Journal of Basrah Researches (Sciences) **52**(1), 14 (2026)
DOI: https://doi.org/10.56714/bjrs.52.1.2

The Deep Study of the Role Multi-Factor Authentication in E-Learning Systems: Primitive Tools and Schemes

Duaa A. Sultan*, Ali A. Yassin

Department of Computer Sciences, College of Education for Pure Sciences, University of Basrah, Iraq.

ARTICLE INFO

Received 13November 2025
Revised 04 January 2026
Accepted 07 January 2026
Published 30 June 2026

Keywords:

Blockchain, Role-Based Access Control, Multi-Factor Authentication, Authentication, Educational Systems.

Citation: D. A. Sultan, A. A. Yassin., J. Basrah Res. (Sci.) **52**(1), 14 (2026). DOI:https://doi.org/10.56714/bjrs.52.1.2

ABSTRACT

Modern technology has brought a revolution in all spheres of human life including in educational systems. Different from the traditional classroom methods, current e-learning environments are rapidly overtaking the conventional forms of school training. This is normally achieved through robust platforms designed to boost skill acquisition systems and continuous engagement with learning. This helps in the attainment of interactive and personalized learning for students anywhere and anytime. E-learning is aligned and fully supported by cloud computing technology, which helps in the synchronization of all operational processes. Nevertheless, these technological advancements results in significant challenges such as data insecurity. The main issues surround the assurance that students and trainees sensitive and personal information remain secure from unauthorized access. The most critical concern appears to be insufficient security offered by the data access control mechanisms in these systems. In this regard, Role-Based Access Control (RBAC) has become very prominent in building secure computing systems lately. RBAC grants and blocks computing systems' information access to individuals hinged on their roles and responsibilities. Over the years, numerous other security solutions have been developed, ranging from shared security protocols, single-factor authentication to multi-factor authentication. These security techniques have been implemented through multiple layers and numerous methods such as biometrics, object, and knowledge-based authentications. Such security technologies have been created to help ensure that the three main security characteristics of confidentiality, integrity, and availability, as well as defense against cyber and malicious threats are attained. This paper aims to present and analyze the most popular and significant security solutions and measures developed over the recent past in the e-learning/educational systems domain.

*Corresponding author email: duaa.ashoor@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

1. Introduction

In the era of modern information communication technologies (ICTs), various powerful tools and applications have been increasingly deployed in different spheres of our life such as socializing, healthcare, finance, banking, communication as well as transportation. In these application domains, ICT helps promote efficiency, enhance connectivity, and increase accessibility. Therefore, these modern ICT technologies have triggered innovation and global interconnectedness among societies [1-3].

The education industry is extremely significant nature and can greatly benefit from the connectedness occasioned by ICTs. For instance, blockchain technology can be deployed to keep lasting academic records of individual from their childhood to advanced levels. In addition, educational institutions have adopted various technologies, such as Google Classroom, virtual classrooms and interactive boards. Applications such as Moodle and the Bologna Process have helped transform teaching and learning through personalized experiences. This has seen the enhancement of accessibility which is boosted sharing of academic materials and provision of instant feedback [4].

Although educational platforms and technologies offer numerous benefits, they have serious challenges related to data security. In this environment it is critical to ensure that only legitimate users have access to sensitive data, such as academic and personal information. Devoid of robust data access control mechanisms, educational data can be tampered with by internal as well as external malicious entities. Since education systems rely on various ways of accessing and retrieving data, they should be treated as an integral part of cyber security. In educational systems access can be viewed from the reliability and trust perspectives. Here reliability enhancement techniques range from single factor authentication methods to multifactor authentication techniques. These techniques are deployable in various components of the e-learning systems to support the protection efforts [5].

Owing to the ever-increasing complexity of cyber threats authentication schemes have evolved from single-factor authentication (SFA) to multi-factor authentication (MFA). SFA relies only on passwords or Personal Identification Number (PINs). Although they are straightforward SFA are exposed to security threats such as Man in the Middle (MITM), replay, insider, phishing and credential theft attack [6]. To improve security two-factor authentication (2FA) has been developed. In these methods additional components are included during the authentication process such as sending of codes to personal devices. While these solutions add extra layer of security they are still susceptible to attacks such as Subscriber Identity Module (SIM) swapping and Short Message Service (SMS) interception [7]. To address this challenge the three-factor authentication (3FA) schemes have been developed. Generally 3FA incorporate a biometric element such as a fingerprint or facial recognition. This helps mitigate against threats such as impersonations. However, 3FA is expensive in terms of increased infrastructural costs. It also raises privacy concerns since biometric databases may be compromised [8]. In all these authentication models 3FA is the most prevalent and robust. Basically, it combines two or more factors, including passwords, secret tokens, biometrics and various contexts (such as geo-location and behavioral dynamics).

In terms of usability and cyber defense MFA is the best technique and can deploy Artificial Intelligence (AI)-based detection. Unfortunately, MFA requires improved and expanded element management to enhance scalability and interactivity [9, 10]. Figure 1 gives a depiction of the various factors utilized during the authentication process. The enhancements in access control techniques have led to the development of Role-Based Access Control (RBAC) to act as an additional layer in the protection of devices. The incorporation of RBAC with MFA can boost safety and efficiency [5, 9]. For instance, this integration can enable schools ensure that only students have access to course materials and can submit assignments. In this way teachers can keep track on the work of pupils in addition to helping them with better planning of their classes. Moreover, this integration enables administrators to have complete control over system settings and important data. Using RBAC the system is designed in a hierarchical way which helps thwart attacks at lower levels. Essentially, RBAC ensures that access privileges are proportionate to user responsibilities. Therefore, the convergence of MFA and RBAC represents a significant step towards building adaptive and scalable authentication systems.

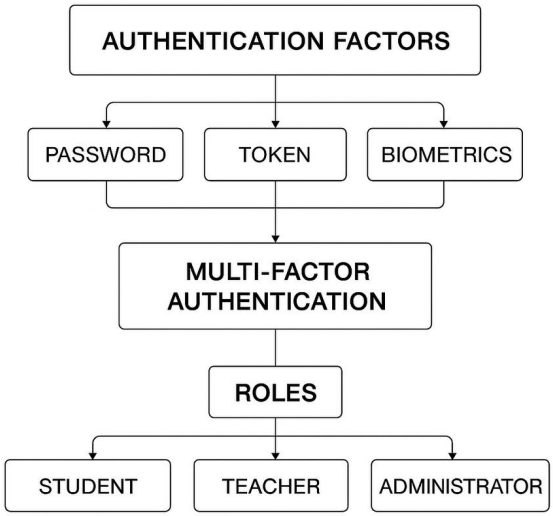


Fig.1. Authentication with Roles

This is particularly important in educational and research environments where security must be carefully balanced with accessibility and usability. Table 1 presents the tasks and requirements of each component of these systems.

Table 1. System components and roles in educational data system

Component	**Authentication Type**	**Role**	**Description**
Student	2FA	Data Consumer	Registers, logs in, retrieves/searches exam data, grades, and course content
Instructor	3FA	Data Provider	Uploads course materials, exams, grades; authorizes sensitive operations.
Registrar/Admin	MFA	Data Controller	Manages user identities, issues keys, controls access and audit logs.
Exam Server	(2FA) + Digital Certificates	Service Node	Hosts secure exam sessions and stores encrypted exam-related data.
Blockchain Network	(MFA) + Encryption	Integrity Layer	Verifies transactions, logs access, and ensures transparency and immutability.
Searchable Encryption Engine (SEE)	2FA	Search Processor	Performs encrypted keyword search without decrypting content.
Key Distribution Center (KDC)	Advanced (MFA)	Trusted Authority	Manages shared key agreements (can be decentralized with blockchain anchors).

