Journal of Technological Information, Management & Engineering Sciences (2025),6(2), 91-103

DOI : https://doi.org/10.5281/zenodo.23985077

Cybersecurity Awareness Among University Students: A Structured Narrative Review of Recent Empirical Evidence

[1]**Dr. Momina Iqbal**
[2]**Hafsa Adil**

How to cite this article:

Iqbal, M., & Adil, H. (2025). Cybersecurity Awareness Among University Students: A Structured Narrative Review of Recent Empirical Evidence *Journal of Technological Information, Management & Engineering Sciences* , 6(2), 91-103.

Received	Accepted	Published
27 August 2025	16 Oct 2025	29 Dec 2025

Abstract

This research paper explores the representation of digital control through smart spaces in Don DeLillo's The Body Artist and Cosmopolis from the perspectives of Jannice Kall and Shoshana Zuboff. The selected novels differ in their settings, human behavior, and narrative structure; however, they share similar capital control, technological intervention, and human subjectivity. This paper examines how digitized spaces reorganize human agency, identity, embodiment, and perception while exposing the economic structures underlying this digital culture. The isolated coastal house in The Body Artist becomes a space of uncertain personal identity, temporal instability, and altered perception. The novel does not explicitly depict a fully developed smart environment; its treatment of spatial isolation, unstable subjectivity, and mediated communication gives an empirical basis to examine digital control in the characters' experience. On the other hand, digital information, technological infrastructures, financial networks, and surveillance dominate the urban environment of Cosmopolis. Eric Packer's technologically advanced limousine functions as an automobile through which Packer mediates his relationship with digital and financial markets. This shows how the intervention of digital capitalism makes urban space into an instrument of social differentiation, surveillance, and economic calculation.

Keywords: *Cybersecurity awareness, University students, Cyber hygiene, Security behavior, Higher Education, Pakistan.*

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
Corresponding Email : mominaiqbal@gmail.com
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan
Email : hafsiadil2656@gmail.com

Copyright (c) 2025 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Introduction:

Background

Students use digital infrastructure every day, in their classrooms, on their personal devices, through social media and on the cloud, in support of their learning, evaluation, communication and administration at the university. This convergence increases students as potential entry points to institutional networks and as frequent victims of cyber threats. Risky user behaviour is an insurmountable hurdle to technical safeguards. According to the 2025 Verizon Data Breach Investigations Report, which includes an analysis of 22,052 security incidents and 12,195 confirmed breaches, a human element played a role in approximately 60% of breaches (Verizon, 2025). These are data from the organizational environment, not the campus, but do show the importance of user knowledge and behavior as part of the central security variables.

Generally, cybersecurity awareness can be defined as the knowledge and understanding that a person has about any cybersecurity issues, the impact they may be having, and what they must do to resolve it (Khan, Ikram, Saleem, et al., 2023). Awareness is wider than technical terminology; it includes attitudes towards risk and the habits in which protective measures are embedded, such as, creating strong passwords, checking links, updating software and securing hardware. Khan, Ikram, Saleem et al. (2023) point out that despite the regular use of the Internet by university students, it is rarely addressed by the institutions regarding security. Student security behavior has implications beyond personal security in Pakistan where there is a large youth population, a growing digital economy and freelance employees (Khan, Ikram, Saleem, et al., 2023).

problem statement and significance.

Although there has been an increase in research interest in student awareness, the evidence is not easily synthesized overall. The various studies have different ways of measuring awareness, from self-reported knowledge of the words to validated behavioral scales, and findings vary regarding the degree of awareness

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

and the role of demographic variables. If there is no consolidated view, universities can design awareness programmes by making assumptions instead of basing them on evidence. This paper attempts to solve this problem by summarizing the most recent empirical results and making implications for higher education practice. The synthesis is important for institutional policy, curriculum outline design, and the general campaign to develop a culture of security among young adults.

Literature Review

Exploring the three components of Awareness, Attitudes, and Behavior as concepts. Human-factors security science often presents a dichotomy between knowledge and attitude, and between attitude and behavior. The Human Aspects of Information Security Questionnaire (HAIS-Q), for example, was created to identify employee awareness on a number of security focus areas by using these components (Parsons et al., 2014). Some organisational research on the relation between rationality-based beliefs and information security awareness and compliance with information security policy has been conducted (Bulgurcu et al., 2010). One consistent message has been that information about safety does not translate to action for safety. Khan, Ikram, Saleem, et al. (2023) found that the majority of students participating in their study in Pakistan were a profile of low risky online behavior but low security practices, meaning that caution does not necessarily lead to safeguarding practices.

