frontiers | Frontiers in Computer Science

TYPE Editorial
PUBLISHED 03 June 2025
DOI 10.3389/fcomp.2025.1631362

OPEN ACCESS

EDITED AND REVIEWED BY
Nicola Zannone,
Eindhoven University of Technology, Netherlands

*CORRESPONDENCE
Muhammad Adnan Khan
✉ adnan@gachon.ac.kr

RECEIVED 19 May 2025
ACCEPTED 20 May 2025
PUBLISHED 03 June 2025

CITATION
Saeed S, Jhanjhi NZ, Khan MA and Yadav DK (2025) Editorial: Digital transformation and cybersecurity challenges.
Front. Comput. Sci. 7:1631362.
doi: 10.3389/fcomp.2025.1631362

Editorial: Digital transformation and cybersecurity challenges

Saqib Saeed[1], Noor Zaman Jhanjhi[2], Muhammad Adnan Khan[3]* and Dileep Kumar Yadav[4]

[1]College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia, [2]School of Computer Science, Faculty of Innovation & Technology, Taylor's University, Subang Jaya, Malaysia, [3]Department of Software, Faculty of Artificial Intelligence and Software, Gachon University, Seongnam-si, Republic of Korea, [4]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India

KEYWORDS

cybersecurity, phishing detection, machine learning, postquantum cryptography, digital transformation

Editorial on the Research Topic
Digital transformation and cybersecurity challenges

1 Introduction

The concept of digital transformation is, without a doubt, the most sought-after way for today's organizations to become and remain relevant, nimble, and in the lead through the innovation of technology and the increasing reliance on digital ecosystems—such is the reality of an era characterized by the ever-growing technological surge (Portion et al., 2023; Wang, 2023). Right from government institutions and multinational corporations to healthcare systems and educational entities, the way we work, the way we communicate, as well as the way we provide services to end-users everything changed dramatically and is being reshaped through digital transformation initiatives (Radenković et al., 2023). However, as the digitization process is getting faster, the complexity and range of cyberattacks grow in parallel (Sanmorino, 2023). The coexistence of two technologies, namely digital transformation, and cybersecurity, can pose several threats and opportunities; hence, it is remarkable that life is made better with the application of these innovative trends and, at the same time, it is the primary cause of generative threats that require urgent readiness to respond, prevent, and protect in this era of digitization (Irmak et al., 2023).

The title "*Digital Transformation and Cybersecurity Challenges*," designed specifically for this Research Topic, is an early, good look into the changing landscape of technology advances, and the various security implications that come with all of the emergent issues (Zatnika and Safariah, 2023). The successful implementation of digital transformation goes beyond only technology—it implies a profound change in organizational culture, process reengineering, data strategy, and end-user communication (Davaasuren, 2023). The transformation encompasses many other technologies as well, like cloud computing, IoT, artificial intelligence for decision-making, blockchain, remote work infrastructure, and many others (Autsadee et al., 2023). Nonetheless, as the journey is taken toward digital maturity, organizations increase their attacks' surface and make them vulnerable to more sophisticated cyberattacks (Multazam and Widiarto, 2023).

Recent global incidents are pieces of evidence of the severe impact of cyber threats on the business, administrative, and user data leakage; however, they are also a demonstration of the continuous search for identification by the attackers (Kuczewska et al., 2023). Although we do witness technological development at lightning speed, the bad actors in the cyber world are always ahead of the innovations (Lottu et al., 2023). No longer are ransomware, phishing, deceitful inducement, advanced persistent threats, and insider attacks all conjectures that you do not have to worry about (Belkhamza, 2023). These risks have become day-to-day events no longer based on a technicality only, but have shown signs of the vulnerability of human beings, the gaps in the organization, and the weak governance frameworks (Ha and Chuah, 2023).

As companies are making their way through digital transformation, cybersecurity is not just a matter of the periphery but now become a strategic pillar (Nazari and Musilek, 2023). This matter seeks to give a clear idea of how urgent the necessity of creating a cybersecurity structure that fits in with digital innovation in society (Lesmana et al., 2023). Although security professionals are the most important and valuable people as they make us feel safe, today their role needs to be fulfilled with a multidisciplinary approach that involves psychology, law, moral philosophy, and cultural diversity (Mijwil et al., 2023).

This Research Topic of articles reveals one of the most crucial topics in cybersecurity: human influence (Housawi and Lytras, 2023). There are a lot of studies that conclude that the number one weakness in the cyber domain is the human factor, and at the same time, it is the first protected one. The fact that all these threat vectors, such as social engineering attacks, poor password behavior, phishing, insider threats, etc., are derived from the user, perpetuates the necessity to make people more secure first by awareness, training, and the cultivation of user-centric security frameworks. It is necessary to deep-dive into the aspect of people's perceptions and behaviors when they deal with the risks during cyber incidents; the Research Topic is especially important when organizations are trying to raise awareness of security issues as well as building a high level of security-conscious culture (Saeed et al., 2023).

