

Exploring Digital Landscape, Awareness and Vulnerabilities: A Case Study of Students of Central University of Rajasthan, India

***Sarath MT¹, Suman Rana² & Wairokpm
Premi Devi³***

¹Department of Society Technology Interface, School of Social Sciences,
Central University of Rajasthan, Bandar Seendri, Rajasthan (India)
E-mail:<2025phdds004@curaj.ac.in>

²Independent Researcher E-mail:<immanuelsuman1985@gmail.com>

³Assistant Professor (Corresponding Author), Department of Society
Technology Interface, School of Social Sciences, Central University of
Rajasthan, Bandar Seendri, Rajasthan (India)
E-mail:<wairokpm@curaj.ac.in>

Abstract

The objective of this research paper is to analyze the awareness of digital literacy and online security among the students at Central University of Rajasthan (CURAJ) in relation to the wide gulf in their extensive digital usage versus their insecurity online. A qualitative methodology including two instruments structured questionnaires (n=27) and semi- structured interviews (n=15) were used to analyze student usage and their attitudes toward privacy and security. According to the findings, the students are extremely digitally literate, and their usage hours is around over six hours a day while a very high level of ignorance about online security awareness is noticeable. All 42 participants stated they were unaware of the digital literacy resources being used in the university, demonstrating a clear gap in the institution's outreach, thus, magnifying their insecurity over the internet. Based on the findings, a key recommendation would be the need for implementing mandatory digital literacy and internet security modules across the curriculum along with effective communication on available resources.

Keywords

Digital literacy, Cybersecurity awareness, Online safety, Digital vulnerability, Higher education.

**Research Foundation International, New Delhi
(Affiliated to UNO)**

Editorial Office : D-59, Shastri Nagar, Meerut - 250 004 (INDIA)
Ph. : 0121-2763765, +91-9997771669, +91-9219658788

4

Exploring Digital Landscape, Awareness and Vulnerabilities: A Case Study of Students of Central University of Rajasthan, India

1. Introduction

Digital technologies have impacted our life very deeply in the twenty-first century, influencing our relationships, learning, and communication. A variety of opportunities for development and education have been created by the spread of internet platforms. However, this digital environment also presents a number of difficulties, particularly in terms of potential vulnerabilities that people, particularly students, may experience. Navigating this digital landscape for students, who are frequently early users of technology, is both liberating and dangerous. This case study tries to understand the complicated web of digital awareness among the students of CURAJ (Central University of Rajasthan), acknowledging the crucial relevance of digital literacy and online safety. In-depth interviews were conducted with 15 students. The interviews allow for a more nuanced exploration of the students' digital experiences, addressing specific themes such as online privacy concerns, encounters with digital scams, and awareness of cybersecurity best practices. The interviews are semi-structured, allowing for flexibility while ensuring key topics are covered. The study identifies usage of online platforms, potential weaknesses and risks faced by the students in the digital landscape, encompassing areas such as online privacy, cybersecurity threats, and digital scams.

The research attempts to assess the level of digital literacy among these students through a thorough assessment. It aims to ascertain their knowledge of digital technology, their expertise with exploring online resources, and most importantly their understanding of key safety precautions in the digital domain. The survey aims to identify the weaknesses faced by CURAJ students, including any areas where their knowledge may be insufficient or where misunderstandings may still exist. This study, which explores the digital world in which CURAJ students live, aims to shed light on their current levels of awareness and provide valuable insights into areas where targeted educational interventions can be implemented. These observations play a critical role in creating prospective educational programmes and tactics, ensuring that students have the information and abilities required to operate safely and responsibly in the digital age. "Digital awareness" includes a deep grasp of online ethics, privacy, and security in addition to being skilled with digital technologies. In addition, the idea of

“vulnerabilities” emphasizes the possible dangers and flaws people may encounter on the huge, linked internet. The need for digital education is urgent because of these risks, which can range from inadvertent data disclosure to falling for sophisticated online frauds.

