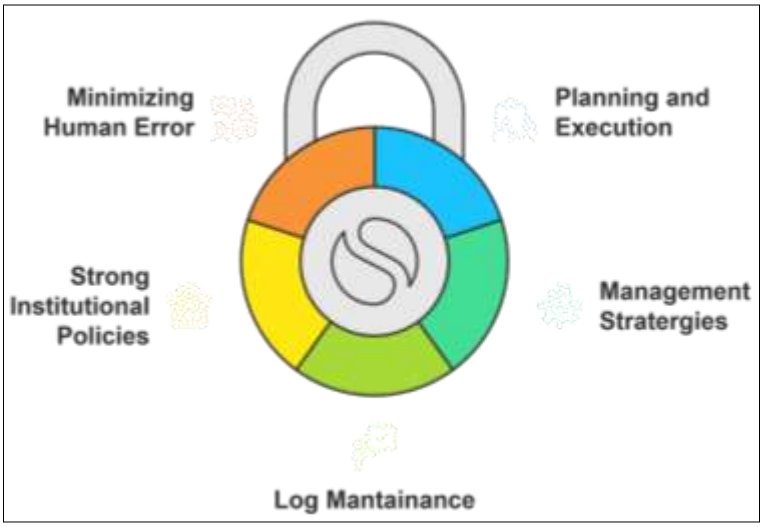

Fig 2: Security Measures for HEI's

E. Log Maintenance

Furthermore, maintaining logs in written format as well as digitized format to support the implementation of the new information security program would be beneficial for institutions. This involves keeping detailed and accurate records of various activities, events, or incidents related to information security. Log maintenance includes various components such as tracking activity in which history of user actions, system changes and transactions can be recorded. Other than that, log maintainace can help identify the root cause of an anomaly by providing a detailed account of actions that led to that attack. Apart from security measures, Logs can also be used to analyse and optimize system performance resulting in improvement of system's efficiency. In summary, keeping logs in a e-governed system in higher education along with a well-managed digital framework can play a vital role in safeguarding sensitive academic and administrative information.

V. Recent innovations in cyber security

The cybersecurity threat landscape in higher education is continuously changing. VMware's" Global Incident Response Threat Report" highlights the rising prominence of new threats targeting APIs and containers over the past year, along with the increasing use of deepfake attacks. Cybercriminals are constantly exploring innovative tactics to deceive individuals, exploit system vulnerabilities, and compromise digital environments, making their malicious activities more difficult to detect and halt. This allows them to infiltrate systems more swiftly, remain undetected for longer, and spread their attacks more extensively.

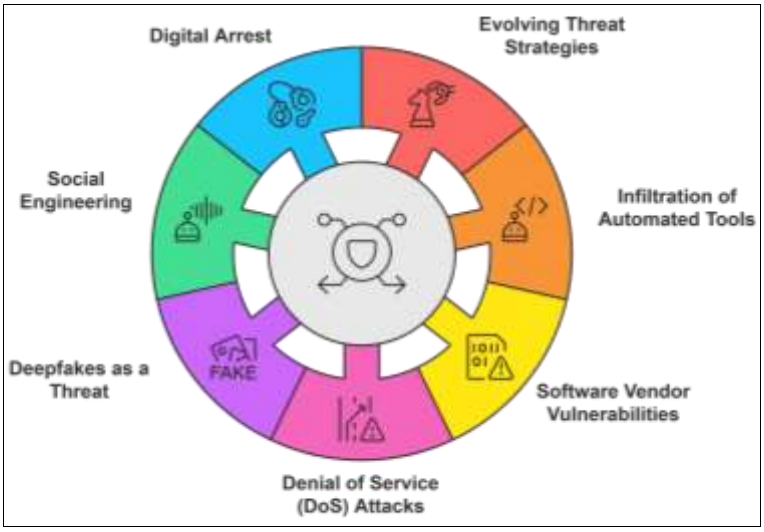
Digital Arrest
Evolving Threat Strategies
Social Engineering
Infiltration of Automated Tools
Deepfakes as a Threat
FAKE
Software Vendor Vulnerabilities
Denial of Service (DoS) Attacks