As shown in the Table1, the educational data system has a number of important components. Each of these parts requires a secure and usable authentication method. As shown below, the assignment of authentication factors depends on how sensitive the performed tasks are, and how much access each entity has:

- **Data consumer (student):** The performed tasks may include logging in, obtaining grades, and accessing course materials. A 2FA method is recommended, integrating a password with a one-time passcode (OTP) sent to a personal device.
- **Data provider (instructor):** Offers support for course content uploading, test management and reporting grades. In this environment, a 3FA trust dependency system is recommended, incorporating parameters such as pass-code, mobile verification code, and biological feature (including fingerprint or face recognition). For maximum security, the authentication factors must be changed regularly.
- **Data Owner (Admin/ Registrar):** Responsible for the generation and management of user identities, cryptographic keys and access control. A MFA solution is required which may include a strong password, security device or OTP, biometric factor and contextual checks (such as geo-location) or trusted device validation.
- **Service node (exam server):** this component enables secure and encrypted exams-based sessions while preserving exam generated data. In this environment, 2FA system based on digital certificates is recommended. This typically involves encrypted key exchanges and Secure Sockets Layer / Transport Layer Security (SSL/TLS) certificates. In this way secure server-to-network connection is assured devoid of reliance on human fingerprints.
- **Integrity layer (blockchain network):** This element ensures that transactions are transparent, immutable and properly validated. In this environment MFA using public/private key crypto and digital signatures is appropriate. Owing to the distributed nature of the blockchain this layer greatly benefits from the provided end-to-end security. Through this distributed nature of the blockchain system, more robust cryptographic techniques are offered to boost system integrity.
- **SEE (search processor):** This searchable encryption engine looks for the keywords in their encrypted form devoid of revealing users' private information. Therefore 2FA is recommended consisting of a key and a pass-code.
- **Trusted authority (Key Distribution Center-KDC):** this component oversees the distribution and interchange of keys among the various system participants. Therefore, it is crucial to use a MFA which combines device-based authentication, digital signature verification and a password with sophisticated cryptographic algorithms.

Finally, the main contributions of this paper are illustrated as follows:

- We provide detailed descriptions of the various mechanisms of deploying multi-factor authentication techniques on each of the components of the educational data system.
- This paper delves into the functions of each of the components in the educational system, and how task distribution can be accomplished in an effective manner. In addition, the most prominent risks and cyber-attacks to which the educational systems are exposed are described.
- Advanced tools and cryptographic techniques used in authentication are explored, including searchable encryption and blockchain.

The rest of this paper is structured as follows: Section 2 describes the evolution of authentication models; while Section 3 describes the required security features within the education systems. On the other hand, Section 5 discusses various attacks in the education systems, while Section 5 explains some of the primitive tools for security enhancement and analysis. Finally, Section 6 concludes the paper and gives directions for future research.

2. Related work

The education systems are plagued by various security threats and vulnerabilities that can be exploited by adversaries to compromise these systems. To remediate this, the recent past has seen a substantial rise in the level of interest in incorporating technologies such as blockchain, searchable encryption and MFA into educational systems [11-12]. The purpose of this integration is to improve trust, safeguard privacy and guarantee that academic records are accessed in a secure and accurate manner. This section describes the most recent works in this domain.

In 2021, Raimondo et al., [13] carried out an indepth analysis of the tertiary sector. Their focus was mainly on the use of blockchain in the education sector for the authentication of academic records and credentials. The research looked at privacy, quality, governance and the ongoing crisis of fraudulent

academic records and qualifications. This study identified two main challenges namely post issuance counterfeiting and record tampering. Among the major requirements there is need to effectively address 51% attack, insider risks and source forgery. While much progress has been made in this regard, the authors highlighted that privacy preservations remain a crucial obstacle. For instance the direct storage of sensitive information in the blockchain needs to be critically examined. To mitigate some of these risks off-chain storage solutions in hybrid architecture have been introduced. Specifically, these strategies help alleviate the probability of data loss, manipulation or leakage.

In 2022, Chamani et al., [14] developed a structured cryptographic processing framework with hybrid indexing. This platform allows one to perform searches based on role over encrypted student information and change the data as required. Throughout their investigation, the authors discovered several critical vulnerabilities. For instance, information could be indirectly exposed through query pattern. Therefore, the major security concern was on how to enhance encrypted search. Although the proposed framework generally performed better, it has some faults. The most significant weaknesses is that it could be easily attacked, and could not block all pattern leaks. This implies that the system is still vulnerable to information breaches based on the manner in which queries are formulated. Therefore, further studies are required on how to design searchable encryption schemes that are more efficient and can mitigate information leaks.

In 2022, Wang et al., [15] proposed the notion of attribute-based searchable encryption (AB-SE). This technique combines multi-key searchable encryption and attribute-based access control (ABAC) to achieve very accurate control of access rights. The attribute-based searchable encryption approach allows all learners to access encrypted educational content. One of the key issues has to do with commercial sustainability, owing to the excessive operating costs. On the flip side, the system is very effective at locking out unauthorized entities which helps minimize various risks. However, this system is not very good at handling large requests, and is vulnerable to a Denial-of Service (DoS) attacks. These limitations indicate that additional work needs to be done to advance AB-SE so that educational data systems can process massive real-time queries.

In 2023, Ota et al., [16] investigated how to mix RBAC in cloud-based learning environments with MFA. As such, several MFA schemes such as push-based authentication, TOTP, and 2FA were investigated in this research. However, the study revealed that there are several barriers for widespread deployment of these advanced authenticate methods. Practical considerations, additional installation costs, poor access control, and credential theft are some of the issues that need to be addressed. In addition, dangers such as phishing and social engineering are still feasible in this environment. Nevertheless, this integration possibly helps curb password theft, and MFA can significantly reduced chance of numerous attacks. Further enhancements can be achieved through the deployment of risk-adaptive MFA frameworks. Depending on the vulnerability of the scenario, these frameworks can alter the login processes.

In 2023, Amorim and Costa [17] looked into the use of homomorphic encryption (HE) in searchable encryption (SE). Their investigation revealed that most searchable encryption systems have security challenges. The authors looked at different HE methods for multi-keyword searches, including how HE can be used in real life. The authors revealed that although Python calendars could be deployed here they encountered serious problems such as inadequate methods for revoking permissions. The study further investigated how HE can be utilized to build SE systems catalogue. An evaluation on the effectiveness of such systems revealed that search methods can be modified to interoperate with different systems. However insiders can possibly compromise the system and expose it to various threats. In addition, HE requires complicated cost dynamic changes that can be tricky with multiple keywords. There is therefore need for further improvements to mitigate these limitations.

