Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

# Strengthening authentication in online learning environments using public key infrastructure: A literature review

Mohammad Husam Alhumsi [1,*], Hamza Alhumsi [2]

[1]College of Sciences and Theoretical Studies, Saudi Electronic University, Riyadh, Saudi Arabia
[2]Saudi Information Technology Company (SITE), Riyadh, Saudi Arabia

ARTICLE INFO

*Article history:*
Received 19 September 2024
Received in revised form
13 January 2025
Accepted 28 January 2025

*Keywords:*
E-learning security
Privacy concerns
Public key infrastructure
Online authentication
Machine learning security

ABSTRACT

Higher education institutions are increasingly adopting e-learning due to its numerous advantages. Although online education technologies have advanced significantly, issues related to security and privacy have not received adequate attention. This paper reviews existing research on security and privacy challenges in online education, with a particular focus on enhancing online learning environments using Public Key Infrastructure (PKI). The review shows that PKI provides a secure foundation for online interactions by ensuring reliable authentication and data protection. Additionally, both service providers and users benefit from mutual trust when PKI certificates are used to support authentication and authorization processes. Further research could explore how machine learning and deep learning can enhance security measures and strengthen the effectiveness of PKI systems.



## 1. Introduction

Due to the rapid growth of information technology in various parts of the world, online learning has become an essential component of modern education (Li et al., 2023). Electronic learning (e-learning) is a cutting-edge technology that offers a robust and scalable learning platform, enabling real-time collaboration between teachers and students from any location. E-learning programs are widely used in educational institutions today because they allow students to complete assignments, access a variety of educational resources at any time, and electronically share learning records and data with other institutions (Khashan et al., 2023). The COVID-19 pandemic prompted many institutions and organizations to make a significant shift toward online operations (Akacha and Awad, 2023). Consequently, there is a substantial need to implement information security systems, as ensuring information security has become increasingly challenging for these entities (Alghazzawi et al., 2014). For instance, preventing illegal data leaks and intrusions is critical. Alghazzawi et al. (2014) confirmed that actions to prevent unauthorized access and intrusion must be taken seriously. Furthermore, Ali and Zafar (2017) noted that the relationship between e-learning and security and privacy has not received much attention in the literature. Despite the widespread adoption of e-learning and numerous instances of cybersecurity breaches, these two subjects have not been explored together. Successful e-learning environments depend on participants who recognize the importance of security and act accordingly (Ali and Zafar, 2017).

In topics related to information security in e-learning settings, trust is a critical issue that should be emphasized. Kambourakis et al. (2007) asserted that trust must be effectively established between learners and e-learning providers, as confidence is pivotal for building a strong level of trust for both parties. Thus, the concept of "trust" is regarded as an essential component in the processes of distance learning, whether represented by interactive e-learning or traditional face-to-face education. For instance, e-learning providers must employ reliable mechanisms such as authorization, authentication, and accounting, ensuring that users accessing the provider's network are authorized for specific activities or services. In return, learners expect to trust the provider's processes while having restricted access, particularly regarding their confidential personal information (Kambourakis et al., 2007). However, few studies have attempted to

* Corresponding Author.
Email Address: husam101010@gmail.com (M. H. Alhumsi)
https://doi.org/10.21833/ijaas.2025.02.015
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-0189-4443

integrate trust concepts with e-learning applications. The significant increase in users participating in e-learning services implies the existence of various trust models. Kambourakis et al. (2007) argued that existing security schemes in current e-learning systems, e.g., symmetric key techniques like passwords and pre-shared secrets/keys, are inadequate. Kambourakis et al. (2007) added that there is an urgent demand to provide more flexible, configurable, and scalable security mechanisms that can self-adjust as fast as e-learning or m-learning systems evolve. One such mechanism is Public Key Infrastructure (PKI), defined as "a framework used in creating and managing digital certificates and public key encryption" (Danquah and Kwabena-Adade, 2020).

Interestingly, public-key encryption does not require the public key to be secret (Albarqi et al., 2015); however, it must be legitimate to ensure integrity and prevent spoofing and replay attacks. A certificate authority can authenticate a user's public key to confirm that it belongs to that particular user (Mogollon, 2008). This authentication process is a key aspect of PKI, which is a comprehensive system for utilizing digital signatures and public-key encryption. As noted by Lozupone (2018), Entrust Corporation demonstrated in 2017 that PKI not only manages certificates and keys but also enables organizations and institutions to establish reliable and secure networking environments. Thus, the role of PKI is crucial in maintaining the integrity of public-key encryption and enhancing overall security, as it is responsible for managing both certificates and keys. Additionally, any organization or institution can initiate and manage secure networking environments when utilizing PKI. Hence, the purpose of this paper is to shed light on the role of public key infrastructure in strengthening and authenticating online learning environments.