Measurement Approaches

Conclusion is influenced by the choice of measurement. The Security Behavior Intentions Scale (SeBIS) includes 16 items that are broken down into device securement, password generation, proactive awareness, and updating (Egelman & Peer, 2015). Bognár and Bottyán (2024) created and tested a personal cybersecurity awareness scale for university students, which involved the application of exploratory and confirmatory factor analyses and structural equation modeling, and they found five dimensions of cybersecurity behavior. Some others (Md Kasim et al., 2025) use Likert-type self-assessment of familiarity with practices and terminology. Self-report instruments are efficient and can be

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

scaled, but may capture self-reported or intended behaviour rather than observed behaviour, as highlighted in the literature (Khan, Ikram, Saleem et al., 2023).

Demonstrates knowledge of demographic and contextual correlates.

Studies with respect to individual differences have yielded inconsistent results. McCormac et al. (2017) concluded that, age and gender explained a moderate amount (roughly 7%) of the differences in security practices among working adults in Australia. Öğütçü et al. (2016) reported that students exhibited more risky behaviors than academics and staff in a university community. A comparison of countries has been carried out using SeBIS, which highlighted differences in behaviour between countries, indicating that caution should be exercised when generalizing from one context to another. (Sawaya et al., 2017) In addition to demographic factors, Dodel and Mesch (2019) have come up with an integrated model that suggests that the cognitive, socioeconomic and digital factors interact with each other to influence cyber-safety practices. This view is evident in the recent discussion of digital inequality in developing countries, where access to the Internet and socioeconomic status could influence protective behavior (Khan, Ikram, & Saleem, 2023).

Research Gap

From this body of work there are three gaps. Conceptual and measurement heterogeneity makes comparisons difficult: self-rated familiarity, knowledge tests, and behavioral-intention scales are sometimes used interchangeably to measure awareness, but they are measuring different constructs. Second, studies on the relationship between gender, age, discipline, and geography are contradictory, and only a small number of studies explored these factors in conjunction with digital access and socioeconomic factors. Third, the evidence on Pakistan found in the sources surveyed for this review comes mainly from one research group's survey program, so it is not clear how well it generalises to other provinces and institution types. Such a synthesis and comparison of recent research between awareness and behaviour, with an identification of the recurring contextual factors is justified.

Objectives

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

This paper aims to provide a synthesis of the recent empirical evidence regarding cybersecurity awareness of university students. The specific objectives are:

To explain the extent of cybersecurity awareness and cybersecurity practices found in recent student surveys.

To determine demographic and contextual variables linked with differences in awareness.

To explore the link between awareness, security measures and risky online behavior patterns.

4. To draw implications that can guide awareness activities in the university and future studies with evidence.

Methodology

Research Design

A structured narrative review was used in this study, which is a secondary research design that involves a search for and synthesis of data from published empirical studies. The design allows for comparing results between contexts and instruments without gathering additional data from human participants. This is not a systematic review, and does not meet the PRISMA guidelines.

How to search for information and where to find it

The search was carried out in October 2026 using a general web search engine that brings up journal websites, open access indexes and repositories, such as PubMed Central and Directory of Open Access Journals. Search strings included words like cybersecurity awareness, university students, security behavior, cyber hygiene and Pakistan. Records were analyzed using title and abstract, and then read on the publisher's page or full text when open access was available. The retrieved articles were used to identify foundational sources related to the human aspects of the information security issue.

Eligibility Criteria

Studies were included if they (a) included empirical data from university or college students, (b) measured cybersecurity awareness, security practices, or risky online behaviors, (c) were published between 2023 and 2026, and (d) had an English-language abstract or full text that was easily accessible. The core set

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

excluded theses, conference abstracts and studies of non-student groups. Only seven studies were able to be retained, not all, but illustrative.

Data extraction and synthesis.

The context, sample size, sampling approach, instrument, main findings, and recommendations were identified for each study. Instruments, scales and analytic methods varied, so quantitative pooling was not appropriate; instead, quantitative finding results were synthesized in a narrative and organized by the review objectives. Statistics are reported as published with no values being recalculated or imputed.

Ethical Considerations

This review was completed without the participation of humans and only published secondary sources were used, which means formal ethical approval was not required. All sources have been cited in the bibliography.