In 2023 Balobaid et al., [18] introduced a technique that aims to permits encryption and student records management based on blockchain. This approach combines the immutable and decentralized benefits of tamperproof blockchain technology. In addition the system incorporates secure off-chain storage mechanisms such as external storage solutions as well as document encryption. Based on the overall examination of higher education the authors recommended the adoption of blockchain technology in academic institutions for the verification of the identity and credentials of students. The study primarily focused on privacy, performance and governance. This investigation uncovered evidences of tampering with some records and post counterfeiting as the two major threats. In addition other

significant issues included 51% attacks, internal threats and even garbage-in attacks. However privacy considerations remain paramount in this environment owing to the direct keeping of personal infomation on the blockchain. The authors recommended the use of hybrid off-chain storage solutions to mitigate to minimize existing vulnerabilities such as data loss, manipulation or leakages.

In 2024 Abdelmagid et al., [19] presented a framework based on blockchain for credential verification. This system could help maintain the integrity of academic degrees through the use of permissioned blockchain technology via hyperledger. This study combined hyperledger with offchain storage to improve data management. In addition the proposed framework helped reduce the possibility of certificate fraud. The findings indicate that attaining both national integration and scalability is a difficult task. Even though the developed solution sought to increase the dependability and credibility of certificate issuance scalability was still a problem. In addition, this framework did not solve problems associated with performance restrictions or international certification requirements. The authors recommended the adoption of blockchain-based credentialing systems so that national and worldwide accrediting frameworks can be accepted and compatible.

In 2024, Khan, Abbas, and Bensawad [20] investigated the use of ABAC in conjunction with semantic searchable encryption (SSE). In this study, searchable encryption was enhanced by the use of deep learning techniques in conjunction with multi-authority attribute-based encryption. The findings indicated that the deployed blockchain-based semantic search engine is secure. In addition, significant problems were identified, which included complicated key administration, inefficient key management, high computational costs, and long response times. As such the authors endeavored to advance this domain by the enhancement of the safety of encrypted search operations. Nevertheless their proposed approach is still computationally expensive and susceptible to insider and external attacks. Therefore further efforts are required to enhance efficiency and mitigate these dangers.

In (2024) Irenna Wanisha, et al., [21] investigated the domain of MFA systems that rely on blockchain, the equilibrium between privacy and utility as well as various security concerns. The findings reveal that several concerns include high application costs in addition to incompatibility of biometrics solutions. The authors have proposed an authentication method that incorporates blockchain technology and biometric that is geared towards the increase in the level of authentication security. The proposed system recorded substantial reduction in the probability of identity theft. However the usability of system presents some challenges due to issues with its configurations as well as its incompatibility with biometric systems. The challenges with user adoption highlight the necessity of further research on interventions that can enhance the performance of the system as well as its realworld applicability.

In (2024) Narkedimilli et al., [22] proposed the FL-DABE-BC approach that can address privacy issues in IoT federated learning. This system incorporates blockchain technology, secure multi-party computing, symmetric encryption as well as decentralized attribute-based encryption. The study uncovered two major problems, which included expensive processing and hard to use gadgets. Inspired by these issues, the authors design a powerful local data protection system. Despite the fact that the underlying concept is correct, the formulation has several problems that must be addressed. For instance, this approach is both computationally expensive and very hard concept to realize. In addition, this framework is quite difficult to implement on instructional Internet of Things (IoT) hardware, which have resource limitations. As such, this framework must be refined to become more realistic in its real world application scenarios. These enhancements must also include usability to render it user friendly.

In 2025, Apthorpe et al., [23] carried out an in-depth assessment of schools compliance to the implementation of MFA-based techniques. This study included a full investigation of tertiary education policy, as well as the extent to which institutions adhere to the multifaceted standards developed by the National Institute of Standards and Technology (NIST). The results indicated that there is a large disconnect between the ambitions detailed in the policy versus the way in which they are implemented. Based on this inquiry, it was noted that while the adoption of MFA is prevalent within institutions, there is lack of uniformity in the implementation of technical regulations. The authors recommend the empirical study of the 140 issues that underline how security and policy are properly implemented using existing frameworks. Table 2 gives the comparative studies versus the security threats. As shown in Table 2, there are eleven factors whose details are as follows: F1-

privacy; F2- forward/backward secrecy; F3- mutual authentication; F4- confidentiality; F5- data integrity; F6- anonymity & unlikability; F7: auditability; F8- access control; A1- identity theft; A2- DoS attack, and A3- data tampering [5].

Table 2. Comparative studies on security threats

STUDY	A1	A2	A3	F1	F2	F3	F4	F5	F6	F7	F8
[31]	Y	N	Y	Y	NA	NA	Y	Y	NA	NA	NA
[32]	NA	N	Y	Y	Y	Y	NA	Y	Y	NA	NA
[33]	Y	N	Y	Y	NA	NA	NA	Y	NA	Y	Y
[34]	Y	N	NA	NA	NA	Y	Y	NA	NA	NA	NA
[35[	Y	N	Y	Y	NA	NA	Y	NA	Y	Y	NA
[36]	Y	N	Y	NA	NA	NA	Y	Y	NA	NA	Y
[37]	Y	N	Y	Y	NA	Y	NA	Y	NA	NA	NA
[38]	Y	N	Y	Y	NA	Y	Y	Y	Y	Y	NA
[39]	Y	N	Y	Y	Y	Y	NA	Y	Y	NA	NA
[40]	N	N	Y	NA	Y	NA	Y	Y	NA	NA	NA
[41]	NA	N	NA	NA	NA	NA	Y	NA	NA	NA	NA

(N=No, Y=Yes, NA=Not Mentioned)

In this paper, we studies works published between the years 2021 and 2025. The outcomes indicated a gradual adoption of blockchain-based multi-factor searchable encryption schemes, trust models, advanced searchable encryption techniques and adaptive multi-factor authentication systems in higher education. However, various challenges were observed regarding privacy preservation, computing efficiency, usability, scalability and governance limitations. As such, these were identified as meaningful opportunities for future studies in this domain. The reviewed literature underscores the importance of integrated approaches that can fill the gap between the sets of tools or methods with complementary functions required to harmonize security, efficiency and user experience in the development of solid and sustainable secure educational systems.

3. Security features

To safeguard computing devices, networks, and data from unauthorized access, theft or destruction, it is advisable to deploy a combination of practices and tools. These threats affect e-learning systems by compromising students' data. disrupting educational platforms, and stealing sensitive information. Moreover, they undermine users' trust in digital education systems and hinder the secure adoption of modern technologies. The fundamental goal of such integration is the protection of confidentiality, integrity and availability of information and systems. This goal is aligned to popular CIA (confidentiality, integrity and availability) Triad [24], [25], [26]. The most salient security features any system include the following:

3.1 Mutual authentication

This is a way of verification that is reciprocally accepted by all parties participating in the communication process (the client and the server). This approach requires the identity of the sender and receiver be verified prior to accepting any message or document. Formerly this is usually achieved through Mutual Transport Layer Security (mTLS) protocol in which digital certificates of both the client and server are jointly validated. This technique offers robust defense against security threats such as dentity spoofing and MITM attacks. It is especially handy in Zero Trust systems and frameworks that secure communication between various platforms enhancing secrecy during the exchange of documents among network parties.

3.2. Anonymity

This refers to a state in which an identity of entity is ambiguous or indistinguishable from that of other group members. It describes the ability of network element to engage in activities such as surfing, chatting or transacting on the Internet and in cyberspace devoid of disclosing their true identity or any personally identifiable information (PII) that could be used to positively recognize them.