## 2. Literature review

### 2.1. E-learning

The international academic landscape is greatly impacted by the expanding significance of e-learning. Following this worldwide trend, E-learning in higher education has grown significantly in most countries (Alhumsi et al., 2021). E-learning, a technological innovation, is regarded as a new paradigm for contemporary education in the twenty-first century, replacing conventional teaching and learning techniques with more creative ones (Dwiastuty and Sulhan, 2018). The body of research on e-learning is vast, which reflects this growth (Alhumsi et al., 2021; Alsayyar and Almakki, 2021). Using e-learning technology, the progress of the world economy and humankind has benefited greatly from technological advancements (Choudhury and Pattnaik, 2020; Nassani et al., 2023). E-learning is a noticeable type of technical innovation holding out the promotion of economic growth because it helps alter the way trading agreements are carried out. Global implementation of plans for institutional information security and privacy is already underway, and these techniques are now the main focus of scientific studies (Medaglia and Serbanati, 2010). Nassani et al. (2023) stressed that E-learning is the basic driver of privacy and security of a firm. Hence, economic development that promptly prioritizes the management of the company's security and privacy has led to a notable increase in technological challenges and issues for all institutions. Specifically, Nassani et al. (2023) stated that E-learning refers to the formalized delivery of learning and training via digital resources such as tablets, cellular phones, and computers that are connected to the Internet. Despite its reference to knowledge acquisition occurring through digital technologies, there are a number of benefits associated with the concept of "e-learning," involving increased transparency in the supply chain, data security enhancement, increased efficiency due to the removal of middlemen's role, and lower expenses. On the other hand, it does have several disadvantages, involving tackling complicated technology, a dearth of regulations, and having trouble merging outdated systems and rules with blockchain (Nassani et al., 2023).

### 2.2. Privacy and security and e-learning

Nassani et al. (2023) affirmed that Privacy refers to the exact control over how an individual's data and information are used and viewed. It concerns an entity's ability to decide for themselves when, for what reason, and how their personal information is handled by outsiders. As for Security, Zhang et al. (2010) stressed that it is the preservation of human safety, autonomy, and dignity as well as the defense against harm and threats. Dhillon et al. (2021) stated that scholars and professionals have long been concerned about information systems security. Many information systems were not designed with security and protection and there are few safety precautions that can be implemented by using technology. Thus, management and procedures need to be followed correctly (Nassani et al., 2023). It should be noted that hardware, software, organizational frames, procedures, processes, and rules are components of security measures.

In their research, Yee et al. (2007) stressed that the four fundamental elements of the e-learning environment are as follows: Information governance and e-learning security; processes and policies for e-learning data safety; countermeasure implementation; and monitoring of the security countermeasures implemented for protecting e-learning information. Interestingly, the organizational aspect of e-learning components guarantees that security execution meets its goals. E-learning prioritizes security management while offering users flexibility, available access, and guaranteeing confidentiality, and integrity of the content (Akacha and Awad, 2023; Costinela-Luminița and Nicoleta-Magdalena, 2012). Because of the behavioral differences of users in e-learning

environments regarding employing technical tools in comparison with those of other online services, improving information security and privacy in e-learning in particular is significantly needed (Majeed et al., 2016). Thus, an integral aspect of every secure information system is security and privacy.

It should be noted that no matter how good the recommended controls are or how much they can help, a system in which information security cannot be managed is not safe. In e-learning environments, security and privacy must be able to function. Therefore, when businesses are learning and working in such an environment, basic security requirements like integrity, confidentiality, and availability must be met (Nassani, 2023). The growing number of potential information privacy concerns associated with Internet use is making e-learning security management increasingly complex (Nassani, 2023). For example, Costinela-Luminiţa and Nicoleta-Magdalena (2012) highlighted specific security issues related to e-learning platforms, arguing that these platforms should be assessed for vulnerabilities to external intrusions, causing potential threats. Additionally, it is essential for e-learning platforms to provide information on peripheral infiltration risks and guidance on how to use search engines for various queries to gather personalized data, such as session hijacking, password cracking, usernames, and passwords.