2. Review of Literature

First and foremost, it is vital to define what exactly is meant by cybercrime in order to determine the actual dimension of these digital threats. Vadza (2013) states that cybercrime is defined as any criminal offense that is committed using the computer, as the tool or the target (like for example hacking or DOS attacks), or both. Despite being often related to normal traditional criminal behaviour (like theft, fraud, forgery, defamation under the Indian penal code), this criminal act is particularly deadly in the digital medium and in fact many believe that this form of crime is often more terrifying and fatal than traditional crime, due to its sheer magnitude.

Because of this severity, gaining knowledge about the methods used by cybercriminals is extremely important. Gunjan, Kumar, and Avdhanam (2013) explore how cybercrimes have evolved over the years, noting a dangerous shift in techniques, targets, and the growing sophistication of online criminal activities. They emphasize that understanding these patterns is vital, as cybercrimes can cause long-term and sometimes irreversible harm to individuals, organizations, and governments. Echoing this, Veresha (2018) points out that these activities pose direct risks to data, financial resources, and the personal safety of individuals. Furthermore, Nayak and Das (2013) highlight the broader consequences of these digital threats, noting their profound impacts on social, economic, and political structures.

The rapid shift in global communication has acted as a major catalyst for these vulnerabilities. As Soomro and Hussain (2019) observe, the internet has completely transformed human interaction, replacing traditional letters and face-to-face meetings with emails, video calls, and global social media platforms. However, they warn that the sheer volume, velocity, and variety of social media networking have generated severe new privacy and security concerns. Beyond technological shifts, cybercrime is also heavily influenced by socio-economic environments. Kshetri (2016) developed a framework demonstrating how formal and informal institutions (such as laws, government policies, and social norms), alongside wealth disparities and international relations, deeply impact cybercrime. His findings reveal that a nation’s level of development and institutional performance significantly dictate its cybersecurity landscape, particularly in underdeveloped nations.

Due to the sophisticated nature of cybercrimes, tracking, laws and prevention tactics are necessary. A data-based system is imperative, whereby, statistical tools are used to analyze cybercriminals as pointed out

by Kshetri (2013). Such data, should then, inform preventive tactics (Veresha, 2018) which was illustrated when statistical data were used to study the impact of cyber laws and the Malaysian Government's responses on cybercrime (Jayabalan, Ibrahim, and Manaf, 2014). Finally, mitigation is achieved when efforts are jointly coordinated. The laws would be initiated by the Government; however, tech firms carry the responsibility of not just detecting and prevention of crimes actively (Nayak and Das, 2013) but through an ever-improving system of prevention techniques (Soomro & Hussain, 2019).

3. Methodology

This research is based on a mixed-methods case study design to gain in-depth insights into CURAJ students' digital awareness and susceptibility to online threats. Quantitative data was collected from a structured online questionnaire (n=27), examining the digital usage, familiarity with various platforms, and basic knowledge about cybersecurity. Semi structured in-depth interviews (n=15) followed, and qualitative data was elicited to supplement survey data by looking into aspects like online privacy and experience with scams. Furthermore, a systematic review of literature was conducted on online threats to build a theoretical background for the collected data.

4. Cyber Threats

There are several risks that might disrupt digital environments and jeopardize people's security in the field of cybersecurity. Malware, which includes viruses, worms, trojan horses, ransomware, and spyware, poses a serious danger by corrupting systems, interfering with business processes, and allowing unauthorized access to confidential data. Phishing assaults are cunning tactics where fraudsters pretend as reliable institutions to trick people into disclosing sensitive information, such as passwords and credit card numbers. Using deceptive methods like impersonation and luring schemes, social engineering techniques force people into unintentionally disclosing private information. Attacks known as Distributed Denial of Service (DDoS) bombard online systems with excessive traffic, which makes them sluggish or even crash. Data manipulation may result from Man-in-the-Middle (MitM) attacks, which include intercepting and changing communication between parties without their knowledge. When unauthorized access is achieved, personal information, financial information, or intellectual property are exposed. Identity theft is a serious issue that includes hackers taking personal data from victims to impersonate them. This leads to monetary loss, poor credit, and legal issues. Online scams, which range from fraudulent tech help programmes to lottery hoaxes, deceive people into handing over money or private information. Ransomware encrypts data and