3.3. Unlinkability

This is a design property which ensures that activities, transactions or events carried out by the same entity cannot be amalgamated together to establish a single behavioral profile of this particular entity. In so doing unlinkability helps mitigate the formation of entity behavioral profiles that can be exploited by attackers. In spite of the fact that the actions are already anonymous, it is designed to safeguard against the association of patterns and behaviors of users. This is because entities may remain anonymous, but if the activities they engage in are linked to one another, their privacy can still be jeopardized. By developing robust unlinkability features, the building of such behavioral records is mitigated.

3.4. Forward secrecy

This is a fundamental encryption quality that ensures that an attacker capable of compromising long-term encryption keys is unable to decipher data (that was enciphered using this key) that was captured in the past. This is normally achieved through the use of ephemeral keys, which are utilized only once for each communication session.

3.5. Backward secrecy

This is an encryption property which ensures that if a network entity's current or future encryption keys are compromised, the breach does not allow an attacker to decrypt future communications that occur after a key re-keying. In other words, if the entity's current key is compromised today and a new key (for the next session) is issued tomorrow, the attacker in possession of today's key cannot read tomorrow's messages.

3.6. Privacy

This is a central concept in modern digital world, which involves maintaining the secrecy of information that should remain confidential. This feature enables entities and individuals to decide when, how, and to what extent their personal information is disclosed to others. Privacy also allows entities and users to control how that information is used. In so doing, it facilitates robust control over the flow of information concerning people's lives and identities.

4. Common cyber attacks

The education system faces numerous malicious attacks [27],[28],[29],[30]. The following are some of the most common security threats that require immediate remediation.

- **MITM attack:** This is a security threat in which a malicious actor (the "man in the middle") intercepts private communication between two or more parties (such as between device web servers).
- **Replay attack:** In this threat, an adversary intercepts a legitimate message or set of data transmitted over the network, modifies and then retransmits it/them later. This can facilitate the impersonation of the original sender. Conversely, this attack may involve the execution of the same action repeatedly in an unauthorized manner.
- **Insider attack:** This refers to any security risk that originates from within an organization. It is a threat posed by individuals who have legitimate and authorized access to the organization's physical assets, data, networks, or systems.
- **Impersonation attacks:** These cyber-attacks rely on techniques such as social engineering, where the adversaries pose as legitimate entities in order to trick the target into doing something detrimental to the system security. Instead of trying to hack the system directly, the hacker masquerades as a trusted entity in order to gain the victim's trust and then takes advantage of it.
- **Sniffing:** This threat is also known as packet sniffing and encompasses intercepting and reading of data packets as they traverse computer networks. It is essentially a form of digital eavesdropping

on the exchanged network traffic. On condition that data is not protected via encryption, this technique allows an attacker to read data as if it were "open mail" as it is transmitted across the network.

- **Social engineering:** This is a collection of methods that target the human component of people and organizations rather than technological systems. Using psychological skills, manipulation is deployed to trick individuals into disclosing private information or performing actions that jeopardize their personal safety or the safety of their organizations.
- **Phishing:** It is a technique whose goal is to steal people's private information online. Such data include bank accounts or login information such as usernames and passwords. As such, the primary motivation of this attack to trick others to give the adversary money.
- **Sybil attack:** This is a security threat in which one individual creates and uses a number of phony identities (such as nodes, accounts, or users) to gain massive control over the system. Instead of breaking into one account, this attack seeks to make one person or entity appear like thousands of different individuals or entities.
- **Distributed Denial of Service Attack (DDoS):** This is a cyber-attack whose goal is to disrupt or disable the functioning of a website, server, or a particular online service. To achieve this, adversaries overload the target with massive illicit traffic and requests which exceeds its processing capacity. This effectively blocks the target system's ability to serve genuine clients.
- **51% attack:** This threat targets blockchain networks that are dependent on the Proof-of-Work (PoW) consensus algorithm, such as the Bitcoin network. It occurs when an attacker has a large amount of influence over the decision-making process of the blockchain network. This influence gives the adversary some powers to alter sections of the recent transaction history for their own personal gain.

5. Primitive tools

All contemporary cryptographic protocols and systems are constructed using fundamental building blocks. In the field of information security, these fundamental procedures (such as encryption, hashing, and key exchange) guarantee the preservation of security goals such as confidentiality, integrity, and authenticity of information. The sub-sections below describes some of these tools.

5.1. Blockchain

Blockchain was originally introduced by Satoshi Nakamoto in 2008 as an attack-proof public ledger. Figure 2 gives the pictorial representation of the blockchain structure. At a global scale, blockchain plays a significant role in facilitating tamper-proof concept. It is a decentralized and distributed network that is built for secure management and mutual sharing of the timestamped secrets. Here, each block contains data, its own cryptographic hash, and the hash of the previous block (constituting integrity) and immutability. Principally, blockchain is guided by core philosophies of transparency and decentralization, which underpin a new financial model. The immutability feature allows secure exchange of information without central dependencies. Transactions in the blockchain network reach consensus through a process usually executed by algorithms such as Proof of Work (PoW). This consensus algorithm validates blocks prior to adding them to the blockchain network.

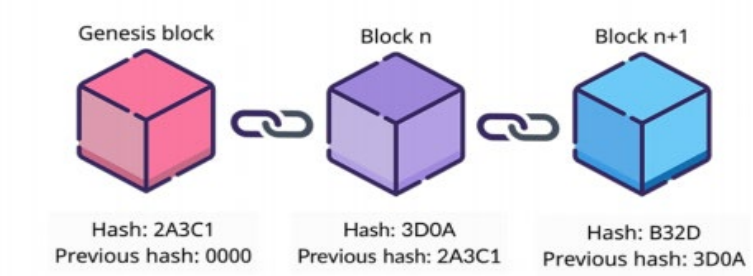


Fig. 2. The blockchain architecture

This structure not only ensures the robustness and tamper-resistance of data but also improves data transparency and privacy through strong cryptographic methods such as SHA-256 algorithm. Owing

to these salient properties blockchain has become a reliable and secure platform for data authorization, identity management and authentication. This is particularly important within heterogeneous domains such as healthcare and IoT,where data confidentiality and integrity are crucial. It Used for storage and decentralized documentation [31], [32], [33], [34], [35].

5.2. Apple File System (APFS)

This is a file system that was developed by Apple that can be deployed in a number of scenarios. Such applications include forensics (such as snapshots), blocklevel encryption, metadata integrity checking (which are comparable to Fletcher-64), B-trees, object mappings, headers to Object Identifier /Transaction/Exchange ID (OID/XID) and so on. Basically APFS is capable of appropriately keeping an eye on changes in systems and files over time. In the event that keys or information are misplaced or stolen, keybag operations and encryption renders it hard to retrieve data. With the assistance of checkpoints and snapshots it is possible to recreate previous states of the system. Other possible techniques for hiding antiforensic information include padding, slack space and undefined fields. Owing to these evasive techniques it is necessary to do a comprehensive low-level block-by-block analysis. In order to carry out a successful forensic investigation it is essential to utilize specialized tools such as AFRO and object identification frameworks. These tools ensure that the recovered evidence is correct and can be verified in an appropriate manner. In order to make a discovery of data that has been disguised or deleted these tools require the preservation of complete block-level photographs comprising of all snapshots as well as the comparison of these images in chronological sequence. It supports strong encryption and fast, efficient copying. Figure 3 shows the architecture of the APFS[36].