Fig 3: Recent Innovations in Cyber Security

A. Evolving Threat Strategies

As institutions are moving towards digitization, cyber attackers are also brainstorming on strategies to infiltrate into institutions. Cyber attackers are using modern day technologies such as Phishing. Phishing is a prevalent method of cybercrime wherein attackers masquerade as reputable entities, such as banks or online service providers, with the intent to deceive individuals into divulging sensitive information, like passwords or credit card numbers [Daksh Dave *et al.*, [16]. Phishing attacks are usually carried out by sending fake emails or creating a cloned websites that resembles the original ones thereby luring an individual into activities such as identity theft and financial frauds. Apart from that cyber attackers are using ransomware attacks to get access to sensitive user information. Ransomware is a malicious software that was first demonstrated by Joseph pop in the year 1989, it is a software that uses symmetric key encryption method (in which one single key is used for both encryption as well as decryption) to lock user's sensitive information and in exchange of that information, attacker demands of some kind of ransom. After the launch of Ransomware in 1989, it evolved with time. In 2005, attack named Gpcoder was launched, in 2006 asymmetric encryption method came into light, in year 2013 attacks named Scareware and Cryptolocker were Commenced, in year 2016 an attack named as Locky was introduced [Philip O'Kane, Sakir Sezer, and Domhnall Carlin, [3]. In addition to these attackers also some methods such as Advanced Persistent Threats (APTs) and DoS attacks to target institutions. Impact of these attacks could tamper institution's services therefore institutions must adhere caution while handling suspicious emails or downloads.

B. Infiltration of Automated tools

Increasing complexity of cyber threats have significantly led to adoption of automated tools in cyber security, safeguarding e governed systems in HEI's. These tools are tailored to streamline threat detection, protect sensitive institutional data and enhance security by providing functionalities such as Realtime threat detection, Faster incident response and analysing network behaviours by integrating AI and Machine Learning in e governed systems. Apart from that, APIs have been there in the IT spectrum for a long time, playing a crucial role in enabling seamless integration and communication between different systems and applications. APIs facilitate transactions, data sharing, and other interactions between automated processes. As their usage grows and their purposes become more critical, APIs have increasingly become attractive targets for attackers. Cybercriminals are exploiting APIs not only to gain unauthorized access to data, systems, and services but also to amplify their attacks. Since API operations are fully automated without human oversight, breaches and misuse are often harder to detect. Therefore, investing in advanced automated tools along with adequately trained staff and updating infrastructure can be beneficial in integrating e-governed learning systems along with traditional learning systems for HEI's.

C. Software vendor vulnerabilities

Attackers thrive on the ability to launch a single attack that can affect multiple targets. A growing trend in this area revolves around supply chain attacks. If attackers manage to infiltrate a software vendor's systems, they may tamper with the software before it gets delivered to customers, giving them access to all the customer environments that use it. The same risk exists with open-source software projects. If an attacker successfully introduces harmful code, backdoors, or other unauthorized access methods into open-source code, they can later exploit those vulnerabilities to compromise higher education institutions and other organizations. The future trajectory of e-Governance in Indian higher education is diverse, with immense potential to revolutionize administrative operations and boost overall efficiency. A key component involves leveraging emerging technologies like artificial intelligence (AI) and blockchain in various administrative functions, strengthen data security and integrity, and enable seamless collaboration among educational institutions.

D. Denial of Service (DoS) attacks

A denial of service (DoS) attack is a type of cyberattack wherein an individual deliberately inundates a network, server, or website with excessive traffic or data to exhaust its resources, rendering it inaccessible to users [Philip O'Kane, Sakir Sezer, and Domhnall Carlin, [3]. Main objective of DoS attack is to block user from using a system or network eventually leading to system crashes. Institutes can face challenges such as interruption in their online learning platforms, disrupting the access to online repositories and it could also lead to significant financial loss as it could lead to prohibition of payments. In order to mitigate risk of attack through DoS, institutes must conduct regular workshops for faculties as well as students and maintain regular backup to retrieve files in case of data loss. To effectively combat DoS attacks, organizations should have a well-defined incident response plan in place [Philip O'Kane, Sakir Sezer, and Domhnall Carlin, [3]. This plan should facilitate swift actions to mitigate the attack's effects and minimize potential damage [Mawuli Afenyo and Livingstone D Caesar, [13].