As for security threats, Akacha and Awad (2023) emphasized that the growing adoption of e-learning software systems introduces a variety of security threats that must be effectively managed. As more students engage with these platforms, the sensitive data they transmit and store becomes an increasingly attractive target for malicious actors. Significant risks include malware, phishing attempts, ransomware incidents, data breaches, insider threats, and inadequate system security measures. Furthermore, the increased online activity of students raises concerns about exposure to dangerous individuals and potential data theft. Several factors impact e-learning safety, such as educators using potentially unsafe online applications, young children's limited computer skills, and accessing online learning platforms over the unprotected home or public networks (Akacha and Awad, 2023; Saleous et al., 2023; Tick et al., 2021). To address these challenges, machine learning or deep learning techniques could offer more effective solutions.

The integration of machine learning or deep learning into security measures significantly enhances the ability to detect threats and manage risks. For instance, the emergence and development of machine learning have greatly expanded anomaly detection systems' capabilities, providing more efficient, accurate, and adaptable ways to spot anomalies in data (Devineni et al., 2023). In their research paper, Devineni et al. (2023) investigated how machine learning methods can be used to improve anomaly detection, especially in government and commercial data systems. Before looking at the basic machine learning models used in anomaly detection, such as supervised, unsupervised, and semi-supervised learning, the researchers defined anomaly detection and discussed its significance. In addition, their study examined the difficulties of integrating these technologies in the public and private spheres, highlighting the necessity of striking a balance between ethical considerations like data privacy and detection accuracy. At the end of their research, Devineni et al. (2023) demonstrated how machine learning-driven anomaly detection may be used to prevent fraud and strengthen network security, indicating how improvements in big data, processing power, and algorithms might enhance anomaly detection systems. As for deep learning, Aldhaheri et al. (2024) argued that for intrusion detection systems, cybersecurity is a critical problem. It has been demonstrated that deep learning can successfully identify and stop cyberattacks on Internet of Things devices. Conventional intrusion detection systems face difficulties in the setting of the Internet of Things, despite the fact that intrusion detection systems are essential for protecting sensitive data by detecting and stopping suspicious activity (Aldhaheri et al., 2024). Thus, the integration of machine learning or deep learning into security measures not only provides automated and intelligent responses to emerging security challenges but also helps organizations adapt to a continuously evolving threat landscape. By leveraging recent research, educational institutions can better fortify their defenses and ensure the reliability of their digital infrastructures.

### 2.3. PKI and e-learning

The growing popularity of e-learning as a teaching mode has led to a greater focus on data security concerns. Data leakage attacks can now target e-learning environments, potentially leading to privacy violations and other adverse consequences. This creates many critical issues in the eLearning setting (Jorayeva and Eyadat, 2023). Due to these challenges, Jorayeva and Eyadat (2023) investigated the data security issues that eLearning poses with regard to encryption, authentication, and the usage of third-party platforms. Their studies showed that keeping control of the devices that students use to access learning is a good way to protect school gadgets and guarantee security for video collaboration and class work. Tools like mobile device management are also necessary and users' device settings, security profiles, and access levels with this mobile device management tool can be controlled from any location in the world. When such tools are employed with PKI for identity management, it offers a potent security combination. By examining current trends and data security best practices, their research provided insights into how eLearning providers may protect user data and ensure that learning settings are secure (Jorayeva and Eyadat, 2023).

In addition to these findings, Hadan et al. (2021) pointed out that PKI provides the basis for reliable and safe online transactions. Universities and other organizations are turning to e-learning to deliver training online for a number of benefits. The mechanics of delivering online education have advanced significantly, but up until now, the concerns for security and privacy have received very little attention (Ali and Zafar, 2017; Yee et al., 2007). To highlight this issue, Ali and Zafar (2017) and Yee et al. (2007) argued that high degrees of privacy and confidentiality in e-learning systems are clearly going to be required more and more, and security solutions need to be implemented to suit the objectives of related systems. Interestingly, it is a matter of trust; in e-learning systems, trust is a crucial issue pertaining to the acceptance of e-learning presented as a transaction with some risk and distinction from the conventional academic practice and settings (Martins and Nunes, 2016). Therefore, a fundamental prerequisite for both users and providers is a trusted relationship (Maulani et al., 2021; Yee et al., 2007). For instance, a service provider must trust that a student possesses authentic credentials and is authorized to enroll in the course or access specific services. However, the student must also have confidence in the services offered. Above all, the learner must have faith that the service provider will use personal data—such as name, address, payment card information, preferences, and learning habits—only in the ways specified in the policies made available to e-learning system users (Yee et al., 2007).

Significantly, trust is a subjective concept that spans various domains and involves multiple topics, items, and situations. Trust mechanisms are supported by two distinct processes: reputation-based mechanisms and policy-based mechanisms (Ren et al., 2021a). The latter relies on stringent authorization management, often utilizing a public key infrastructure (Ren et al., 2021b). To clarify the concept of trust mechanisms, Xia et al. (2022) provided a definition highlighting the roles of the trustor (the one granting trust) and the trusted party (the one receiving trust) in a typical request scenario. When information is successfully exchanged, the node is seen as trustworthy, leading to an increase in its trust rating. Conversely, if a node provides incorrect information, it is deemed malevolent, and its reputation value is lowered as a form of punishment. This mechanism illustrates that trust can indeed be a double-edged sword.

For the above reason, digital certificate-based Mechanisms are the most often used trust mechanisms in relation to digital certificate-based techniques. The idea that certificates express a trusted party is the foundation for them. The digital certificate is the fundamental idea underlying these techniques. To verify if a public key actually belongs to the stated owner, a certification authority issues a Digital Certificate (Yee et al., 2007). Thus, both service providers and customers can benefit from mutual trust when authentication and authorization services are supported by public key infrastructure and attribute certificates. They also realize how important privacy protection and security features are (Kambourakis et al., 2007). It is interesting to note that a certificate typically consists of the certificate information, the public key, and the digital signature of the certifying authority. The digital signature verifies that the user is the legitimate owner of the public key, and the certificate information includes the user's name and other relevant identity information. The two most often used methods nowadays are PGP and X.509/PKIX based. A framework for the provision of authentication services is defined by X.509/PKIX (Yee et al., 2007). It is important that digital certificate-based trust mechanisms, such as PGP and X.509/PKIX, offer a number of methodical and thorough ways to identify, validate, and manage trusted parties. It has been demonstrated that these procedures are effective means of establishing one entity's credentials when implementing online transactions. Also, the validity of the public key is what determines how confident and trustworthy the user is with these processes (Yee et al., 2007). Despite this significance, certificate-based systems continue to face numerous dangers and uncertainties (Yee et al., 2007). Considering these vulnerabilities, it is important to recognize that cyber adversaries frequently attempt to exfiltrate sensitive information. Given that database servers serve as critical infrastructure for organizations, they often become the primary target of such incursions (Ibrahim et al., 2020). This highlights the need for robust security measures to protect these essential systems from increasingly sophisticated threats.

Consequently, implementing comprehensive security protocols is imperative to thwart malicious attacks aimed at safeguarding end-user data and information. For the previous reason, Ibrahim et al. (2020) conducted a study investigating cybersecurity concerns pertaining to the database management system, e-learning, and its importance. Their research discussed the main database security risks and solutions. For instance, they found that the security component is frequently neglected in numerous online course management systems available to improve the process of collaborative learning. Critically, there are security flaws in the present e-learning platforms that facilitate online education (Abouelmehdi et al., 2018; Ibrahim et al., 2020). This situation could result in security problems that impact administrative functions, including students attempting to gain unauthorized access to their peers' accounts, and tutors or administrators falsifying students' academic performance (Ibrahim et al., 2020).

Consequently, Ibrahim et al. (2020) highlighted the importance of PKIs as a solution for mitigating the risks and challenges and confirmed that such public keys make it easier for users and devices to securely transfer data while maintaining operational integrity, secrecy, and authenticity. Building on this

foundation, Hadan et al. (2021) conducted a comprehensive study involving interviews with eighteen experts—both academicians and practitioners—in the field of security during two conferences. Specifically, the researchers carried out a qualitative and quantitative research design. In the qualitative research, they explored how security and policy specialists perceived PKI and explained how they viewed PKI failures. As for the quantitative study, a quantitative examination of real-world PKI incidents that have been reported online since 2001 was carried out to assess if perceived failures correspond with actual documented failures. The results were surprising; the researchers discovered a discrepancy between expert opinions and actual PKI occurrences. The researchers concluded that significant causes of PKI failures exist, which neither the traditional computer security nor usability communities can effectively address on their own. They identified consistent flaws in organizational procedures that put everyone relying on PKI at risk. Fortunately, their findings also point to configuration and organizational decisions that could reduce or even eliminate some of these vulnerabilities.

Building on the insights into PKI, Kausar et al. (2023) explored a secure e-learning system tailored for the dissemination of examination-related resources, ensuring robust defenses against a spectrum of security threats. The materials involved encompassed quizzes, answer sheets, tests, question papers, answer sheets, and aptitude evaluations. The researchers highlighted the role of PKIs in solving issues concerning e-learning security. For example, they referred to the study conducted by Al-Hamdani (2014). In his empirical study, Al-Hamdani (2014) suggested an e-learning approach for learners to access and obtain data from any location. He noted that a safe e-learning platform that offers availability, confidentiality, and integrity is an essential requirement. Therefore, a novel cryptograph e-learning paradigm based on cryptography access control and PKI is provided by Al-Hamdani (2014). According to the paradigm, a safe shell system relying on PKI must be created, and each block added must be verified in order to be evaluated. One of the key issues with e-learning security is that students can copy any author's text, meaning that they engage with e-cheating. To solve such an issue, cryptography components and PKI can be employed (Al-Hamdani, 2014; Kausar et al., 2023).

In a related exploration, Lozupone (2018) conducted a case study that began with an overview of symmetric and asymmetric encryption systems. He then delved into the benefits and drawbacks of PKI, providing a thorough examination and comparison of symmetric and asymmetric encryption algorithms. In his study, receiver keys and distinct transmitters were used in asymmetric encryption systems. It has been found that it is exceedingly challenging to separate one key from the other; one common key is used by symmetric systems. Lozupone (2018) concluded that symmetric key encryption offers significantly better security than asymmetric key encryption. Since it enables cryptographically secure authentication techniques in risky contexts, TLS plus PKI is a superior option for cloud platforms. The same researcher pointed out that PKI is a collection of tools, policies, software, and technicians that use public key digital infrastructure to administer an environment. In the same vein, in their study, Kambourakis et al. (2007) employed the distribution of attribute certificates over the general packet radio service network as a case study. The researchers focused on the integration of Public Key Infrastructure within the system, highlighting its necessity for supporting attribute certificate technology. They evaluated the application of attribute certificates to enhance mobile technology in education through an experimental test bed adopting the general packet radio service network. Their findings indicated that issuing attribute certificates is feasible within service timeframes, while also providing scalable and flexible solutions for both e-learning providers and learners.

## 3. Conclusions

Consumers and providers eagerly seize the opportunity to implement e-learning programs (Ali and Zafar, 2017). They realize how important privacy protection and security measures are. When an educational institution decides to introduce e-learning programs, it must thoroughly analyze its infrastructure, policies, and strategies to ensure the security of these programs. In addition, an increasing number of e-learners are requesting similar services from operators, and they expect those services to protect their data in transit, secure their customer data, offer dependable mechanisms for authentication, authorization, and accounting, and guarantee availability and high-quality service. For the above reasons, this paper reviews the literature relating to security and privacy concerns regarding online education. In this respect, it explores the empowerment and authentication of online learning environments by employing Public Key Infrastructure, investigating how public key certificates arranged under PKI may offer robust mutual authentication and precise trust management for popular e-learning services. When arranged under a PKI, public key certificates and attribute certificates can offer robust mutual authentication and trust control over e-learning services. It is recommended that there should be an appeal to policymakers, researchers, and practitioners to work together to fully utilize AI-driven PKI in order to create a more robust and safer digital ecosystem. Further studies could provide more focus on how machine learning can improve security posture, strengthen PKI capabilities, and adjust to changing cyberthreats in the digital era. Additionally, case studies, collaboration across industries, and interdisciplinary research are

essential in relation to public key infrastructure (Hadan et al., 2021).