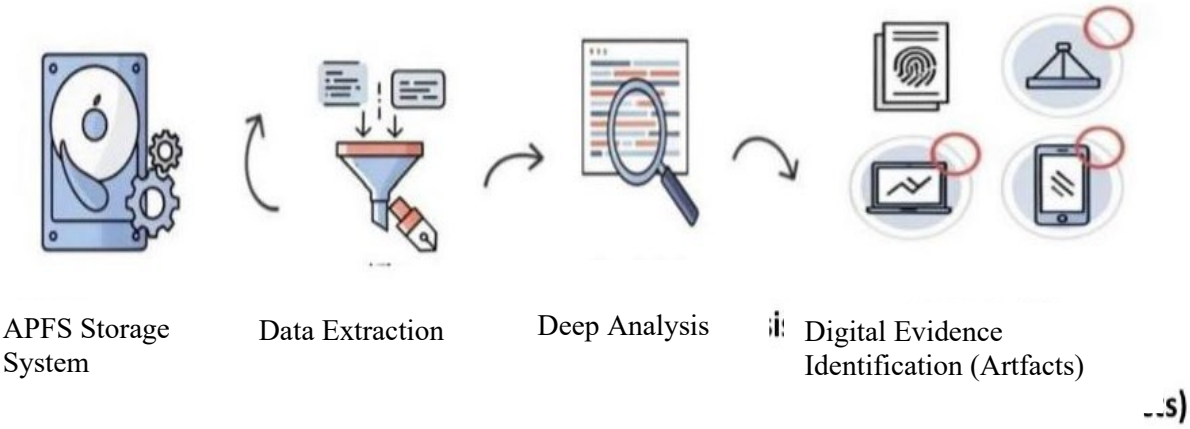
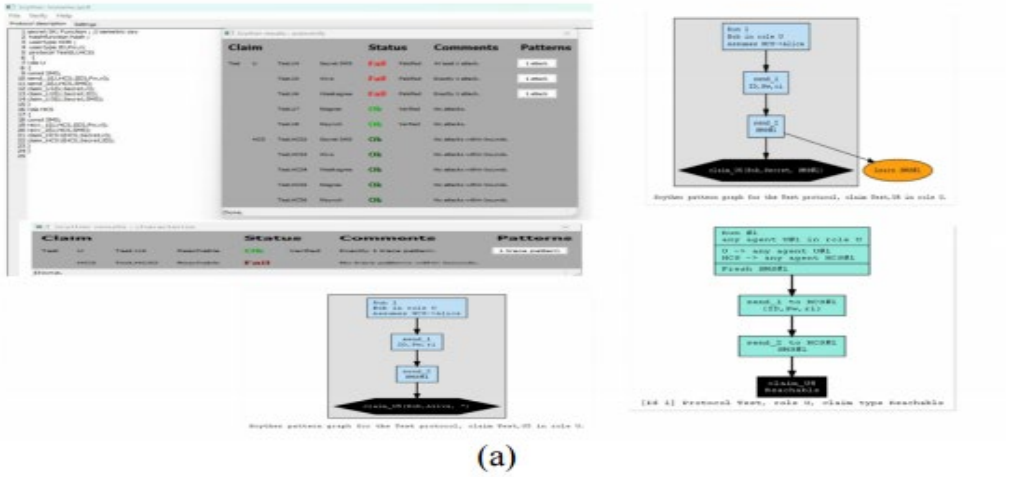


Fig. 3. The apple file system architecture

This is a symbolic security protocols analysis tool designed to automatically verify properties such as confidentiality and authentication. This also includes validation of multi-level claims such as aliveness and agreement. In this tool, users model the protocol in the Security Protocol Description Language (SPDL), and specify the security claims. To determine if the claims hold or if an attack exists, the tool examines the protocol's messages, roles, and keys against a symbolic attacker, presenting any vulnerabilities as concrete attack scenarios. Scyther is popular, owing to its rapid attack discovery (falsification). This popularity is also attributed to its accessible modeling language, which accommodates Graphical User Interface (GU), Command Line Interface (CLI), and Python bindings. This tool easy to use, supports automatic verification, and detects vulnerabilities. - Comparison: Lighter than AVISPA and faster at handling simpler protocols. Figure 4 gives the basic architecture of the Scyther tool.



(a)

Scyther results : autoverify

Claim				Status		Comments	Patterns
Test	W	Test,W2	Secret Cert	Ok		No attacks within bounds.	
		Test,W3	Secret SMS	Ok		No attacks within bounds.	
		Test,W4	Alive	Ok		No attacks within bounds.	
		Test,W5	Weakagree	Ok		No attacks within bounds.	
		Test,W6	Niagree	Ok		No attacks within bounds.	
		Test,W7	Nisynch	Ok		No attacks within bounds.	
	CHS	Test,CHS3	Secret Cert	Ok		No attacks within bounds.	
		Test,CHS4	Secret SMS	Fail	Falsified	At least 1 attack.	1 attack
		Test,CHS5	Alive	Fail	Falsified	At least 1 attack.	1 attack
		Test,CHS6	Weakagree	Fail	Falsified	At least 1 attack.	1 attack
		Test,CHS7	Niagree	Fail	Falsified	At least 1 attack.	1 attack
		Test,CHS8	Nisynch	Fail	Falsified	At least 1 attack.	1 attack

Done.

(b)

Fig. 4. (a) Demonstrates the scyther tool's graphical user interface, (b) shows the parameter in scyther tool.

Nevertheless, Scyther necessitates an exact protocol model. In addition, it is less adaptable compared to tools such as Tamarin or ProVerif deployable for the analysis of intricate characteristics. To verify the protocol's security, the standard approach involves the drafting of the protocol and claims, executing the tool, and evaluating the output [37].

5.4. Automated Validation of Internet Security Protocols and Applications (AVISPA)

This is a fully open-source tool that was developed for automatic assessment of the level of security in internet protocols and applications. Figure 5 shows the basic architecture of AVISPA. Using the Dolev-Yao symbolic attacker model, it simulates security threats such as interception and manipulation of messages. It was developed as part of European project in collaboration with a number of academic and business organizations.