demands bitcoin in exchange for their release; however, paying the ransom may not always result in the recovery of the encrypted contents. An emerging digital threat known as cyberbullying causes emotional harm to victims through harassment and humiliation. Devices are susceptible on insecure Wi-Fi networks, enabling for data interception and unauthorized access. If IoT devices don't have enough security, Internet of Things vulnerabilities might jeopardize home networks and user privacy. Zero-Day exploits provide hackers an edge while a fix is being created by taking advantage of software flaws that suppliers are unaware of. Credential stuffing is another concerning practise where attackers take advantage of users' propensity for reuse by leveraging username and password combinations from one site's database to obtain unauthorized access to other accounts. These attacks highlight the urgent need for strong cybersecurity measures and digital literacy in order to protect people.

5. Presentation of Cases

Participants during non-working days offered insightful responses to the question about daily screen time on digital devices, including computers, smartphones, and tablets. No respondents reported using digital devices for between one and two hours, showing a considerable departure from this time range. Instead, a sizeable portion 4 participants acknowledged using digital gadgets for two to four hours every day. A noteworthy finding was that 13 respondents said they had spent between 4 and 6 hours, which represents a sizable share of the participants. What was even more startling was the finding that a large majority 25 people used their digital gadgets for at least 6 hours per day. This significant reaction reveals a common pattern across participants, pointing to a high degree of digital participation in their everyday lives and the potential for it to affect a number of elements of their routines and activities.

No respondents mentioned using digital devices for between one and two hours each day on working days, showing a noteworthy absence during this period. A small but significant proportion of respondents to the poll, totaling 8, confessed devoting 2 to 4 hours per day. The bulk of the participants, who consisted of 21 responders, admitted to sleeping between 4 and 6 hours each day. 13 people also admitted to using their gadgets for 6 hours or longer, underscoring the fact that a sizeable portion of the population was heavily engrossed in their digital screens. These comments highlight the participants' common screen-time habits and highlight how ingrained role digital devices play in participants' everyday lives.

42 people responded to the question "Which of the following online platforms do you use frequently?" and shared insightful information about their online habits. Social media emerged as the most popular platform

among these respondents, with all 42 participants confirming their participation in a variety of social media networks. Particularly, 10 respondents mentioned using Facebook frequently, underscoring the platform's continued popularity with the sampled population. Instagram also showed up as a favourite platform, with a significant 25 respondents admitting to using it frequently. Instagram is a visual-focused social networking site. Even while fewer respondents picked Twitter, it nevertheless had importance because seven of them confirmed regular usage. These answers highlight the various social media preferences among the sampled population and highlight the crucial role that these platforms play in their online interactions and social networking activities.

Regarding messaging platform preferences, all 42 participants reported utilizing digital communication tools in their daily lives. WhatsApp overwhelmingly dominated as the primary medium, frequently used by 38 respondents. The remaining participants were evenly split, utilizing either Facebook Messenger (n=2) or other alternative texting services (n=2). These findings underscore the ubiquitous nature of instant messaging applications in contemporary student communication, explicitly highlighting WhatsApp as the central hub for their digital interactions. From the 42 respondents (n=35), they chose YouTube as a primary platform for online learning, much larger than other structured e-learning platforms, Coursera (n=4), BYJU's (n=2), and UpGrad (n=1). The results revealed that YouTube provided the most accessed instruction to this group of respondents, while a supplement form of a course-based e-learning platform was adopted to be YouTube alternatives to some extent. Of the 28 people who played games online, these varied across the genres. Games in the category 'battle royale competition', e.g. PUBG (n=8) and Free Fire (n=7), comprised more than half of the users currently playing games online. People also tended to play games of strategy, where Clash of Clans had a significant uptake from 6 users. A smaller number played 'online casual board games' i.e. Ludo (n=4) and 'online puzzle games' e.g. Candy Crush (n=3).