## Compliance with ethical standards

## Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## References


Abouelmehdi K, Beni-Hessane A, and Khaloufi H (2018). Big healthcare data: Preserving security and privacy. Journal of Big Data, 5: 1. https://doi.org/10.1186/s40537-017-0110-7

Akacha SAL and Awad AI (2023). Enhancing security and sustainability of e-learning software systems: A comprehensive vulnerability analysis and recommendations for stakeholders. Sustainability, 15(19): 14132. https://doi.org/10.3390/su151914132

Albarqi A, Alzaid E, Al Ghamdi F, Asiri S, and Kar J (2015). Public key infrastructure: A survey. Journal of Information Security, 6: 31-37. https://doi.org/10.4236/jis.2015.61004

Aldhaheri A, Alwahedi F, Ferrag MA, and Battah A (2024). Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and Cyber-Physical Systems, 4: 110-128. https://doi.org/10.1016/j.iotcps.2023.09.003

Alghazzawi DM, Hasan SH, and Trigui MSA (2014). Information systems threats and vulnerabilities. International Journal of Computer Applications, 89(3): 25-29. https://doi.org/10.5120/15483-4248

Al-Hamdani WA (2014). Secure e-learning and cryptography. In: Sullivan KPH, Czigler PE, and Hellgren JMSC (Eds.), Cases on professional distance education degree programs and practices: Successes, challenges, and issues: 331-369. IGI Global, Pennsylvania, USA. https://doi.org/10.4018/978-1-4666-4486-1.ch012

Alhumsi MH, Alshaye RA, and Sendi KK (2021). The effect of e-learning sessions on the development of reading comprehension: A case of EFL students' perceptions at Saudi electronic university. Journal of Education and e-Learning Research, 8(4): 431-439. https://doi.org/10.20448/journal.509.2021.84.431.439

Ali R and Zafar H (2017). A security and privacy framework for e-learning. International Journal for E-Learning Security, 7(2): 556-566. https://doi.org/10.20533/ijels.2046.4568.2017.0070

Alsayyar A and Almakki R (2021). The impact of augmented reality on E-learning systems in Saudi Arabia universities. Computer and Information Science, 14(2): 50-62. https://doi.org/10.5539/cis.v14n2p50

Choudhury S and Pattnaik S (2020). Emerging themes in e-learning: A review from the stakeholders' perspective. Computers & Education, 144: 103657. https://doi.org/10.1016/j.compedu.2019.103657

Costinela-Luminița CD and Nicoleta-Magdalena CI (2012). E-learning security vulnerabilities. Procedia-Social and Behavioral Sciences, 46: 2297-2301. https://doi.org/10.1016/j.sbspro.2012.05.474

Danquah P and Kwabena-Adade H (2020). Public key infrastructure: An enhanced validation framework. Journal of Information Security, 11(4): 241-260. https://doi.org/10.4236/jis.2020.114016

Devineni SK, Kathiriya S, and Shende A (2023). Machine learning-powered anomaly detection: Enhancing data security and integrity. Journal of Artificial Intelligence and Cloud Computing, 2(2): 1-9. https://doi.org/10.47363/JAICC/2023(2)184

Dhillon G, Smith K, and Dissanayaka I (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4): 101693. https://doi.org/10.1016/j.jsis.2021.101693

Dwiastuty N and Sulhan M (2018). The using of readutainment as e-learning to improve students' reading comprehension skill. In the MATEC Web of Conferences: The 2nd International Conference on Engineering and Technology for Sustainable Development, EDP Sciences, Yogyakarta, Indonesia, 154: 03007. https://doi.org/10.1051/matecconf/201815403007

Hadan H, Serrano N, and Camp LJ (2021). A holistic analysis of web-based public key infrastructure failures: Comparing experts' perceptions and real-world incidents. Journal of Cybersecurity, 7(1): 1-17. https://doi.org/10.1093/cybsec/tyab025

Ibrahim H, Karabatak S, and Abdullahi AA (2020). A study on cybersecurity challenges in e-learning and database management system. In the 8th International Symposium on Digital Forensics and Security, IEEE, Beirut, Lebanon: 1-5. https://doi.org/10.1109/ISDFS49300.2020.9116415

Jorayeva S and Eyadat MS (2023). Ensuring data security in elearning: Challenges and solutions. In the International Conference on Computational Science and Computational Intelligence, IEEE, Las Vegas, USA: 900-906. https://doi.org/10.1109/CSCI62032.2023.00150

Kambourakis G, Kontoni DPN, Rouskas A, and Gritzalis S (2007). A PKI approach for deploying modern secure distributed e-learning and m-learning environments. Computers and Education, 48(1): 1-16. https://doi.org/10.1016/j.compedu.2004.10.017

Kausar S, Huahu X, Ullah A, Wenhao Z, and Shabir MY (2023). Fog-assisted secure data exchange for examination and testing in e-learning system. Mobile Networks and Applications, 28: 673–689. https://doi.org/10.1007/s11036-019-01429-x