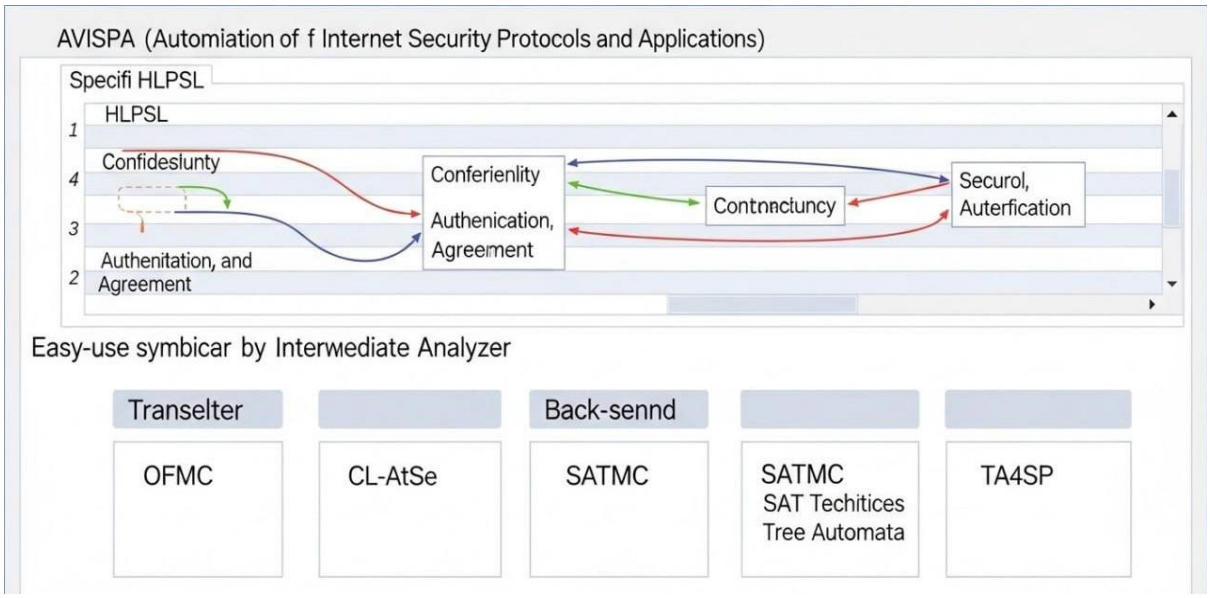


Fig. 5. AVISPA architecture

This tool deploys a sophisticated formal language referred to as High-Level Protocol Specification Language (HLPSL) to specify protocols and security features such as authentication, consensus, synchronization, and secrecy. AVISPA incorporates a graphical user interface that is easy to understand, in addition to a compiler that transforms specifications into a format that is intermediate. The On-the-Fly Model Checker (OFMC), Constraint-Logic-based Attack Searcher(CL-AtSe), SAT-based Model Checker (SATMC), and Tree Automata for Security Protocols (TA4SP) back-ends are all capable of performing accurate evaluation of this format. Symbolic model checking, tree automata, SAT methods, and constraint logic are some of the strategies that these back-ends utilize to discover weaknesses and ensure that the security requirements are not violated. Its ability to quickly and efficiently recognize symbolic attacks is one of the characteristics that separate it from the rest of the tools. Nevertheless, the attack model based on the Dolev-Yao may not be suitable for complicated configurations or advanced security features. In addition, it performs dismally for protocols and applications that are time consuming or mathematically intensive. It supports deeper analysis and assessment of broad threat models. - Comparison: More robust than Scyther but offers broader coverage and more comprehensive analysis [38], [39].

5.5. PROVERIF

This tool operates within the realms of the Dolev–Yao symbolic framework. It is a sophisticated formal verification tool developed for specifically evaluating the security of cryptographic protocols. Here, protocol implementation specifications utilize Horn Clauses within the program. In addition, this tool automates the reasoning during the testing of crucial security properties such as confidentiality, authentication, and data integrity. ProVerif may also analyze co-domains of infinite sizes from protocol traces and vulnerability parsing to discover attack trails in a timely manner. By the use of this feature, developers obtain very important data which is helpful in the discovery and resolving of vulnerabilities within systems. This tool has proved handy in the analysis of numerous cryptographic primitives, such as Diffie-Hellman (DH) key exchange, symmetric or asymmetric encryption, and digital signatures. Figure 6 shows the basic architecture of this tool.

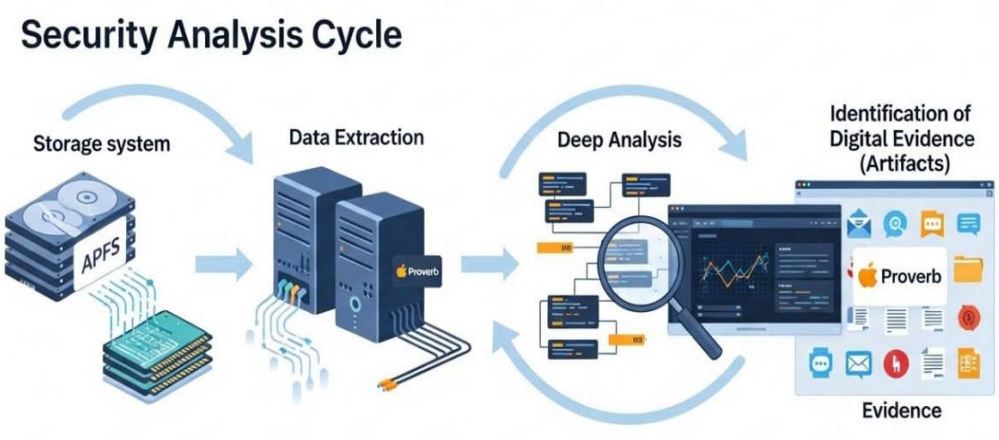


Fig. 6. Pro Verif architecture

On the flipside, the ProVerif analysis disregards any computation errors which the model is permitted to make. In addition, ProVerif may sometimes yield inconclusive findings due to its dependency on approximations or due to the difficulties of recreating complex processes. As such, there is need for exercising great caution during the conversion of symbolic models to actual software implementations [40]. In spite of this, ProVerif is widely acknowledged as a trustworthy and well-established instrument for cryptographic protocol analysis. More powerful than Scyther and AVISPA in terms of capabilities, but more difficult to use.

6. Burrows–Abadi–Needham (BAN) Logic

This is a well-known formal proof technique deployed for the verification of security strength of authentication protocols. Its goal is to reason about the beliefs established among the user (U), the authentication server (AS), and the key distribution center (KDC) during the authentication process [41]. After the KDC verifies the user's multi-factor credentials, it generates a session key (K_{US})and securely delivers it to both the user and the server. This logic transforms the protocol into an idealized collection of abstract messages utilizable for reasoning at higher levels. The goal of the BAN model is that:
(1) AS and U believe they share K_{US}.
(2) During mutual authentication, session K_{US} is fresh.
(3) The communicating parties assume that session key K_{US} is not easily guessed and was generated by a trusted authority (KDC) . Another assumption is that the KDC can create a session keys that all parties depend on to keep their long-term keys (K_U for users and $K_S$for servers) safe. During the BAN logic analysis, three inference rules (message meaning, nonce verification, and jurisdiction) are applied sequentially (KDC) [42]. The details of these rules are described below.

$$U \mid \mid \equiv (U \leftrightarrow_{K_{US}} AS), AS \mid \mid \equiv (U \leftrightarrow_{K_{US}} AS)$$

indicating a shared belief in the new and authentic session key.
Both U and AS believe that shared key K_{US} which has been safely distributed by the KDC, is a fresh (that is, $\#K_{US}$). This further confirms the existence of effective mutual authentication. This is then deployed to demonstrate that the authentication protocols achieve authenticity, confidentiality and trust between communicating entities. The integration of MFA increases resistance to replay attacks as well as credential theft [41-43].