Participants' replies to the question "How confident do you feel about identifying and avoiding online scams?" revealed a varied picture of their digital literacy and awareness. A significant number of respondents, 13 people, stated that they were "very confident" in spotting and avoiding internet frauds. In addition, 17 people said they were "somewhat confident", indicating a modest level of confidence in their ability to traverse the digital realm safely. In contrast, 8 respondents stated that they were "not very confident", indicating a vulnerability to internet frauds. The study also indicated that 5 participants, a small but substantial proportion, were "not at all" confident in their ability to recognize and avoid online frauds, underlining the vital need for digital education and awareness in this area.

These different replies highlight the survey group's diverse degrees of digital literacy, emphasizing the significance of focused training activities to improve online safety and empower individuals to navigate the digital domain securely.

Regarding whether respondents have previously attended any digital awareness or online safety sessions or not. Many of the respondents (n=40) have never attended any sessions. Only two of them have participated in formal digital education program. The comparison shows the stark lack of digital education programs for those sampled. This demonstrates the need to implement more effective and affordable programs and campaigns to enhance students' knowledge.

Table-1: Cybersecurity Knowledge

Cybersecurity knowledge	Yes	No
Phishing	19	23
Identity theft	38	4
Social engineering	16	26
Data breach	18	24
Malware	39	3
Cyberbullying /harassment	36	6
Unsecured wifi network	12	30

The study gave a comprehensive perspective of participants' cybersecurity expertise, covering topics such as phishing, identity theft, social engineering, data breaches, malware, cyberbullying, and insecure Wi-Fi networks. Impressively, 38 respondents indicated knowledge of identity theft, demonstrating a high level of awareness in this sector. Similarly, a sizable majority of 39 participants demonstrated knowledge of malware, demonstrating their familiarity with this digital menace. Social engineering, a sophisticated cyber strategy, was identified by 16 respondents, indicating a modest degree of awareness. In contrast, the survey revealed areas where individuals lacked expertise. Only 19 respondents knew phishing, a common internet fraud, showing a significant knowledge gap. Furthermore, 18 participants were aware of data breaches, and 12 were aware of the hazards connected with insecure Wi-Fi networks. Cyberbullying, a disturbing online behaviour, was identified by 36 respondents, although there remained a group of 6 people who were unaware of the situation. These findings highlight both the participants' cybersecurity knowledge's strengths and flaws. While many people knew concerns like identity theft and malware, there were major gaps in understanding phishing, social engineering, and unprotected Wi-Fi network vulnerabilities. Addressing these gaps is critical for improving digital literacy and maintaining a safer online environment for everyone. The

findings highlight the importance of tailored educational activities that focus on specific cybersecurity issues in order to raise participants' awareness and encourage a secure digital experience.

Participants' replies to the question "Do you use strong, unique passwords for your online accounts?" revealed varied levels of password security practises. By consistently using strong and unique passwords for their accounts, 12 respondents displayed a great dedication to online security. A larger group of 19 participants recognized the significance of password strength, deciding to use strong and unique passwords on occasion, demonstrating a proactive attitude to their online security, but not consistently. On the other hand, 11 respondents highlighted a troubling trend, confessing to seldom using strong and unique passwords in their online accounts. These replies reflect a range of security practises among those polled. While many people understand the necessity of strong passwords, there is still a requirement for regular adherence to this critical cybersecurity practise. The findings highlight the significance of ongoing education and awareness programmes to urge users to prioritize strong password management, hence improving their overall digital safety. Developing a practise of using strong, unique passwords on a regular basis can considerably help to protect sensitive online information.