Khashan OA, Alamri S, Alomoush W, Alsmadi MK, Atawneh S, and Mir U (2023). Blockchain-based decentralized authentication model for IoT-based e-learning and educational environments. Computers, Materials and Continua, 75(2): 3133-3158. https://doi.org/10.32604/cmc.2023.036217

Li Z, Lou X, Chen M, Li S, Lv C, Song S, and Li L (2023). Students' online learning adaptability and their continuous usage intention across different disciplines. Humanities and Social Sciences Communications, 10: 838. https://doi.org/10.1057/s41599-023-02376-5

Lozupone V (2018). Analyze encryption and public key infrastructure (PKI). International Journal of Information Management, 38(1): 42-44. https://doi.org/10.1016/j.ijinfomgt.2017.08.004

Majeed A, Baadel S, and Haq AU (2016). Global triumph or exploitation of security and privacy concerns in e-learning systems. In the 11th International Conference on Global Security, Safety and Sustainability-The Security Challenges of the Connected World, Springer International Publishing, London, UK: 351-363. https://doi.org/10.1007/978-3-319-51064-4_28

Martins JT and Nunes MB (2016). Academics' e-learning adoption in higher education institutions: A matter of trust. The Learning Organization, 23(5): 299-331. https://doi.org/10.1108/TLO-05-2015-0034

Maulani G, Gunawan G, Leli L, Nabila EA, and Sari WY (2021). Digital certificate authority with blockchain cybersecurity in education. International Journal of Cyber and IT Service Management, 1(1): 136-150. https://doi.org/10.34306/ijcitsm.v1i1.40

Medaglia CM and Serbanati A (2010). An overview of privacy and security issues in the the Internet of Things. In: Giusto D, Iera A, Morabito G, and Atzori L (Eds.), The Internet of Things:

389-395. Springer, New York, USA. https://doi.org/10.1007/978-1-4419-1674-7_38

Mogollon M (2008). Certificates and public key infrastructure. In: Mogollon M (Ed.), Cryptography and security services: mechanisms and applications: 217-245. IGI Global, Pennsylvania, USA. https://doi.org/10.4018/978-1-59904-837-6.ch009

Nassani AA, Grigorescu A, Yousaf Z, Trandafir RA, Javed A, and Haffar M (2023). Leading role of e-learning and blockchain towards privacy and security management: A study of electronics manufacturing firms. Electronics, 12(7): 1579. https://doi.org/10.3390/electronics12071579

Ren Y, Qi J, Liu Y, Wang J, and Kim GJ (2021b). Integrity verification mechanism of sensor data based on bilinear map accumulator. ACM Transactions on Internet Technology, 21(1): 5. https://doi.org/10.1145/3380749

Ren Y, Zhu F, Zhu K, Sharma PK, and Wang J (2021a). Blockchain-based trust establishment mechanism in the Internet of Multimedia Things. Multimedia Tools and Applications, 80: 30653-30676. https://doi.org/10.1007/s11042-020-09578-y

Saleous H, Ismail M, AlDaajeh SH, Madathil N, Alrabaee S, Choo KKR, and Al-Qirim N (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digital Communications and Networks, 9(1): 211-222. https://doi.org/10.1016/j.dcan.2022.06.005 **PMid:35765301 PMCid:PMC9222023**

Tick A, Cranfield DJ, Venter IM, Renaud KV, and Blignaut RJ (2021). Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. Electronics, 10(22): 2865. https://doi.org/10.3390/electronics10222865

Xia Z, Wei Z, and Zhang H (2022). Review on security issues and applications of trust mechanism in wireless sensor networks. Computational Intelligence and Neuroscience, 2022: 3449428. https://doi.org/10.1155/2022/3449428 **PMid:36203716 PMCid:PMC9532060**

Yee G, Xu Y, Korba L, and El-Khatib K (2007). Privacy and security in e-learning. In: Shih TK and Hung J (Eds.), Future directions in distance learning and communication technologies: 52-75. IGI Global, Pennsylvania, USA. https://doi.org/10.4018/978-1-59904-376-0.ch003

Zhang C, Sun J, Zhu X, and Fang Y (2010). Privacy and security for online social networks: Challenges and opportunities. IEEE Network, 24(4): 13-18. https://doi.org/10.1109/MNET.2010.5510913