Besides, there is an issue of similar importance that needs to be raised—ensuring the privacy of personal information in the new world of data-as-coin (Alenezi and Akour, 2023). As the digital services that users gain access to become more individual-oriented, concerns about privacy, consent, and data misuse are becoming ever more acute. The legislation, for example, GDPR, has had a crack at making the data analytics industry conduct business in a morally responsible manner, but many issues still have been raised, mainly due to differences in the public and system culture and technical gaps (Tavana et al., 2022).

Moreover, the content of the journal issue demonstrates that it is forward-looking by matching the courses of some emerging paradigms in the industry with the development of cybersecurity, such as quantum computing and machine learning (Alsaywid et al., 2023). An example of quantum computing is a technology that can potentially overthrow old encryption models, making businesses have to change their security architecture. The inclusion of a zero-trust model in the organization's design, as a precautionary measure, is increasing as a response to security threats and changes in organizations. At the same time, machine learning, and AI present a dual use case where they are not only used for threat detection and mitigation but at the same time, they raise new ethical and security issues such as bias, explainability, and misuse.

The Research Topic of the magazine is an opportunity for the community to discuss the readiness of organizations and the implications of policies. The translation of an organization to be cyber-ready in a digital world is the conversation starter. How do regulations, rules, and governance structures adapt to the constant technological changes in the evolving technological environment? The necessity of cross-sector collaboration, cyber threat intelligence sharing, and the availability of an integrated response mechanism cannot be overestimated. Furthermore, there is always one issue that needs to be studied, which is cybersecurity from a sociocultural perspective. This is to ascertain how the community perceives threats, deals with technology, and gives priority to security.

The Research Topic comprises various scholarly contributions and entails some theories, cases, practices, and different disciplines. This Research Topic has been put into print for the main reason that it is informative and will provide readers with a deep understanding of the subject matter, that is, citizen engagement in cybersecurity, ethical dilemmas in data handling, legal frameworks for digital security, and the role of culture that is instrumental in the formation of cybersecurity awareness are some of the topics included in the magazine.

The kind of blog that we were allowed to work on, we hope, can be highly useful to researchers, practitioners, policymakers, and technologists at the same time. At a point in time, when cyber-readiness edges subsume digital convenience, and cyber threats are more of a certainty, a call for strong, inclusive, and flexible cybersecurity measures is really loud. We encourage our readers to share these discoveries, to give a thought to the current problems, and to join in the worldwide effort aimed at keeping the digital future secure.

2 Research Topic

In this Research Topic, eight articles bring the newest research trends at the intersection of digital transformation and cybersecurity. Diverse in number, starting from quantum threats to blockchain, phishing detection, machine learning in intrusion detection, and the evolving roles in offensive cyber operations, these studies are the drivers of solving the current problems and those that might emerge in the future for the digital future's safety. The summaries of these papers are described below:

In the first article (Almuhammadi and Alghamdi), the authors discussed in a paper the new peril that can influence a cryptocurrency, which, through the usage of blockchain, has secured its place as one of the most important digital innovations of the 21st century. Since blockchain is so much connected to public-key cryptography, the use of quantum computing to attack the networks can leave blockchains vulnerable. The paper is a threat assessment to the $2.7 trillion cryptocurrency market

and a study about which ways for the cryptocurrency industry to switch from being quantum-hackable to quantum-resistant. The paper introduces a novel transition protocol that is less disruptive by conducting a soft fork for the entire migration process, rather than having a hard fork. The success of the protocol is tested through theoretical analysis and it is also statistically compared with other existing solutions, thus confirming the practicality and the best move for blockchain migration after quantum computers.

The second paper (Kour et al.) is devoted to ensuring the cybersecurity of Industry 5.0, where human-centricity, resilience, and sustainability are priorities. This paper is grounded on the cyber security issues within Industry 5.0 that have interconnection and intelligence as their main paradigm. The authors consider the issue not only from a theoretical perspective but also from the empirical one where they run the systematic literature review using the PRISMA methodology and consensus algorithms. The study emphasizes that AI, blockchain technology, and IoT appear to be the primary cybersecurity measures, while the lack of observability, measurability, or traceability has been slowing the growth of engineering and technology in this field. These are the technologies that should, according to the authors, have trans-paradigmatic capability and therefore be multi-paradigm in interpreting and controlling the industry of sustainable and resilient systems by assuring security, trustworthiness, and traceability of the industrial system as a whole.