E. Deepfakes as a threat

A deepfake can be considered as a content generated by artificial Intelligence. The technology induces the creation of fake videos and images alongside the cloning of voice messages hence presenting an opportunity for cybercriminals to utilize the technology in various social engineering attacks [Bibhu Dash and Pawankumar Sharma, [15]. Using neural networks, deepfakes can manipulate facial expressions, voice, and movements to make it appear as if individuals are saying or DOIng things they never actually did. These deepfakes can appear entirely genuine, even though they are fabricated. With respect to addressing challenges in higher education, deepfakes proposes various threats such as threat to academic integrity in which fake or fabricated videos could be prepared that can spread misinformation through online framework of classes. Apart from that administrative risks are also there; intruder might gain unauthorized access to institute's systems by creating deepfake images of administration. Furthermore, a fraudulent video of faculty could hamper university's reputation. In recent years, it has become clear that much of the information shared through social media and other technologies is often inaccurate or misleading. Advances in artificial intelligence and graphics have led to a new wave of disinformation in the form of" deepfake" videos. Hence, institutes must formulate some policies or adopt some tools and educate faculty members as well as students about the risks that could lead to cyber-attacks.

F. Social Engineering

Apart from traditional methods used for gaining unauthorized access such as DoS attacks, Phishing, Ransomware Attacks, Cyber criminals are now frequently using tricks to Psychologically manipulate individuals by exploiting human behaviour thereby luring them into revealing sensitive information that in turn compromises security. This technique of psychologically manipulating individuals is termed as Social Engineering. While some researchers see cyber psychology as a modern approach or in other words new way of DOIng old things, others emphasize on the fact that differences in online behaviour tends to develop new methodological strategies to develop cyber-attacks [Vladlena Benson, John McAlaney, and Lara A Frumkin, [4]. The objective of social engineering ranges from sending fraudulent emails and notifications to creating deepfakes using AI generated tools to manipulate students and staff into revealing sensitive data. In order to mitigate the risks of Social Engineering, institutions must increase vigilance and provide comprehensive education to students as well as faculty via workshops and security programs [Philip O’Kane, Sakir Sezer, and Domhnall Carlin, [3].

G. Digital Arrest

With the advancement in technologies, ways to retrieve data from individual as well as institutions are also evolving. Cyber criminals are using a method in which the scammers falsely accuse victims of their involvement in illegal activities via phone and video calls (Online), thereby putting them in pressure to immediately pay ransom to get themselves out of that situation. This method of harassing an individual or an entity comes under the category of social engineering and can be termed as Digital Arrest. In the sector of educational institutions, students are vulnerable to such scams that could lead to risk of financial loss. Not only students but Faculty and staff, who are often more educated than students can fall into scam of digital arrest. This is because cyber criminals manipulate psychology of an individual to exploit their vulnerability. Therefore, educational institutes can safeguard their as well as an individual’s environment by providing students and administration with security awareness programs and contributing towards a secure academic digital ecosystem.

Conclusion

The digital transformation of higher education in India through e-governance presents a tremendous opportunity to revolutionize the sector. By tackling issues such as manual procedures, and restricted access to information and resources, e-governance can lead to greater transparency, more streamlined administrative processes, improved access to educational resources, and enhanced collaboration among stakeholders. Case studies and best practices from Indian universities and colleges show that successful e-governance implementations have resulted in increased administrative efficiency, better student services, and overall institutional effectiveness. Concerns about data security, privacy, and infrastructure are to be addressed, highlighting the importance of strong cyber security measures, data protection policies, and sufficient technological infrastructure. This underscores the need for robust cyber security measures to overcome the risks of cyber-attacks by creating a digital ecosystem that strengthen institutions and supports student access. To enforce CIA (Confidentiality Integrity and Availability) Triad, there is a need to formulate a Security Framework for e-Governance - GOVeSHIELD – GOVernance enforced by Security Hierarchy for Integrity, Encryption, Logging, and Defence.

VII. IMPLICATION OF STUDY

Findings of this study has several implications, both theoretical as well as practical. From a theoretical point of view, this research contributes to the existing knowledge on cyber security in higher education institutions. The study in this paper supports previous research while introducing new perspectives to help refine existing frameworks.

Financing

The authors declares that the research has not received any funding

References

1. Bandara I, Ioras F, Maher K. Cyber security concerns in e-learning education. In: ICERI2014 Proceedings. IATED; c2014. p. 728-34.
2. Oktem MK, Demirhan K, Demirhan H. The Usage of E-Governance Applications by Higher Education Students. Educ Sci Theor Pract. 2014;14(5):1925-1943.
3. O'Kane P, Sezer S, Carlin D. Evolution of ransomware. IET Networks. 2018;7(5):321-7. DOI: 10.1049/iet-net.2017.0207.
4. Benson V, McAlaney J, Frumkin LA. Emerging threats for the human element and countermeasures in current cyber security landscape. In: Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications. IGI Global; c2019. p. 1264-1269. DOI: 10.4018/978-1-5225-4053-3.ch016.
5. AlRousan M, Intrigila B, *et al.* Multi-factor authentication for e-government services using a smartphone application and biometric identity verification. J Comput Sci. 2020;16(2):217-224. DOI: 10.3844/jcssp.2020.217.224.
6. Paudyal R, Shakya S. Secure data mobility in cloud computing for e-Governance application. J Eng Technol Plan. 2021;2(1):1-14. DOI: 10.3126/joetp.v2i1.39203.
7. AlDaajeh S, *et al.* The role of national cybersecurity strategies on the improvement of cybersecurity education. Comput Secur. 2022;119:102754. DOI: 10.1016/j.cose.2022.102754.
8. Cheng ECK, Wang T. Institutional strategies for cybersecurity in higher education institutions. Inf. 2022;13(4):192. DOI: 10.3390/info13040192.
9. Das P, Adhikary C. Transformative e-governance and access in higher education. Online J Distance Educ e-Learn. 2022;10(1):162-168.
10. Pollini A, *et al.* Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn Technol Work. 2022;24(2):371-390. DOI: 10.1007/s10111-021-00683-y.
11. Savaş S, Karataş S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. Int Cybersecurity Law Rev. 2022;3(1):7-34. DOI: 10.1365/s43439-021-00045-4.
12. Shah IA, *et al.* The influence of cybersecurity attacks on e-governance. In: Cybersecurity Measures for E-Government Frameworks. IGI Global; 2022. p. 77-95. DOI: 10.4018/978-1-7998-9624-1.ch005.
13. Afenyo M, Caesar LD. Maritime cybersecurity threats: Gaps and directions for future research. Ocean Coast Manag. 2023;236:106493. DOI: 10.1016/j.ocecoaman.2023.106493.
14. Chhangani MK, Hussain SI. Digital Transformation of

Higher Education: Leveraging eGovernance in India. 2023.

15. Dash B, Sharma P. Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review. Int J Eng Appl Sci. 2023;10(1):21-29.
16. Dave D, *et al*. The new frontier of cybersecurity: emerging threats and innovations. In: 2023 29th International Conference on Telecommunications (ICT). IEEE; c2023. p. 1-6. DOI: 10.1109/ICT60153.2023.10374044.
17. Duggineni S. Impact of controls on data integrity and information systems. Sci Technol. 2023;13(2):29-35. DOI: 10.5923/j.scit.20231302.04.
18. Handri EY, Wibowo Putro PA, Sensuse DI. Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government. In: 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs). IEEE; c2023. p. 82-87. DOI: 10.1109/ICoCICs58778.2023.10277024.
19. Mijwil M, *et al*. The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. Mesopotamian J Cybersecurity. 2023;2023:1-6. DOI: 10.58496/MJCS/2023/001.
20. Ness S, Khinvasara T. Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector. J Eng Res Rep. 2024;26(2):107-17. DOI: 10.9734/JERR/2024/v26i21075.
21. Prakoso T, *et al*. Analysis of the influence of information system applications, digital trainings, and technology adoption on financial information system performance. J Inf Technol. 2024;6(1):250-254. DOI: 10.60083/jidt.v6i1.510.
22. Leal Filho W, editor. Service Learning. In: Encyclopaedia of Sustainability in Higher Education. Cham: Springer; c2019. DOI: 10.1007/978-3-030-11352-0_300217.