The survey revealed a profound lack of awareness regarding institutional digital literacy initiatives. Specifically, all 42 respondents (100% of the sample) stated they were entirely unaware of any digital literacy programs offered by the Central University of Rajasthan (CURAJ). This total absence of awareness indicates a severe communication breakdown between the university administration and the student body. The findings suggest that while CURAJ may provide resources, current outreach strategies are failing to reach the target demographic, thereby limiting students' access to critical digital skill development. Consequently, there is an urgent need for the institution to overhaul its communication strategies to ensure students are informed of, and can actively engage with, available digital literacy tools, fostering a more secure online academic environment.

6. Personal Experiences of Students

In a recent incident respondent 1, enrolled in the department of artificial intelligence, found himself facing financial difficulties and urgently needed funds. During this crisis, he learned about online money lending apps, providing instant financial assistance upon submission of identification documents and a selfie. He availed himself of this option, successfully securing the required funds after the initial registration. He diligently repaid the borrowed amount along with the stipulated interest rates. However, despite his timely repayments, he experienced an unexpected increase in the

interest rates. Ignoring the subsequent calls, he faced continuous and threatening messages via WhatsApp. Faced with this alarming situation, he took the matter seriously and filed a formal complaint with the local police station. Complicating matters, the lending company was headquartered in Delhi, posing logistical challenges. Fortunately, after some efforts, the issue was eventually resolved, highlighting the complexities and risks associated with online financial transactions.

Respondent 2, a student enrolled at CURAJ, accessed an educational platform for her academic needs. During her visit, she refrained from providing any personal information such as her phone number or email address. However, shortly after her interaction with the site, she began receiving a barrage of unsolicited emails from the platform. The situation escalated when, starting the next day, she received persistent phone calls from various numbers affiliated with the same education platform, continuing over several days. Perplexed and alarmed by this intrusion into her privacy, she decided to take a stand and informed the callers that she intended to report the matter to the police. The incident left her questioning the security measures of the platform, pondering over how her data was compromised and how the platform acquired her contact number without her consent.

Respondent 3, a student at CURAJ, found herself entangled in a deeply unsettling privacy breach. Unbeknownst to her, security cameras captured her images, which were then circulated among guards who sought further personal details about her. Upon discovering this violation of her privacy, she expressed her profound distress, stating, "I was anxious, worried, terrified. I don't know what was happening." This invasive incident was not only distressing but also had a significant impact on her mental well-being. Investigation revealed that a senior security officer was responsible for this breach of privacy. Subsequently, the officer was arrested, and legal proceedings are currently underway in the court to address this serious violation of her privacy rights.

Respondent 4, a diligent student enrolled in the Department of Social Work, found himself entangled in a distressing ordeal that shook his sense of security. The distressing situation unfolded when he began receiving a flurry of alarming phone calls and messages from concerned friends and relatives, all questioning the sudden financial desperation he seemed to be facing. Perplexed and initially unaware of the cause, he delved deeper into the issue and was horrified to discover that he had fallen victim to a malicious identity theft scheme. In this troubling scenario, an unknown impostor had craftily constructed a fake Facebook account under his name. Exploiting the trust of his friends and connections, this impostor deceitfully portrayed a scenario of urgent crisis, leading to solicitation for funds. Realizing the gravity of the

situation, he swiftly took action to protect his reputation and alert his network. He promptly informed his friends about the fraudulent account, aiming to raise awareness about the scam that was preying on his social circles. Understanding the need for formal intervention, he wasted no time and decided to escalate the matter to the authorities. With a resolute determination for justice, he filed a comprehensive complaint with the local police, initiating a formal investigation into the identity theft and financial fraud. Despite these efforts, the identity of the perpetrator remains elusive, shrouded in anonymity, leaving he and his social circle in a state of heightened vigilance and concern. This incident serves as a stark reminder of the challenges posed by digital impersonation and the importance of digital literacy and online security in the modern age.

7. Discussion

The findings of this study reveal a stark dual narrative among the students of the Central University of Rajasthan (CURAJ): they possess a high degree of digital participation, yet they face severe vulnerabilities in the online landscape. Digital devices are deeply ingrained in the students' daily lives, with a significant majority spending over six hours per day on screens during non-working days, and no participants reporting less than two hours of daily use. Social media engagement is universal, with all 42 respondents actively participating in networks like Instagram and Facebook, while heavily relying on WhatsApp for messaging and YouTube for online learning. Despite this extensive immersion, the study exposes a concerning gap in the students' ability to securely navigate the digital world. Confidence in identifying and avoiding online scams is highly mixed, with several students indicating they are "not very confident" or "not at all" confident in their abilities, exposing a direct vulnerability to online frauds.

This vulnerability is further highlighted by specific gaps in cybersecurity knowledge and inconsistent safety practices. While students demonstrate a high awareness of widespread threats like malware and identity theft, there are significant knowledge gaps regarding deceptive cyber tactics such as phishing, social engineering, and the dangers of unsecured Wi-Fi networks. This theoretical vulnerability is compounded by poor password management; only a fraction of respondents consistently use strong and unique passwords, while a troubling number admit to rarely using them, leaving their sensitive online information exposed to potential breaches.

The theoretical risks associated with these knowledge gaps are validated by the distressing personal experiences of the students interviewed, demonstrating that the digital landscape has subjected CURAJ students to severe, real-world consequences. Students reported falling victim to predatory online money lending apps that resulted in persistent harassment,

as well as experiencing unwarranted privacy intrusions and data compromises from educational platforms. Furthermore, students have faced severe identity theft schemes on Facebook utilized for financial fraud, deeply unsettling privacy breaches involving campus security cameras, and targeted harassment against minority students on platforms like WhatsApp. These incidents highlight the tangible dangers students face and the urgent need for a secure and tolerant digital community.

Perhaps the most critical finding of this study is the systemic failure of institutional outreach regarding digital education. An overwhelming majority of the sample 40 out of 42 respondents have never attended any digital awareness or online safety sessions. Furthermore, absolutely every participant (100% of the sample) stated they were completely unaware of any digital literacy programs offered by CURAJ. This total absence of awareness signifies a severe communication breakdown between the university administration and the student body. While the university may have resources available, current strategies are entirely failing to reach the target demographic, depriving students of the critical knowledge required to protect themselves and magnifying their insecurity over the internet. Ultimately, bridging this communication gap and mandating digital literacy education is vital for fostering a safe academic environment.

8. Conclusion and Recommendations

This study reveals a dual narrative: one of active digital engagement among participants, and another of insufficient awareness regarding essential digital literacy programs. The participants' heavy reliance on digital platforms, especially social media, underscores the need for comprehensive digital literacy education to ensure safe and responsible online behaviour. Furthermore, the lack of awareness about available digital literacy initiatives indicates a significant area for improvement within the educational institution.

Enhanced Digital Literacy Programs: CURAJ should invest in robust digital literacy programs, encompassing online safety, privacy protection, and responsible digital citizenship. These programs should be widely promoted and made easily accessible to all students.

Regular Workshops and Training Sessions: Organize regular workshops, webinars, and training sessions focusing on cybersecurity, online scams, and safe internet practices. These sessions should be interactive and tailored to address specific concerns raised by the students.

Collaboration with Industry Experts: Collaborate with cybersecurity experts, industry professionals, and digital safety organizations to conduct specialized workshops. Real-world insights can significantly enhance students' understanding of digital threats and how to mitigate them.

Promotion and Awareness Campaigns: Implement extensive awareness campaigns within the university, using various mediums such as posters, social media, and university newsletters.

Encourage students to actively participate in these campaigns to foster a culture of digital responsibility. Regular Updates and Refreshers: Given the ever-evolving nature of digital threats, provide regular updates and refreshers on the latest cybersecurity practices. Encourage students to remain vigilant and proactive in keeping their digital skills up-to-date. By implementing these recommendations, CURAJ can bridge the existing knowledge gap, empowering its students with essential digital literacy skills and creating a safer digital environment within the university community.

References

- Al-Janabi, S., and Al-Shourbaji, I., "A Study of Cyber Security Awareness in Educational Environment in the Middle East", *J. Inf. Knowl. Manag*, 15(01), 2016, 15, 1650007.
- Aloul, F.A., "The Need for Effective Information Security Awareness", *J. Adv. Inf. Technol*, 3(3), 2012, 176-183.
- Armstrong, M. E., Jones, K. S., Namin, A. S., and Newton, D. C., "The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), 2018, 709-713. <https://doi.org/10.1177/1541931218621161>
- Broadhurst, R., and Chang, L. Y., "Cybercrime in Asia: Trends and challenges", *Handbook of Asian Criminology*, Chapter 4, New York: Springer, 2012, 49-63.
- Das, S., and Nayak, T., "Impact of cybercrime: Issues and challenges", *International Journal of Engineering Sciences & Emerging Technologies*, 6(2), 2013, 142-153.
- Florencio, D., and Herley, C., "A Large-Scale Study of Web Password Habits", *Proceedings of the 16th International Conference on World Wide Web*, Banff, AB, Canada, 8-12 May 2007.
- Garba, A., Maheyazah, B. S., Siti, H., and Ibrahim, B. D., "Cyber security awareness among university students: A case study", *Science Proceedings Series*, 2(1), 2020, 82-86. <https://doi.org/10.31580/sps.v2i1.1320>
- Han, G., Yu, Y., Li, X., Chen, K., and Li, H., "Characterizing the semantics of passwords: The role of Pinyin for Chinese Netizens", *Comput. Stand. Interfaces*, 54, 2017, 20-28.
- Iqbal, J., and Beigh, B. M., "Cybercrime in India: Trends and challenges", *International Journal of Innovations & Advancement in Computer Science*, 6(12), 2017, 187-196.
- Kshetri, N., "Reliability, validity, comparability and practical utility of cybercrime-related data, metrics, and information", *Information*, 4(1), 2013, 117-123.
- Kshetri, N., "Cybercrime and cybersecurity in India: causes, consequences and implications for the future", *Crime, Law and Social Change*, 66(3), 2016, 313-338.
- Sad, S. N., and O. G'oktas, "Preservice teachers' perceptions about using mobile phones and laptops in education as mobile learning tools", *British Journal of Educational Technology*, 45(4), 2013, 606-618.

- Sait, S.M., Al-Tawil, K.M., Ali, S., and Hussain, A., *Use and effect of Internet in Saudi Arabia*, KFUPM: Dhahran, Saudi Arabia, 2003.
- Senthilkumar, K., and Easwaramoorthy, S., "A Survey on Cyber Security awareness among college students in Tamil Nadu", *Proceedings of the IOP Conference Series: Materials Science and Engineering*, Vellore, India, 2-3 May 2017.
- Shaukat, K., Luo, S., Chen, S., and Liu, D., "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective", *Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS)*, Albany, NY, USA, 17-18 March 2022.
- Soomro, T. R., and Hussain, M., "Social Media-Related Cybercrimes and Techniques for Their Prevention", *Appl. Comput. Syst.*, 24(1), 2019, 9-17.
- Valcke, M., B. De Wever, H. Van Keer, and T. Schellens, "Long-term study of safe internet use of young children", *Computers & Education*, 57(1), 2011, 1292-1305, .
- Veresha, R., "Preventive measures against computer related crimes: Approaching an individual", *Informatologia*, 51(3-4), 2018, 189-199. ★