The third paper (Tamal, Islam, Bhuiyan, Sattar, Prince, et al.) is concerned with the serious problem of phishing attacks, which have grown in complexity and gravity. The authors of the paper present a complete anti-phishing solution that combines an Optimal Feature Vectorization Algorithm (OFVA) and supervised machine learning classifiers. They mine 41 features from a large dataset which contains about 270,000 URLs and compare 15 machine learning algorithms across multiple performance metrics. The model that is based on the random forest technique is the best one as it reaches an accuracy rate of more than 97%. This work solves the problem of a great amount of data that is difficult to mine. However, the model is also easy to implement in real environments, and thus, it offers an excellent direction for further research of practical anti-phishing tools that can be put into operation.

The fourth paper (Ali et al.) makes a very thorough survey of Intrusion Detection Systems (IDS) and the increasing contribution of machine learning and deep learning in boosting their efficiency. This paper outlines new Machine Learning/Deep Learning-based IDS approaches that are required to substitute the outdated IDS-augmented techniques due to higher false identification and lower adaptability toward unknown threats. The coverage is particularly focused on crucial aspects related to IDS, for instance, the datasets, the metrics, the indicators of performance, and the new trends. By weighing up the good and the bad of the current IDS research, possibilities for the future are identified and it is shown how cyber defenses of institutions are improved when AI is proffered as the solution to their security risks.

The fifth paper (Arik et al.) discusses the involvement of Offensive Cyber Operations (OCO) in national and corporate cybersecurity which still is an area hardly touched upon but of utmost importance. The case study presented in this paper is a qualitative one on the issue of OCO that takes the position of the people planning the OCO training as the central actors. Hybrid plainness is the trait of the learning sequences that have been drawn up in the case study. Besides this, the partner version of the company's cyber range and the delegating of cognitive strategies to it are also some of the main components that are mentioned. The research provides a clear insight into the issue of dual competencies—technical and strategic—arguing that for cyber planners to successfully execute cyber campaigns, they must be correctly trained with standardization in OCO training being the solution.

The sixth paper (Tamal, Islam, Bhuiyan, Sattar, et al.) outlines a novel, real-life, tagged dataset that is made for the detection of phishing only using intra-URL features. A focus of 250,000 examples is on the detection of URL anomalies, like in the case of typosquatting, misleading subdomains, and unusual extensions for which only observable features can be exploited. The authors performed OFVA to get 42 features that have a high potential for preventing being used by phishers. Also, by sharing this dataset with the community, the article has made a big step in this area of research and at the same time, this way are being encouraged to establish such security tools that are data-driven, scalable, robust, and efficient.

A seventh paper (Rana et al.) covers the use of attack trees for modeling cyber threats that exist on organizational networks, further developing the traditional method by the association of the FAIR (Factor Analysis of Information Risk) framework. The technique presented in this way can describe the risk involved with it, at each level of the attack tree, thus enabling the analysis of the dependency among the assets and also allowing for more detailed risk evaluation. The study conducted a comparison of the various techniques of threat modeling, and it is demonstrated that the FAIR-enhanced attack tree is quite preferable since it provides more details and can be construed with ease; these are the factors that make it possible for the management or higher authorities to take some initiatives. This way of paper can be even more useful for those who are involved in information security risk management and seek systematic collection and processing of data on the attacked cyber risks according to their nature, size, and location.

In the eighth paper (Saran), the authors conduct a comprehensive review of password hashing algorithms and their ability to defend against time-memory trade-off (TMTO) attacks. Although password hashing is the main step of the authentication and key derivation process, it is also the part that is most targeted by the advanced schemes of cryptanalysis. The paper covers the measures that have been recently developed to be taken for TMTO attacks and how modern hashing schemes are much more resistant to the same. To help developers and the staff members of information systems make decisions on the selection, implementation, and migration of secure hashing algorithms, the work is of real, practical value., With changes in the way the central authentication system works, the insights that have been offered at the end of this review will be important as far as keeping the system simple and also building the structures of the authentication used for the future are concerned.

All in all, these eight papers together present a very good and detailed view of cybersecurity difficulties and clever ideas in the environment of data conversion. From basic security technologies to the strategies of organizations and policy implications, the Research Topic gives us a set of knowledge that is strong and good for scientists, professionals, and policymakers who are seeking to build secure and resilient digital ecosystems.