BAN logic core rules

1. Message-Meaning Rule (MMR):

$$\frac{P \mid \equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P \mid \equiv Q \mid \equiv X} \quad (1)$$

2. Nonce-Verification Rule (NVR):

$$\frac{P \mid \equiv \#(X),\ P \mid\equiv Q \mid \sim X}{P \mid\equiv Q \mid \equiv X} \tag{2}$$

3. Jurisdiction Rule (JR):

$$\frac{P \mid\equiv Q\mid \Rightarrow X,\ P \mid\equiv Q \mid\equiv X}{P \mid\equiv X} \tag{3}$$

4. Freshness Rule (FR):

$$\frac{P\mid \equiv \#(X)}{P\mid \equiv \#(X,Y)} \tag{4}$$

5. Belief Rule (BR):

$$\frac{P\mid\equiv Q\mid \equiv X}{P\mid \equiv (X)} \tag{5}$$

7. Conclusion

This study has shown that contemporary learning establishments are exposed to a myriad of security threats such as unauthorised access, data breach, MITM, phishing, and denial-of-service attacks. Therefore, these institutions need to implement robust procedures and techniques to defend against these security issues. A sound security system should also preserve security properties such as mutual authentication, data integrity, and privacy. In this paper, we have presented recent authentication techniques as well as other security techniques applicable in the educational sector. We have provided detailed descriptions of the various required security features within the e-learning environment, all of which are required for the proper functioning of these systems. The findings of this study showed that the most appropriate defense against unauthorized access is to permit access based on the role of the entity in the educational system. For instance, since most of the information required by students is restricted to grades and learning materials, they should only need single-factor authentication. This is majorly because their access tends to be publicly limited. Consequently, any successful compromise at this level cannot affect the overall system security. Basically, permissions accorded to entities should not exceed their correlated significance and role in the system. In terms of authentication, it is recommended that educational systems implement authentication methods that have been shown to be resilient against several attacks. In addition the deployed security techniques should have demonstrated salient security properties. Moreover these security solutions should seamlessly interoperate with new technologies such as cloud and fog computing, blockchain and next generation private networks (5G or 6G). For effective administrative support any proposed authentication or access control mechanisms should be subjected to approval from heads of the various departments. To ensure robust security assurances each of these security techniques should be exposed to formal and informal security analysis employing tools such as ProVerif, AVISPA and BAN Logic.

References

[1] M. S. Jayawardhena and P. Foley, “Changes in the banking sector: The case of Internet banking in the UK,” *International Journal of Bank Marketing*, vol. 18, no. 4, pp. 160–170, 2000.

[2] W. Webb, “The evolution of telecommunication systems,” *IEEE Communications Magazine*, vol. 43, no. 10, pp. 60–65, Oct. 2005.

[3] D. Blumenthal and M. Tavenner, “Health information technology in the United States: Where we stand and where we are going,” *New England Journal of Medicine*, vol. 362, no. 14, pp. 1323–1326, Apr. 2010.

[4] C. Jacomme, S. Kremer, and S. K. An, “Extensive formal analysis of multi-factor authentication protocols,” *ACM Transactions on Privacy and Security*, vol. 24, no. 2, 2021, DOI: 10.1145/3440712.

[5] I. Cahyanto, H. Madihah, I. Budiarso, A. Sutrisno, and T. Hidayat, "Effectiveness of multifactor authentication technology for protecting student privacy: A systematic literature review," *Edum Journal*, vol. 7, no. 2, pp. 253–269, Jan. 2025, DOI: 10.31943/edumjournal.v7i2.286.
[6] A. Boldyreva, Z. Gui, and B. Warinschi, "Understanding leakage in searchable encryption: A quantitative approach," *Proceedings on Privacy Enhancing Technologies*, vol. 2024, no. 4, pp. 503–524, Oct. 2024, DOI: 10.56553/popets-2024-0127.
[7] S. G. Lyastani, M. Backes, and S. Bugiel, "A systematic study of the consistency of two-factor authentication user journeys on top-ranked websites," in *Proc. NDSS*, San Diego, CA, USA, 2023, DOI: 10.14722/ndss.2023.23362.
[8] W. Kennedy and A. Olmsted, "Three factor authentication," in *Proc. 12th Int. Conf. Internet Technology and Secured Transactions (ICITST)*, Cambridge, UK, 2018, pp. 212–213, DOI: 10.23919/ICITST.2017.8356384.
[9] M. K. Kabier, A. A. Yassin, and Z. A. Abduljabbar, "Towards designing educational systems using role-based access control," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 2, pp. 50–63, 2023, DOI: 10.22266/ijies2023.0430.05.
[10] A. H. Y. Mohammed, R. A. Dziyauddin, and L. A. Latiff, "Current multi-factor authentication: Approaches, requirements, attacks and challenges," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, 2023. [Online]. Available: https://www.ijacsa.thesai.org
[11] M. A. Syahreen, N. Hafizah, N. Maarop, and M. Maslinan, "A systematic review on multi-factor authentication framework," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 5, 2024, DOI: 10.14569/IJACSA.2024.01505105.
[12] B. M. Elomda, T. A. A. Abdelbary, H. A. Hassan, K. S. Hamza, and Q. Kharma, "An enhanced multi-layer blockchain security model for improved latency and scalability," *Information*, vol. 16, no. 3, Mar. 2025, DOI: 10.3390/info16030241.
[13] R. Raimundo and A. Rosário, "Blockchain system in higher education," *European Journal of Investigation in Health, Psychology and Education*, vol. 11, no. 1, pp. 276–293, 2021, DOI: 10.3390/ejihpe11010021.
[14] J. G. Chamani, D. Papadopoulos, M. Karbasforushan, S. Cruz, and I. Demertzis, "Dynamic searchable encryption with optimal search in the presence of deletions," in *Proc. USENIX Security Symposium*, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/chamani
[15] L. Yan et al., "Attribute-based searchable encryption: A survey," *Electronics*, vol. 13, no. 9, 2024, DOI: 10.3390/electronics13091621.
[16] S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A systematic survey of multi-factor authentication for cloud infrastructure," *Future Internet*, vol. 15, no. 4, Apr. 2023, DOI: 10.3390/fi15040146.
[17] I. Amorim and I. Costa, "Homomorphic encryption: An analysis of its applications in searchable encryption," *Mathematics*, vol. 11, no. 13, 2023, DOI: 10.3390/math11132948.
[18] A. S. Balobaid, Y. H. Alagrash, A. H. Fadel, and J. N. Hasoon, "Modeling of blockchain with encryption-based secure education record management system," *Egyptian Informatics Journal*, vol. 24, no. 4, 2023, DOI: 10.1016/j.eij.2023.100411.
[19] S. Khan, H. Abbas, and M. Binsawad, "Secure semantic search using deep learning in a blockchain-assisted multi-user setting," *Journal of Cloud Computing*, vol. 13, no. 1, 2024, DOI: 10.1186/s13677-023-00578-5.
[20] I. Wanisha et al., "Multi-factor authentication using blockchain: Enhancing privacy, security and usability," *International Journal of Computer Technology and Science*, vol. 1, no. 3, pp. 41–55, 2024, DOI: 10.62951/ijcts.v1i3.24.
[21] S. Narkedimilli, A. V. Sriram, and S. Raghav, "FL-DABE-BC: A privacy-enhanced decentralized authentication framework for IoT scenarios," arXiv:2410.20259, 2024.
[22] N. Apthorpe et al., "Measuring NIST authentication standards compliance by higher education institutions," in *Proc. SOUPS*, 2025, pp. 335–350, DOI: 10.48550/arXiv.2409.00546.
[23] A. Braeken, "Highly efficient symmetric key-based authentication and key agreement protocol using Keccak," *Sensors*, vol. 20, no. 8, 2020, DOI: 10.3390/s20082160.
[24] M. Ramadan, G. Du, F. Li, and C. Xu, "A survey of public key infrastructure-based security for mobile communication systems," *Symmetry*, vol. 8, no. 9, 2016, DOI: 10.3390/sym8090085.