Results

Characteristics of the Included Studies

Table 1 provides an overview of the seven studies selected. The samples ranged from 142 to 361 students and all seven used self-report surveys among those who gave an indication of sample size in abstracts.

Table 1

Summary of Included Empirical Studies

The context of a text should be restated in the form of a textual sample and a discussion of design.

Md Kasim et al. (2025) Malaysia Overall awareness was high (M = 4.656, SD = 0.792 on a 5-point scale), significantly higher in the age group of 18–24, and slightly less in the age group of 25–34.

Hantouly & Alzboun (2025) Jordan Descriptive survey; stratified random sample (n = 361) Moderate cybersecurity culture awareness, concept, and domains; no significant differences by gender, academic level, or college.

Titi (2026) Jordan Structured survey; n = 150; Several academic departments; Computing and IT students more prepared than others; urban students were more aware than rural students.

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Ahmed et al. (2023) in Somaliland (Mogadishu) used questionnaire on the respondents, n = 250, at five Universities, significant differences were identified and the problems were: viruses, weak passwords, phishing and social network misuse.

Khan, Ikram, Saleem et al. (2023) surveyed 294 participants (6 universities, risky behavior) and 281 participants (6 universities, secure behavior) and found that proactive awareness predicted lower risky behaviors, although some differences were found based on gender, age, and Internet-access frequency.

Lax smartphone security behavior among students with more Internet access and high socio-economic status (N = 306) stratified multistage sampling; Khan, Ikram, & Saleem (2023) Pakistan Survey on smartphone security

Bognár & Bottyán (2024) Student in the university environment (scale development)Exploratory and confirmatory factor analysis, structural equation model Developed a validated, personal cybersecurity awareness scale containing five dimensions of behavior and compared male and female, age, discipline, and cultural groups.

Note. The information is based on article abstracts, as well as on the full text of the article for Khan, Ikram, Saleem, et al. (2023).

Levels of Awareness

Awareness was reported on a study-by-study and instrument-by-instrument basis. The overall awareness level of 142 Malaysian university students (M = 4.656, SD = 0.792 on a five-point scale) was found high by Md Kasim et al. (2025). On the other hand, Hantouly and Alzboun (2025), conducted a study on cybersecurity culture, concepts, and domains awareness among Jordanian students with a stratified random sampling of 361 students, and found that students' awareness was in the medium level. Research on practices as opposed to self-reported familiarity yielded poorer results. The study by Khan, Ikram and Saleem (2023) found that 306 Pakistani students had lax information security practices when using their smartphones, whereas Ahmed et al. (2023) reported issues with students in Mogadishu using their smartphones for virus attacks, weak passwords, phishing and misuse of social networks.

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

What are the differences in the population and contexts?What are the differences in the population and context?

Gender. Hantouly and Alzboun (2025) found no statistically significant differences between males and females, by academic level, or college. In Khan's et al. (2023) Pakistani sample, the gender difference on the security behavior measure was not significant ($p = .853$), but there was a significant difference between the Internet risky behavior measures with women reporting significantly less risky behavior than men ($p < .001$), and men accounted for 82.6% of the high-risk, low-security cluster.

Age. According to Md Kasim et al. (2025), the age group 18-24 showed higher level of awareness compared to the age group 25-34. While Khan et al. (2023) did not see any difference in security behavior based on age, they did see a difference in risky behavior, with students between 18-20 years being less risk-prone than students between 21-25 years ($p = .024$).

Discipline and geography. Titi (2026) reported that the students of computing and information technology had a better preparation compared to other disciplines and the awareness of urban students was higher than that of rural students. In contrast, Khan, Ikram, Saleem et al. (2023) did not observe any significant difference between urban and rural areas on either measure.

Institution and digital access. Ahmed et al. (2023) reported that there were significant differences across five universities in Mogadishu, suggesting an impact of the institutional context. The Pakistani data indicated that more frequent access to the Internet was associated with more secure behavior as compared to less frequent use, $\chi^2(2, N = 281) = 10.51$, $p = .005$ (Khan, Ikram, Saleem, et al., 2023). Similarly, Khan et al. (2023) found a positive relationship between increased Internet access and increased ability to use the settings and disaster recovery mechanisms on smartphones.

The elements of awareness, practice and risky behavior

Khan, Ikram, Saleem, et al. (2023) profiled students on measures of security and risky behaviors using cluster analysis. There were three profiles: low risky behavior with good security practices (36.3%), low risky behavior with weak

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

security practices (47.3%) and high risky behavior with weak security practices (16.4%). Results of a hierarchical regression indicated that checking links before clicking and ensuring the safety of information submitted significantly predicted the lower level of risky behavior (B = 0.654, β = .269; $p < .001$), and also the four dimensions of security behavior accounted for an additional 8.9 percentage points in the explained variance ($\Delta R^2 = .089$).

All studies that made recommendations generally advocated educational action. The training courses to promote cybersecurity culture was suggested by Hantouly & Alzboun (2025); for the practical, age-sensitive training was proposed by Md Kasim et al. (2025); for integration of cybersecurity topics into curricula across all fields of study was proposed by Titi (2026); for educating student and parents about safe Internet usage was proposed by Ahmed et al. (2023); and for tailor-made training and interventions was proposed by the study conducted in Pakistan (Khan, Ikram, Saleem, et al., 2023; Khan, Ikram, & Saleem, 2023).

Discussion

The Principal Finding is interpreted as follows:

Three patterns emerge. Firstly, the level of awareness is subjective and can be measured in several different ways. There is a moderate level of perceived awareness (Hantouly & Alzboun, 2025), and there is a weak level of behavior on the measures focused on practice (Khan, Ikram, & Saleem, 2023; Khan, Ikram, Saleem, et al., 2023), while self-rated familiarity scores are high (Md Kasim et al., 2025). This separation is in line with the human factors paradigm and its knowledge–attitude–behaviour model (Parsons et al., 2014) and indicates that security knowledge does not automatically imply security behaviour. The fact that the biggest Pakistani profile had low risky behavior coupled with poor security practices does prove the point. The contrast should only be interpreted as indicative, as the studies are not a like-for-like comparison due to the differences in country, sampling and instrument.

Secondly, the demographic effects are not consistent. Students in some samples were differentiated by gender, age, discipline, and geography; in others, they were not. This heterogeneity is consistent with previous studies, which indicated

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

that only a small percentage of the variance in behavior is attributable to demographic variables (McCormac et al., 2017), as well as cross-national differences that make generalizations difficult (Sawaya et al., 2017). It may seem like the most obvious correlate because compute students were better prepared (Titi, 2026); but it is not that other students are safe, it is that exposure to security content at present is highly dependent on field of study.

Third, there are correlates of access and of institutional context. The variation in regard to the frequency of Internet use, socioeconomic status, and university indicate that the digital-inequality perspective proposed by Dodel and Mesch (2019) is relevant. Students who do not use the digital technologies often may not have as many opportunities to build security habits, while institutions that give students different instructions, may end up with different results (Ahmed et al., 2023).

Implications for Universities

The evidence backings four practical directions. To the extent that the SeBIS measures (Egelman & Peer, 2015) address behavior, the first step in awareness programs should be to focus on behavior and not terminology, including password management, verifying links, updating software and locking devices. Second, content must be able to be spread across all disciplines, for instance, in orientation or general education classes as Titi (2026) suggests. Third, programs should be tailored: the Pakistani profile analysis indicates that programs should be targeted at students who engage in risky behaviors and demonstrate a lack of security practices (Khan, Ikram, Saleem, et al., 2023), and age-responsive formats are recommended by Md Kasim et al. (2025). Fourth, programs should be tested for effectiveness before they are scaled, which Khan, Ikram, Saleem, et al. (2023) are connected to the constraints on budgets for security interventions in developing countries.

Limitations

There are some limitations to these conclusions. The review is narrative and not comprehensive, and was conducted with open web sources, not a comprehensive set of subscription databases, so relevant studies may not have been identified.

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Most included studies provided abstracts from published articles, which makes it difficult to assess sampling, instruments, and effect sizes in most of the studies. Several of the studies were based on convenience samples or small samples, and the studies relied on self-report data that may have overstated or underestimated behavior; in fact, the studies in question note that their samples are too small to be generalizable (Md Kasim et al. 2025). Lastly, no formal risk-of-bias assessment was done and there was no quantitative pooling due to instrument heterogeneity. Directions for future research.

The instruments used in the current study should be validated behavior-based instruments (e.g., SeBIS or the scale developed by Bognár and Bottyán 2024) and knowledge measures to allow for direct comparison between awareness and behavior in the future. To determine if the trends observed above are generalizable, multi-institution, probability-based samples are required in each province of Pakistan. Complementing self-report, observed or experimental indicators, including simulated phishing exercises, would be useful; and longitudinal assessments would help determine the effectiveness of training formats in driving lasting behavior change.

Conclusion

This structured narrative review critically synthesized seven recent studies on cybersecurity awareness of University students and placed them in the human-factors literature. At the level of reported awareness, from moderate to high, students' knowledge and familiarisation with the issue, as perceived, are limited, while in relation to practice-oriented measures, there are recurring low levels in terms of security of their smartphone, management of their password, and verification of links. The differences across contexts are not consistent in terms of the demographics, however, the disciplines, digital access and institutional context are apparent as meaningful correlates. In the case of Pakistani undergraduates, proactive security behavior was positively related to lower risky online behavior, thus the case of behavior-based training was supported. Therefore, the awareness should be not "knowledge" but "practiced habits", should be taught in all subjects, should be adapted to sensitive target groups and

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

should be monitored for its results. This paper is a secondary synthesis, so it has tentative conclusions, and primary, validated, multi-institution studies are required to validate the conclusions.

References

Ahmed, A. A., Elmi, A. H., Abdullahi, A., & Ahmed, A. Y. (2023). A comparative study on cyber security awareness of Mogadishu University students. Indonesian Journal of Electrical Engineering and Computer Science, 32(3), 1580–1588. https://doi.org/10.11591/ijeecs.v32.i3.pp1580-1588

Bognár, L. and Bottyán, L. (2024). Development and validation of personal cybersecurity awareness scale among university students. Education Sciences, 14(6), Article 588. https://doi.org/10.3390/educsci14060588

In fact, bulgurcu, Cavusoglu, and Benbasat are correct.In fact, bulgurcu, Cavusoglu and Benbasat are right. (2010). An empirical study of rationality-based beliefs and information security awareness in information security policy compliance. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

Dodel, M., & Mesch, G. (2019). An integrated model of cyber-safety behaviors: The roles of cognitive, socioeconomic and digital determinants in a variety of safety behaviors. Computers & Security, 86, 75–91. https://doi.org/10.1016/j.cose.2019.05.023

Egelman, S., & Peer, E. (2015). Creating a security behaviour intentions scale (SeBIS). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '92).In CHI '92: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2873–2882). ACM.

Hantouly, A. and Alzboun, M. S. (2025). The actual awareness of the Jordanian university students regarding the culture of cyber security, concepts and domains from their perspective. Manarah, Educational and Psychological Sciences Series, 4(1). https://doi.org/10.59759/educational.v4i1.748

Khan, N. F., Ikram, N., & Saleem, S. (2023). Empirical findings on Digital Divide and Socio-economic disparity in Smartphone information security behaviour among university students in Pakistan. International Journal of Mobile Communications, 22(1). https://www.inderscience.com/offers.php?id=131802

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Risky behaviours and cyber-security in a developing country context: Pakistan's perspective. Security Journal, 36(2), 373–405. https://doi.org/10.1057/s41284-022-00343-4

MCCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences, personal attitudes to information security. Computers in Human Behavior, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Md Kasim, M. F. R., Wan Abu Bakar, W. H. R., Mohamad, Z., & Kamarozaman, Z. (2025). University students' cybersecurity awareness in the era of digital. Jurnal 'Ulwan, 10(2), 140–156. https://www.ejournal.unimel.edu.my/index.php/JULWAN/article/view/2060

Öğütçü G., Testik Ö. M., & Chouseinoglou, O. (2016). Research into personal information security practices and knowledge. Computers & Security, 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Measuring employees' awareness by the use of Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Sawaya Y., Sharif M., Christin N., Kubota A., Nakarai A., Yamada A. (2017). Self-confidence is more important than knowledge: A cross-cultural comparison of security behavior. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 2202–2214). ACM.

Titi, K. M. I. (2026). The analysis of awareness and security practices of students in Jordanian universities regarding cyber security. S. Koelman, S. Al Nagi and D. Arshad, "An Architecture for Distributed Computing in SSI," Indonesian Journal of Electrical Engineering and Computer Science, 42(2), 619–630, 2008. https://doi.org/10.11591/ijeecs.v42.i2.pp619-630

Verizon. (2025). 2025 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[1] Department of Management Sciences, National University of Sciences and Technology, Islamabad, Pakistan
[2] Department of Computer Science, COMSATS University Islamabad, Pakistan

Copyright (c) 2026 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.