Author contributions

SS: Formal analysis, Writing – original draft. NJ: Formal analysis, Writing – review & editing. MK: Formal analysis, Writing – original draft. DY: Formal analysis, Writing – review & editing.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Alenezi, M., and Akour, M. (2023). Digital transformation blueprint in higher education: a case study of PSU. *Sustainability* 15:8204. doi: 10.3390/su15108204

Alsaywid, B. S., Qedair, J., Alkhalifah, Y., and Lytras, M. D. (2023). "Research and education skills as a core part of digital transformation in healthcare in Saudi Arabia," in *Digital transformation in healthcare in post-COVID-19 Times* 205–216. doi: 10.1016/B978-0-323-98353-2.00010-1

Autsadee, Y., Jeevan, J., Mohd Salleh, N. H. B., and Othman, M. R. B. (2023). Digital tools and challenges in human resource development and its potential within the maritime sector through bibliometric analysis. *J. Int. Maritime Safety, Environ. Affairs Ship.* 7:2286409. doi: 10.1080/25725084.2023.2286409

Belkhamza, Z. (2023). Cybersecurity in digital transformation applications: analysis of past research and future directions. *Int. Confer. Cyber Warfare Secur.* 18, 19–24. doi: 10.34190/iccws.18.1.1005

Davaasuren, A. (2023). Digital transformations in mongolia: challenges and opportunities. *Inf. Innov.* 18, 13–21. doi: 10.31432/1994-2443-2023-18-2-13-21

Ha, H., and Chuah, C. K. P. (2023). Digital economy in Southeast Asia: challenges, opportunities and future development. *Southeast Asia Multidisc. J.* 23, 19–35. doi: 10.1108/SEAMJ-02-2023-0023

Housawi, A. A., and Lytras, M. D. (2023). "Digital transformation from a health professional practice and training perspective," in *Digital Transformation in Healthcare in Post-COVID-19 Times,* 193–204. doi: 10.1016/B978-0-323-98353-2.00011-3

Irmak, E., Kabalci, E., and Kabalci, Y. (2023). Digital transformation of microgrids: a review of design, operation, optimization, and cybersecurity. *Energies* 16:4590. doi: 10.3390/en16124590

Kuczewska, J., Garbin Praničević, D., Borowicz, A., and Talaja, A. (2023). Digitalni transformacijski proces u sektoru malih i srednjih poduzeća (MSP) u eri pandemije COVID-19. *Management* 28, 27–41. doi: 10.30924/mjcmi.28.2.3

Lesmana, D., Afifuddin, M., and Adriyanto, A. (2023). Challenges and cybersecurity threats in digital economic transformation. *Int. J. Human. Educ. Soc. Sci.* 2:515. doi: 10.55227/ijhess.v2i6.515

Lottu, O. A., Abdul, A. A., Daraojimba, D. O., Alabi, A. M., John-Ladega, A. A., and Daraojimba, C. (2023). Digital transformation in banking: a review of nigeria's journey to economic prosperity. *Int. J. Adv. Econ.* 5, 215–238. doi: 10.51594/ijae.v5i8.572

Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., and Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. *Mesopot. J. CyberSecur.* 2023, 1–6. doi: 10.58496/MJCS/2023/001

Multazam, M. T., and Widiarto, A. E. (2023). Digitalization of the legal system: opportunities and challenges for Indonesia. *Rechtsidee* 11:1014. doi: 10.21070/jihr.v12i2.1014

Nazari, Z., and Musilek, P. (2023). Impact of digital transformation on the energy sector: a review. *Algorithms* 16:211. doi: 10.3390/a16040211

Portion, U. C., Chidimma, I., and Nwokike, C. E. (2023). Digital transformation of public services and its influence on the business landscape in african states. *Int. J. Res. Public. Rev.* 4, 467–472.

Radenković, S. D., Hanić, H., and Bugarčić, M. (2023). "Applying artificial intelligence in the digital transformation of banking sector," in *International Scientific Conference on Digital Transformation in Business: Challenges and New Opportunities,* 19. doi: 10.3390/proceedings2023085019

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., and Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations. *Sensors* 23:6666. doi: 10.3390/s23156666

Sanmorino, A. (2023). Emerging trends in cybersecurity for health technologies. *J. Ilmiah Inf. Global* 14, 76–81. doi: 10.36982/jiig.v14i3.3530

Tavana, M., Shaabani, A., Raeesi Vanani, I., and Kumar Gangadhari, R. (2022). A review of digital transformation on supply chain process management using text mining. *Processes* 10:842. doi: 10.3390/pr10050842

Wang, Z. (2023). Digital transformation and risk management for smes: a systematic review on available evidence. *Adv. Econ. Manag. Polit. Sci.* 65, 209–218. doi: 10.54254/2754-1169/65/20231639

Zatnika, Y., and Safariah, I. (2023). Transformation of management accounting in the digital era: current challenges and opportunities. *J. Mirai Manag.* 8:5282. doi: 10.37531/mirai.v8i2.5282