[25] F. M. Salem et al., "AMAKAS: Anonymous mutual authentication and key agreement scheme for multi-server environments," *Journal of Cloud Computing*, vol. 12, no. 1, 2023, DOI: 10.1186/s13677-023-00499-3.
[26] U. E. Chinanu and O. Amujo, "Comparative survey of cyber-threat and attack trends," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 6, 2018.
[27] A. O. de Sá et al., "Intelligent attacks on cyber-physical systems and critical infrastructures," 2024, DOI: 10.3233/NICSP240033.
[28] S. Gao et al., "A robust and efficient authentication and key agreement for UAV-assisted AGS communication," *Journal of King Saud University – Computer and Information Sciences*, vol. 37, no. 6, 2025, DOI: 10.1007/s44443-025-00151-x.
[29] H. S. Lallie et al., "Analysing cyber attacks and cyber security vulnerabilities in the university sector," *Computers*, vol. 14, no. 2, p. 49, 2025, DOI: 10.3390/computers14020049.
[30] A. el Koshiry et al., "Unlocking the power of blockchain in education," *Blockchain: Research and Applications*, vol. 4, no. 4, Dec. 2023, DOI: 10.1016/j.bcra.2023.100165.
[31] C. McCabe, A. I. C. Mohideen, and R. Singh, "A blockchain-based authentication mechanism," *Sensors*, vol. 24, no. 17, Sep. 2024, DOI: 10.3390/s24175830.
[32] V. R. Kebande et al., "A blockchain-based multi-factor authentication model for cloud-enabled IoV," *Sensors*, vol. 21, no. 18, Sep. 2021, DOI: 10.3390/s21186018.
[33] O. A. Khashan et al., "Blockchain-based decentralized authentication model for IoT-based e-learning," *Computers, Materials and Continua*, vol. 75, no. 2, pp. 3133–3158, 2023, DOI: 10.32604/cmc.2023.036217.
[34] M. Al-Hemairy et al., "Blockchain-based framework for academic certification validation," *Education and Information Technologies*, vol. 29, no. 14, pp. 18203–18232, Oct. 2024, DOI: 10.1007/s10639-024-12493-6.
[35] G. S. Cho, Y. H. Kim, and S. Y. Lee, "Design and implementation of APFS object identification tool," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 32, no. 5, pp. 1049–1062, 2022, DOI: 10.13089/JKIISC.2022.32.5.1049.
[36] C. J. F. Cremers, *Scyther: Unbounded Verification of Security Protocols*, ETH Zurich, Tech. Rep. 572, 2011, DOI: 10.3929/ethz-a-006809966.
[37] A. Armando et al., "The AVISPA tool for the automated validation of Internet security protocols," *LNCS*, vol. 3576, 2005. [Online]. Available: http://www.avispa-project.org
[38] C. Hummert and D. Pawlaszczyk, *Mobile Forensics: The File Format Handbook*, Springer, 2022, DOI: 10.1007/978-3-030-98467-0.
[39] B. Blanchet et al., "ProVerif 2.00: Automatic cryptographic protocol verifier," *User Manual*, 2018. [Online]. Available: https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf
[40] T. Arpitha, D. Chouhan, and J. Shreyas, "Anonymous and robust biometric authentication for social IoT healthcare," *Journal of Engineering and Applied Science*, vol. 71, no. 1, 2024, DOI: 10.1186/s44147-023-00342-1.
[41] A. Li et al., "Analysis and improvement on an authentication scheme for WSNs in IoT," *Wuhan University Journal of Natural Sciences*, vol. 28, no. 6, pp. 541–552, 2023, DOI: 10.1051/wujns/2023286541.
[42] H. Park et al., "Provably quantum secure three-party mutual authentication," *Electronics*, vol. 13, no. 19, 2024, DOI: 10.3390/electronics13193930.
[43] M. Saqib and A. H. Moon, "Design of a three-factor authentication and key agreement scheme using biometrics for IoT," Research Square, 2024, DOI: 10.21203/rs.3.rs-4181532/v1.

Journal of Basrah Researches (Sciences) **52**(1), 14 (2026)
DOI: https://doi.org/10.56714/bjrs.52.1.2

دراسة متعمقة لدور المصادقة متعددة العوامل في أنظمة التعلم الإلكتروني: الأدوات والمخططات البدائية

دعاء عاشور سلطان*، علي عادل ياسين،

جامعة البصرة كلية التربية للعلوم الصرفة /قسم علوم الحاسوب.

معلومات البحث

الاستلام	13 تشرين ثاني 2025
المراجعة	04 كانون ثاني 2026
القبول	07 كانون ثاني 2026
النشر	30 حزيران 2026

الكلمات المفتاحية

بلوك تشين، التحكم في الوصول على أساس الأدوار، المصادقة متعددة العوامل، المصادقة، الأنظمة التعليمية.

Citation: D. A. Sultan, A. A. Yassin., J. Basrah Res. (Sci.) **52**(1), 14 (2026). DOI:https://doi.org/10.56714/bjrs.52.1.2

الملخص

أحدثت التكنولوجيا الحديثة ثورة في جميع مجالات الحياة البشرية، بما في ذلك أنظمة التعليم. وبخلاف أساليب التدريس التقليدية في الفصول الدراسية، فإن بيئات التعلم الإلكتروني الحالية تتفوق بسرعة على الأشكال التقليدية للتدريب المدرسي. ويتم تحقيق ذلك عادةً من خلال منصات قوية مصممة لتعزيز أنظمة اكتساب المهارات والمشاركة المستمرة في التعلم. وهذا يساعد في تحقيق التعلم التفاعلي والشخصي للطلاب في أي مكان وزمان. يتوافق التعلم الإلكتروني مع تقنية الحوسبة السحابية ويدعمها بشكل كامل، مما يساعد في مزامنة جميع العمليات التشغيلية. ومع ذلك، فإن هذه التطورات التكنولوجية تؤدي إلى تحديات كبيرة مثل عدم أمان البيانات. تتمحور القضايا الرئيسية حول ضمان بقاء المعلومات الحساسة والشخصية للطلاب والمتدربين آمنة من الوصول غير المصرح به. يبدو أن الشاغل الأكثر أهمية هو عدم كفاية الأمان الذي توفره آليات التحكم في الوصول إلى البيانات في هذه الأنظمة. في هذا الصدد، أصبح التحكم في الوصول على أساس الدور (RBAC) بارزًا جدًا في بناء أنظمة حوسبة آمنة مؤخرًا. يمنح RBAC ويمنع وصول الأفراد إلى معلومات أنظمة الحوسبة بناءً على أدوارهم ومسؤولياتهم. على مر السنين، تم تطوير العديد من حلول الأمان الأخرى، بدءًا من بروتوكولات الأمان المشتركة والمصادقة أحادية العامل إلى المصادقة متعددة العوامل. تم تنفيذ هذه التقنيات الأمنية من خلال طبقات متعددة

***Corresponding author email:** duaa.ashoor@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq