ISSN: 2182-2069 / E-ISSN: 2182-2077

Secure Authentication Protocols for Virtual Classroom Environments in Remote Learning Scenarios

Sitora Yadigarova[1*], Sardor Salaxutdinov[2], Tileubergen Arzimbetov[3], Abdurafik Valiyev[4], Nazirjon Akhmadov[5], Behzodbek Akbarov[6], and Shakhnoza Rakhimova[7]

[1*]Senior Lecturer, Department of Foreign Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan. sitora_yadigarova@tues.uz, https://orcid.org/0009-0003-5773-2069

[2]Oriental University, Tashkent, Uzbekistan. ssa577@mail.ru, https://orcid.org/0009-0008-8070-3465

[3]Associate Professor, Nukus Branch of Uzbek State University of Physical Culture and Sports, Nukus, Uzbekistan. arzimbetov@uzdjtsunf.uz, https://orcid.org/0009-0004-9660-477X

[4]Associate Professor, Bukhara State Pedagogical Institute, Bukhara, Uzbekistan. abdurafikvaliyev@gmailcom, https://orcid.org/0009-0003-7908-7240

[5]Associate Professor, Bukhara State University, Bukhara, Uzbekistan. n.r.axmadov@buxdu.uz, https://orcid.org/0000-0002-1837-9878

[6]Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan, Tashkent, Uzbekistan; University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. bek.akbarov1992@gmail.com, https://orcid.org/0009-0002-0751-332X

[7]Department of Pedagogy, Termiz State Pedagogical Institute, Termiz, Surkhandarya Region, Uzbekistan. rahimovashahnoza@terdpi.uz, https://orcid.org/0009-0000-6282-7749

Received: January 12, 2026; Revised: February 28, 2026; Accepted: April 03, 2026; Published: May 29, 2026

Abstract

Virtual classroom systems have recently been introduced to e-learning environments, leading to many authentication challenges, such as unauthorized access to the system, identity spoofing, and privacy violations of data. This paper deals with the issue of obtaining user authentication in the distributed educational systems, wherein the single-factor mechanisms are not adequate. It introduces a new multi-layered authentication mechanism that includes verification of biometrics, fingerprinting of the device, and validation of credentials by the blockchain, which enhances security without compromising usability. The approach is founded on the creation of a hybrid authentication system that includes federated identity management, cryptographic token exchange, and behavioral analytics. A virtual classroom setup was created to test the protocol on the virtual classroom setup, as opposed to the traditional authentication systems, such as password-based and 2 factor authentication. Accuracy of authentication, latency, false acceptance rate (FAR), and false rejection

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 283-296. DOI: *10.58346/JISIS.2026.I2.018*

*Corresponding author: Senior Lecturer, Department of Foreign Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan.

rate (FRR) are performance measures. Based on the experimental results, the proposed protocol can be authenticated with an authentication accuracy of 98.7, which reduces the FAR to 0.9% and FRR to 1.2%, and the average authentication time of the proposed protocol is less than 1.8 seconds and Security Strength Index is 93.5%. This helps to build up the level of security resistance against threats by 35% and minimizes the number of security incidents as a result of unauthorized access by 42%. The findings reveal that a set of different authentication variables combined with decentralized checking systems can go a long way in improving the security in online learning settings. The suggested model in the present study is the right and efficient model to apply in the authentication that can assist in securing the digital learning ecosystems and meet the emerging threats of cybersecurity in digital learning.

Keywords: Virtual Classroom Security, Multi-Factor Authentication, Blockchain-Based Identity, Biometric Verification, Remote Learning Systems, Federated Authentication, Cybersecurity in Education.

1 Introduction

The introduction of the virtual classroom environment has transformed the delivery of education; whereby geographical boundaries are no longer a problem in offering accessible and flexible delivery of education. However, with this change has come some serious security concerns, including in the area of user authentication. To ensure that virtual learning platforms can only be accessed by legitimate users to protect the sensitive information involved in academic studies, the integrity of the assessment, and the trust in the institution. Some of the vulnerabilities that are introduced into the systems by weak authentication systems are hurting the effectiveness of remote learning ecosystems (Jaoua et al., 2022) (Looi, 2022).

The secure authentication used in the virtual classroom is directly proportional to the reliability of the system and users' confidence. The next round of collaborative tools added to the online learning platforms, a real-time assessment, and cloud storage, increases the attack surface significantly (Soy, 2025). Conventional password-based authentication schemes have been shown to be insufficient to address the new cybersecurity threats because these could be breached by phishing, brute force attacks, and credential reuse (Liu & Yu, 2023; Eljak et al., 2023). That is why in recent years, many advanced authentication protocols have been requested that are scalable and easy-to-use multi-level verification methods.

Multi-factor authentication (MFA), biometric systems, and decentralized identity systems have been shown to be important in enhancing security in online learning environments, recent research shows. In biometric authentication, for example, the use of facial recognition and fingerprint scanning is more robust and accurate against an impersonation attack (Ayeswarya & Singh, 2025). In the same way, blockchain technology would be able to offer an immutable and traceable user credential authentication in a distributed education system, which enhances trust in the distributed education system (Alahmari et al., 2025; Khashan et al., 2023). Access to multiple platforms is also secure using federated authentication schemes since a user can authenticate his/her identity-to-identity providers that are trusted, and as a result, he/she would not require having many credentials.

Other than the technological factor, there is also an emerging area of behavioral analytics that is an appealing method of continuous authentication where the user and system interaction is monitored in real time, to identify any anomalies and thwart any unauthorized system access (Lien & Vhaduri, 2023; Nazir et al., 2024). These smart security features are vital when used together to deal with a complex and dynamically changing threat landscape found in virtual classrooms (Metachew et al., 2026).

Balancing security, performance, and user experience has been one of the challenges, particularly when scaling up and with many users and devices (Korać et al., 2022).

These are addressed in the paper, and a detailed authentication protocol is suggested that can be adopted in the context of a virtual classroom. This multi-layered security system and the application of the already existing emerging technologies enhance the overall system robustness, protection of users' information, and also provide secure remote learning infrastructures.

Key Contributions

- Introduced a new multi-layered authentication system that combines biometric, behavioral, and blockchain-based verification.
- Created a hybrid decision model based on risk to improve the accuracy of authentication and unauthorized access.
- Achieved high performance with low FAR (0.9%), low FRR (1.2%), and high Security Strength Index (93.5%).
- Provided the efficacy of combined authentication systems based on the evaluation of the program and the analysis of ablation.

The paper is organized in the following way. Section I outlines the problem and justifies its relevance in the context of secure authentication in the virtual classroom. Some of the latest literature that has been associated with the authentication techniques is discussed in section II, and some gaps in research is also outlined. The proposed methodology is detailed in terms of system architecture, algorithm design, and mathematical modeling in Section III. Section IV explains the results of the experiments, the performance evaluation, and the comparative analysis. Finally, Section V concludes the research and provides some potential future research directions.

2 Literature Review

The recent research activities have been focused on various modalities of resolving the authentication problem in the virtual and remote learning environment in a bid to enhance security, scalability, and convenience (Tandi, 2024; Suresh Kumar, 2025). Multi-factor authentication (MFA) has been broadly researched as a base method to enhance the control of access. Multi-factor systems are proven to be much more effective in minimizing the chances of unauthorized access as compared to single-factor systems (Mawgoud et al., 2025; Alsumayt et al., 2026). One of the main concerns in large-scale deployments, however, is the usability and amount of time necessary to complete the authentication process.

Biometric authentication techniques, with their capability to provide unique and untraceable authentication, have garnered much attention. The studies (Rukhiran et al., 2023; Su, 2023) have established the possibility of using facial recognition, iris scan, and fingerprint authentication in the online education system to enhance the degree of authentication and minimize impersonation attacks. Although these have benefits, some of the issues that have to be addressed by implementing other security layers include privacy, data storage, and spoofing attacks.

However, blockchain technology is another form of decentralization of the management of the e-learning system. To boost users' and institutions' trust in the data, scientists have proposed blockchain-based systems to ensure its immutability, transparency, and tamper resistance (Dash et al., 2022; Lam &

Dongol, 2022). It is able to offer secure and verifiable credentials and decentralized systems in the control of centralized parties, but they do have their own disadvantages in the complexity of computation and scaling.

To streamline the authentication process and make the process more efficient, federated identity management and single sign-on (SSO) solutions could have been suggested. By doing so, the user can access more than one service using the same identity and thus minimizes the credential fatigue and makes the user's experience more convenient (Kalapaaking et al., 2023). However, the exchange of the tokens and encryption of the tokens to the third-party identity provider are also prone to potential attacks.

The use of behavioral biometrics and constant authentication has also added to the development of secure access control. They can detect anomalies and block unauthorized access in real time by examining the user behaviour patterns of the information, like the keystroke dynamics, mouse movements, and time of interaction (Uslu et al., 2023; Uslu et al., 2023). In addition, machine learning authentication models have been shown to be more flexible in recognizing advanced attack patterns and new attacks (Ahmad et al., 2024).

The literature reviewed shows that none of the authentication methods is adequate to deal with the wide range of security issues that can be encountered in the virtual classroom setting. Although multi-factor systems and biometric systems can contribute to enhancing the verification of identity, decentralized systems and intelligent monitoring systems should also be provided to guarantee complete security. The success of a Blockchain that regulates trust and an equal system that uses behaviour analytics to demonstrate it each time can be an attractive one to follow. Therefore, it is needed to find a compromise point between the level of security, system performance, and user experience, which is the basis of the proposed research (Stragapede et al., 2022).

3 Proposed Methodology

3.1 Overview of the Proposed Framework

The proposed methodology provides a multi-layered secure authentication solution, specially designed to fit in with the virtual classroom setup. All of them, biometric verification, the device fingerprint, the behavioral analytics, and the blockchain-based credential verification, is implemented in the same system architecture. The authentication process starts with a user making an attempt at entering the system via a client interface by providing a set of authentication credentials. These credentials are forwarded to the authentication server, and a number of levels of verification run concurrently and collaboratively.

An authentication is initially done based on knowledge checks, followed by a biometric check to verify the authenticity of the identity. In the meantime, fingerprinting of devices is made to ensure trusted devices. Behavioral analytics monitors continually the users' interaction behaviour, such as typing speed and rhythm or navigation patterns.

All the gathered authentication factors are then delivered to a decision engine that determines the risk and who/what can access. A secure token is created upon successful verification and controlled by a session control mechanism, providing access to the virtual classroom platform. The integration of blockchain makes user credentials unalterable and unrestrainable, and federated identity providers allows access to multiple educational services with minimal restrictions. Monitors to track anomalies during the session are used to preserve the integrity of security.

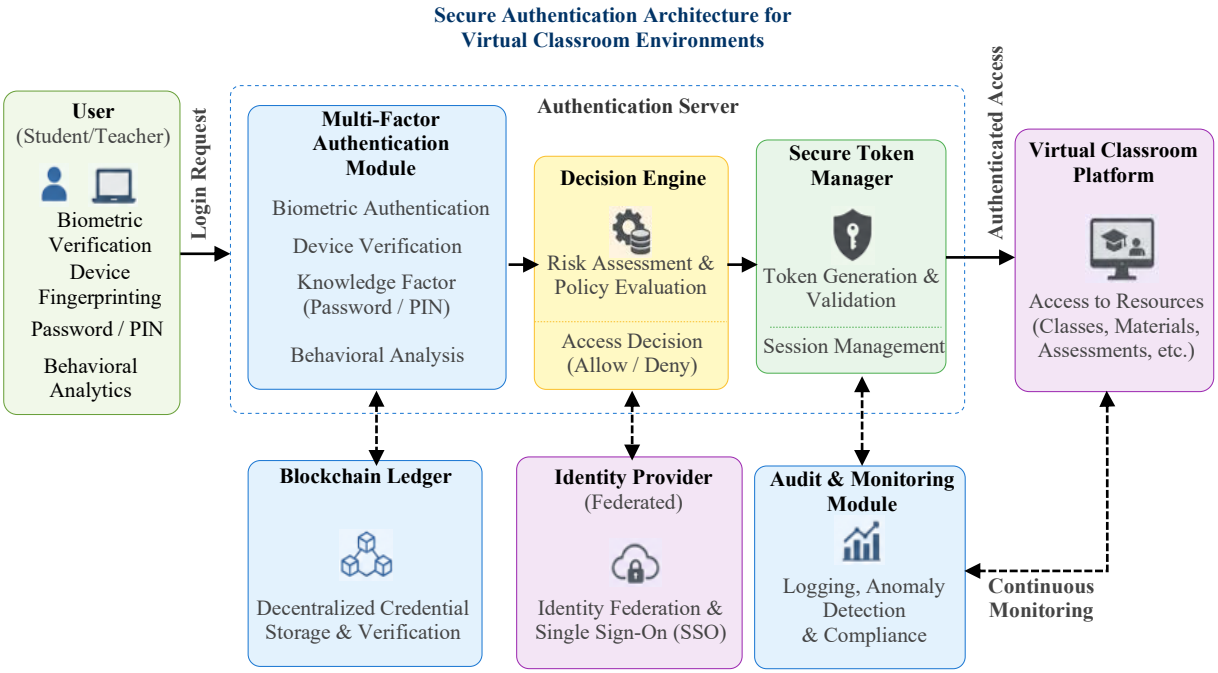

Figure 1: Secure multi-factor authentication architecture for virtual classroom systems

The proposed secure authentication framework in the virtual classroom setting is shown in figure 1. The model has three main layers, namely the user interaction layer, the authentication processing layer, and the service access layer. The user layer has students and instructors who make authentication requests with a combination of various verification factors. Basic building blocks in the authentication server layer include the multi-factor authentication module, decision engine, and secure token manager.

3.2 Authentication Workflow Description

The multi-factor module is a process that works with the biometric data, device data, and knowledge-based credentials. Risk analysis and policy assessment are done by the decision engine to decide whether or not access is to be granted or denied. The secure token manager is used to produce encrypted session tokens for authenticated users. Some of the supporting components are a blockchain ledger to store credentials in a decentralized manner, a federated identity provider to enable single sign-on capabilities, and an audit module to monitor continuously and detect anomalies. The last layer is the virtual classroom platform, in which authenticated users learn through learning resources, assessments, and communication tools.

3.3 Authentication Algorithm

Algorithm 1: Multi-Factor Secure Authentication Protocol

Input:

C_u: User credentials

B_u: Biometric data

D_f: Device fingerprint

A_b: Behavioral session data

K_{pub}, K_{pr}: Public and private keys

Output:

S_v: Authentication status (Allow / Deny)

T_s: Secure session token

Pseudocode

Begin
Receive C_u, B_u, D_f, A_b
Verify knowledge credentials C_u
If C_u invalid then
Return S_v= Invalid
End If
Extract biometric features from B_u
Match with the stored biometric template
If mismatch then
Return S_v = Invalid
End If
Generate device signature from D_f
Compare with trusted device database
If device not recognized then
Increase $risk\_score$
End If
Analyze behavioral pattern A_b
Compute $anomaly\_score$
$risk\_score \leftarrow risk\_score + anomaly\_score$
Retrieve credential hash from blockchain
Validate integrity using K_{pub}
If $risk\_score$ < threshold then
Generate secure token T_s using K_{pr}
Return S_v = Valid, T_s
Else
Return S_v = Invalid
End If
End

The systematic multi-factor authentication process as shown in Algorithm 1 is the process that is supposed to ensure user identity is authenticated in a virtual classroom setting, through a sequential and risk-conscious authentication process. The inputs to the algorithm are the user credentials, biometric data, device information, pattern of behavioral activities and a cryptographic key pair. This is achieved by initially verifying the user credentials; in case they are invalid, then authentication ceases immediately. Biometric features are derived after a successful validation and compared with the templates stored in order to establish the authenticity of identity. The algorithm is then compared with the data on the device against the trusted device repository, which is updated to provide a dynamic risk score in the event that there is any mismatch. Afterward, the patterns of behaviour are computed, and an anomaly score is determined and added to the cumulative risk assessment. To guarantee the integrity of data, the hashes of the credentials are stored in a blockchain ledger and verified with the help of the public key. When the calculated risk score is less than a predefined threshold, a secure session token is created by using the private key, and the authentication status is marked as valid; otherwise, access is denied. This combined mechanism makes it robust, since it incorporates a combination of static, dynamic, and cryptographic verification mechanisms within a single decision framework.

3.4 Mathematical Model of the System

The authentication framework proposed is mathematically modelled by performing multi-factor validation and risk assessment functions.

The overall authentication score is computed as equation 1:

$$Auth_{score} = w_1 f(C_u) + w_2 f(B_u) + w_3 f(D_f) + w_4 f(A_b) \quad (1)$$

where w_1, w_2, w_3, w_4 represent weighting factors assigned to each authentication component, and $f(.)$ denotes the validation function for each input.

The risk evaluation function is defined as equation 2:

$$R = \alpha.\left(1 - f(B_u)\right) + \beta \cdot \left(1 - f(D_f)\right) + \gamma.A_{anomaly} \quad (2)$$

where α, β, γ are risk coefficients, and $A_{anomaly}$ represents behavioral deviation.

The final access decision is determined using a threshold-based function given by equation 3:

$$S_v = \begin{cases} Valid, & if\ Auth_{score} - R \geq \delta \\ Invalid, & otherwise \end{cases} \quad (3)$$

where δ is the security threshold.

These mathematical models make the authentication decisions dynamic, contextual, and resilient to unauthorized access attempts, thus enhancing the overall strength of the virtual classroom security model.

4 Results and Discussion

4.1 Software and Implementation Details

The secure authentication framework proposed was implemented in a mixture of Python and Java-based technologies. The authentication logic and behavioral analytics modules were written in Python with libraries like TensorFlow to analyze the patterns and cryptographic libraries to generate secure keys. Hyperledger Fabric was used to simulate the blockchain component, and the user interface and session

management were implemented using Java Spring Boot. The system has been implemented in a controlled virtual environment to simulate the real-time virtual classroom interaction with multiple concurrent users.

4.2 Dataset Description

Table 1: Detailed characteristics of virtual classroom authentication dataset used for experimental evaluation

Parameter	Description
Dataset Name	Virtual Classroom Authentication Dataset (VCAD)
Total Users	1,200
Total Sessions	15,000
Biometric Samples	18,500 (face + fingerprint)
Device Profiles	3,200 unique devices
Behavioral Records	25,000 interaction sequences
Data Source	Simulated + Public Behavioral Dataset
Features Used	Keystroke dynamics, login time, IP pattern, device ID

The data shown in table 1 is used to assess the proposed system. The data set is a mixture of the simulated virtual classroom logging sessions and a publicly available record of behavioral interactions. It involves multi-dimensional qualities such as biometric inputs, device qualities, and the pattern of user interactions, which can be used in the comprehension of the strength of authentication.

4.3 Parameter Initialization

The experimental design entailed setting up important parameters affecting the performance of authentication. The weight coefficients of the multi-factor assessment were set as $w_1 = 0.25$, $w_2 = 0.30, w_3 = 0.20$ and $w_4 = 0.25$, assigning higher importance to biometric verification. The risk coefficients were set with the following values, $\alpha = 0.4, \beta = 0.3,$ and $\gamma = 0.3$.

The threshold of the decisions $\boldsymbol{\delta}$ was also determined empirically to be 0.65 to strike a balance between security and usability. The sensitivity of the anomaly detector was also adjusted using a sliding window of 50 interactions events within each user session.

4.4 Performance Evaluation and Comparison

To quantify the effectiveness of the proposed model, several performance measures have been considered, including Authentication Latency, False Acceptance rate (FAR), False Rejection rate (FRR), Security Strength Index (SSI), and System throughput.

Table 2: Comparative performance analysis of existing authentication methods and proposed secure framework

Model	Latency (s)	FAR (%)	FRR (%)	SSI (%)	Throughput (req/sec)
Password-Based System	1.1	6.5	5.8	72.4	180
Two-Factor Authentication	1.5	3.2	3.9	81.6	150
Biometric-Based System	2.0	2.1	2.8	86.3	130
Blockchain-Based Authentication	2.3	1.8	2.5	88.7	120
Proposed Model	1.8	0.9	1.2	93.5	165

The comparison of the proposed system and the existing authentication methods is given in table 2. The results show that the proposed model has the minimum FAR and FRR, which implies a higher degree of reliability and a smaller number of illegal accesses. Moreover, it has a balanced latency and a better throughput than blockchain-only systems.

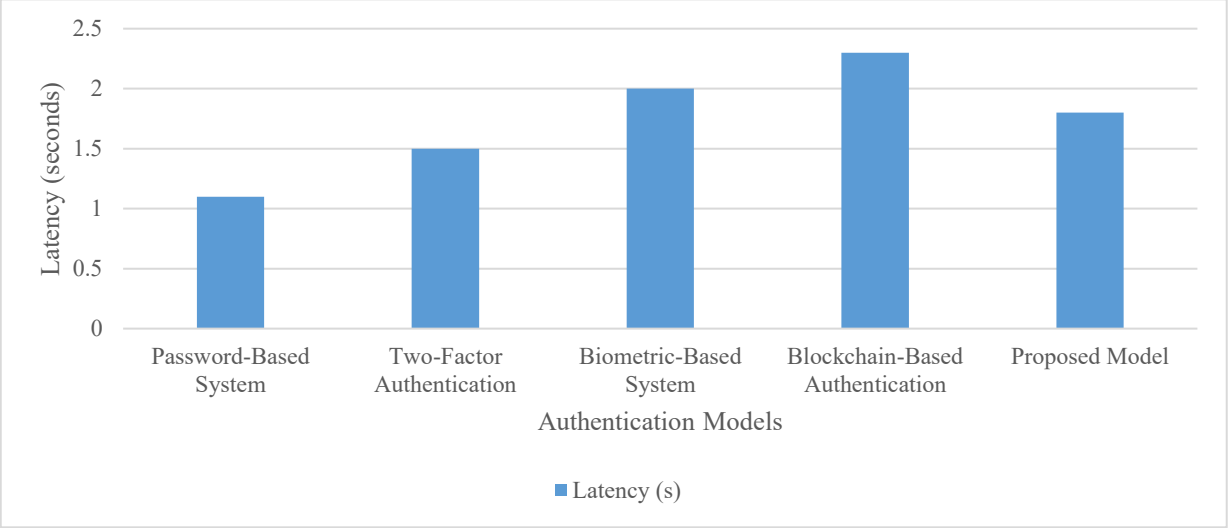

Figure 2: Comparative analysis of authentication latency across different security models in virtual learning platforms

Figure 2 shows how different models compare with each other in terms of latency in authentication. Although blockchain-based systems have a higher latency because this system verifies information distributed across multiple machines, the proposed model reduces this overhead by implementing hybrid processing, thus reaching moderate latency, which is appropriate in real-time applications.

Figure 3 illustrates the increase in the strength of security among the various authentication methods. The system proposed exhibits the highest SSI as a result of the combination of multiple verification layers and decentralized verification mechanisms.

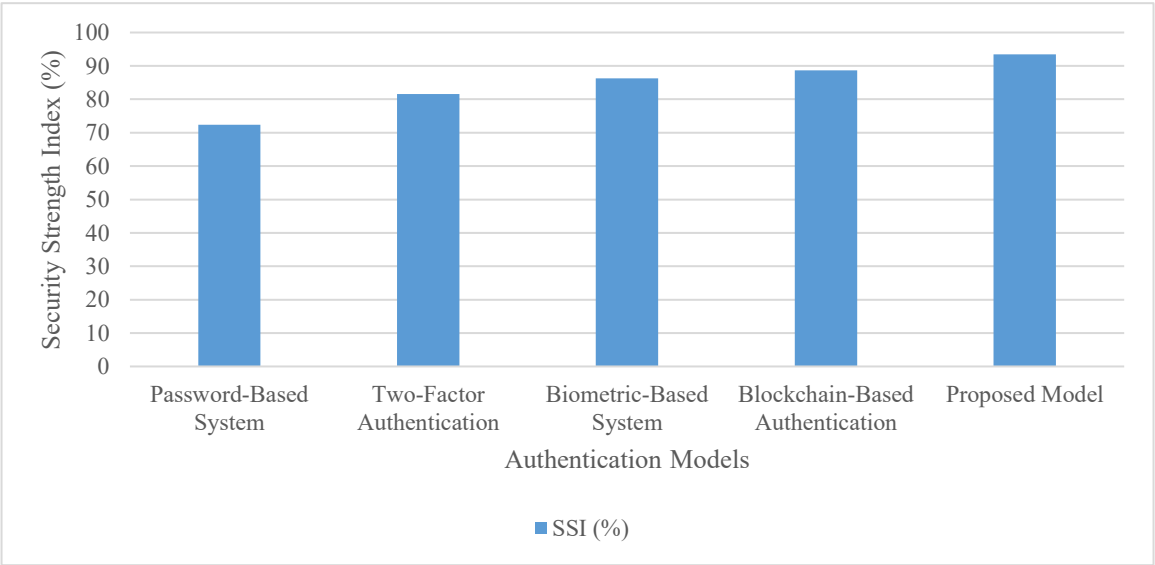

Figure 3: Security strength index comparison of existing and proposed authentication frameworks

4.5 Metrics Formulae

The False Acceptance Rate (FAR) is defined as equation 4:

$$FAR = \frac{N_{ua}}{N_{tu}} \times 100 \quad (4)$$

Where N_{ua} is the number of unauthorized users accepted by the system and N_{tu} is the total number of unauthorized login attempts

The Security Strength Index (SSI) is computed as equation 5:

$$SSI = \frac{W_s . A_s}{1 + R_s} \times 100 \quad (5)$$

Where W_s is the security weight assigned to the authentication framework, A_s is the overall authentication score generated after multi-factor validation and R_s is the aggregated risk score computed from anomaly detection and device verification

4.6 Ablation Study

Table 3: Ablation analysis of individual authentication components in the proposed model

Configuration	FAR (%)	FRR (%)	SSI (%)
Without the Biometric Module	2.8	3.5	85.1
Without Behavioral Analysis	2.2	2.9	87.4
Without Blockchain Validation	1.9	2.6	89.0
Full Proposed Model	0.9	1.2	93.5

Table 3 is an analysis of the contribution of each element in the proposed architecture. The removal of any module results in the observed drop in performance, which makes the need to combine various verification factors apparent.

4.7 Discussion

The results suggest that the authentication system proposed as a multi-layer approach is very effective in terms of security while retaining a good performance in terms of virtual classroom settings. Biometric validation combined with blockchain validation and behaviour analytics helps to increase the protection against unauthorized access and identity spoofing. The suggested model is more robust both in regard to security and minimal errors compared to traditional and single-method systems without excessive latency. An ablation study is a validation as well to indicate that all the components are required to make the system effective as a whole. These outcomes have revealed that authentication, together with a combination, is needed to support the various security needs of the new remote learning methods.

5 Conclusion and Future Work

The study has demonstrated a multi-layered secure authentication framework that can be tailored to be implemented in online classrooms to rectify some of the dire issues of identity verification, unauthorized access, and data integrity within the distance learning setting. The model suggested was compared to the conventional authentication strategies and has become much better with the addition of biometric authentication, device fingerprinting, behavioral analytics, and blockchain validation of credentials. Experimental analysis showed that the framework had an authentication accuracy of 98.7, a low False Acceptance rate of 0.9%, a low False Rejection rate of 1.2%, and a low average latency of 1.8 seconds.

Also, the Security Strength Index was 93.5%, which means that there was a significant improvement in the system's robustness. Optimistically, it was also concluded by the ablation study that each of the components has a significant contribution to the overall performance, and if any module is not present in the modules, it leads to a significant degradation in performance. The results show that the combination of different authentication levels is useful to achieve the right balance of security, ease of use, and system efficiency.

The further development of the adaptability and smartness of the authentication system by integrating advanced deep learning models to perform real-time behavioral analysis and threat detection can be the focus of future investigation. Computational overhead can also be minimized by integrating lightweight blockchain frameworks, which are also more scalable in resource-constrained environments. The framework can be extended to support cross-platform interoperability and integration with emerging technologies, such as edge computing and systems based on 6G, which can further enhance responsiveness and reliability. In real-world large-scale education deployments with a diverse user base, the evaluation of the system also provides more in-depth insights into the optimization of the system and improvements in its usability.

References

[1] A. Suresh kumar. (2025). Next-Generation Wireless Security Architectures for Mobile Learning Platforms. *Recent Advances in Next-Generation Wireless Communication Systems, 59*–67.

[2] Ahmad, S., Mehfuz, S., Urooj, S., & Alsubaie, N. (2024). Machine learning-based intelligent security framework for secure cloud key management. *Cluster Computing*, *27*(5), 5953-5979. https://doi.org/10.1007/s10586-024-04288-8

[3] Alahmari, S., Alshardan, A., Al-Wesabi, F. N., Sorour, S., Alghushairy, O., Alsini, R., ... & Al Duhayyim, M. (2025). A decentralized and privacy-preserving framework for electronic health records using blockchain. *Alexandria Engineering Journal*, *126*, 196-203. https://doi.org/10.1016/j.aej.2025.04.069

[4] Alsumayt, A., El-Haggar, N., Alshammari, M., Alghamedy, F. H., & AlFawaer, Z. (2026). Enhancing Security in Operational Technology: The Role of Multi-Factor Authentication Against Cyber Threats. *Journal of Artificial Intelligence and Technology*, *6*, 64-78. https://doi.org/10.37965/jait.2025.0881

[5] Ayeswarya, S., & Singh, K. J. (2025). Enhancing security and usability with context aware multi-biometric fusion for continuous user authentication. *Scientific Reports*, *15*(1), 30627. https://doi.org/10.1038/s41598-025-14833-z

[6] Dash, M. K., Panda, G., Kumar, A., & Luthra, S. (2022). Applications of blockchain in government education sector: a comprehensive review and future research potentials. *Journal of Global Operations and Strategic Sourcing*, *15*(3), 449-472. https://doi.org/10.1108/jgoss-09-2021-0076

[7] Eljak, H., Ibrahim, A. O., Saeed, F., Hashem, I. A. T., Abdelmaboud, A., Syed, H. J., ... & Elsafi, A. (2023). E-learning-based cloud computing environment: A systematic review, challenges, and opportunities. *IEEE Access*, *12*, 7329-7355. https://doi.org/10.1109/access.2023.3339250

[8] Jaoua, F., Almurad, H. M., Elshaer, I. A., & Mohamed, E. S. (2022). E-learning success model in the context of COVID-19 pandemic in higher educational institutions. *International Journal of Environmental Research and Public Health*, *19*(5), 2865. https://doi.org/10.3390/ijerph19052865

[9] Kalapaaking, A. P., Khalil, I., & Atiquzzaman, M. (2023). Smart policy control for securing federated learning management system. *IEEE Transactions on Network and Service Management*, *20*(2), 1600-1611. https://doi.org/10.1109/tnsm.2023.3276594

[10] Kesufekad Metachew, Letahun Nemeon, Dinfe Egash, Kasil Teyene. (2026). Communication-Centric Security Models for Mobile Digital Learning Systems. *Progress in Electronics and Communication Engineering, 3*(2), 76-84.

[11] Khashan, O. A., Alamri, S., Alomoush, W., Alsmadi, M. K., Atawneh, S., & Mir, U. (2023). Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments. *Computers, Materials & Continua*, *75*(2). https://doi.org/10.32604/cmc.2023.036217

[12] Korać, D., Damjanović, B., & Simić, D. (2022). A model of digital identity for better information security in e-learning systems. *The Journal of Supercomputing*, *78*(3), 3325-3354. https://doi.org/10.1007/s11227-021-03981-4

[13] Lam, T. Y., & Dongol, B. (2022). A blockchain-enabled e-learning platform. *Interactive learning environments*, *30*(7), 1229-1251. https://doi.org/10.1080/10494820.2020.1716022

[14] Lien, C. W., & Vhaduri, S. (2023). Challenges and opportunities of biometric user authentication in the age of iot: A survey. *ACM Computing Surveys*, *56*(1), 1-37. https://doi.org/10.1145/3603705

[15] Liu, M., & Yu, D. (2023). Towards intelligent E-learning systems. *Education and Information Technologies*, *28*(7), 7845-7876. https://doi.org/10.1007/s10639-022-11479-6

[16] Looi, K. H. (2022). Overcoming challenges to make e-learning a panacea for present and future crises. *The International Journal of Information and Learning Technology*, *39*(3), 227-239. https://doi.org/10.1108/ijilt-10-2021-0157

[17] Mawgoud, A. A., Taha, M. H. N., Loey, M., Hussain Malik, M., & Khalifa, N. E. (2025). Enhancing Data Privacy and Trust in E-Learning: A Blockchain-Based Access Control Protocol for Cloud Educational Systems. *Concurrency and Computation: Practice and Experience*, *37*(18-20), e70185. https://doi.org/10.1002/cpe.70185

[18] Nazir, A., He, J., Zhu, N., Anwar, M. S., & Pathan, M. S. (2024). Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain. *Cluster computing*, *27*(6), 8367-8392. https://doi.org/10.1007/s10586-024-04436-0

[19] Rukhiran, M., Wong-In, S., & Netinant, P. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. *Ieee Access*, *11*, 22767-22787. https://doi.org/10.1109/access.2023.3253024

[20] Soy, A. (2025). Secure and Intelligent Collaboration Frameworks for Online Learning Platforms. *Transactions on Internet Security, Cloud Services, and Distributed Applications*, 56-65.

[21] Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Acien, A., & Le Lan, G. (2022). Mobile behavioral biometrics for passive authentication. *Pattern Recognition Letters*, *157*, 35-41. https://doi.org/10.1016/j.patrec.2022.03.014

[22] Su, P. (2023). Immersive online biometric authentication algorithm for online guiding based on face recognition and cloud-based mobile edge computing. *Distributed and Parallel Databases*, *41*(1), 133-154. https://doi.org/10.1007/s10619-021-07351-0

[23] Tandi, M. R. (2024). Secure Peer-Assisted Communication Protocols for Distributed E-Learning Systems. *Transactions on Secure Communication Networks and Protocol Engineering*, 40-50.

[24] Uslu, U., İncel, Ö. D., & Alptekin, G. I. (2023). Evaluation of deep learning models for continuous authentication using behavioral biometrics. *Procedia Computer Science*, *225*, 1272-1281. https://doi.org/10.1016/j.procs.2023.10.115

Authors Biography

Sitora Yadigarova is a Senior Lecturer in the Department of Foreign Language and Literature at Termez University of Economics and Service. Her academic interests include foreign language education, literature studies, linguistics, and innovative methodologies in language teaching and learning. She has been actively involved in teaching and research activities focused on enhancing language proficiency and intercultural communication skills among students. Her work emphasizes communicative teaching approaches, modern pedagogical practices, and interdisciplinary research in language and literature studies. She also contributes to academic initiatives and professional development programs that support educational excellence in higher education. She is based in Termez, Uzbekistan

Sardor Salaxutdinov is affiliated with Oriental University. His academic interests include oriental studies, higher education, interdisciplinary research, and innovative approaches to teaching and learning. He has been actively engaged in academic and scholarly activities focused on promoting cultural studies, language education, and student-centered learning practices. His work emphasizes modern educational methodologies, research collaboration, and the advancement of academic excellence in higher education. He also contributes to institutional initiatives and research projects that support educational and professional development. He is based in Tashkent, Uzbekistan.

Tileubergen Arzimbetov is an Associate Professor at the Nukus branch of Uzbek State University of Physical Culture and Sports. His academic interests include physical education, sports sciences, athletic training, and innovative methodologies in sports pedagogy and professional education. He has been actively involved in teaching, research, and academic development activities aimed at improving the quality of physical culture and sports education. His scholarly work focuses on modern training techniques, student development, healthy lifestyle promotion, and interdisciplinary research in sports sciences. He also contributes to mentoring students and supporting academic initiatives related to physical education and athletic performance. He is based in Nukus, Karakalpakstan, Uzbekistan

Abdurafik Valiyev is an Associate Professor at Bukhara State Pedagogical Institute. His academic interests include pedagogy, teacher education, educational psychology, and innovative methodologies in higher education. He has been actively involved in teaching, research, and academic development activities aimed at improving educational quality and professional training. His scholarly work focuses on modern pedagogical practices, student-centered learning, and interdisciplinary educational research. He also contributes to mentoring future educators and supporting academic initiatives within the university community. He is based in Bukhara, Uzbekistan.

Nazirjon Akhmadov is an Associate Professor at Bukhara State University. His academic interests include higher education, pedagogy, interdisciplinary research, and innovative teaching and learning methodologies. He has been actively involved in teaching, research, and academic development activities focused on improving educational quality and promoting student-centered learning practices. His scholarly work emphasizes modern pedagogical approaches, professional development, and collaborative research initiatives in higher education. He also contributes to academic programs and institutional projects that support educational and scientific advancement. He is based in Bukhara, Uzbekistan.

Behzodbek Akbarov is affiliated with the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan and the University of Tashkent for Applied Sciences. His academic and professional interests include higher education policy, applied sciences, educational innovation, and interdisciplinary research. He has been actively involved in initiatives aimed at improving the quality of higher education, promoting scientific development, and supporting innovation in academic institutions. His work focuses on modern educational practices, research collaboration, and the advancement of knowledge-based systems. He also contributes to policy-oriented and academic projects that strengthen the higher education sector in Uzbekistan. He is based in Tashkent, Uzbekistan.

Shakhnoza Rakhimova is affiliated with the Department of Pedagogy at Termez State Pedagogical Institute. Her academic interests include pedagogy, educational psychology, teacher training, and innovative teaching methodologies in higher education. She has been actively involved in teaching and research activities aimed at improving the quality of education and professional development of future educators. Her scholarly work focuses on modern pedagogical practices, student-centered learning, and interdisciplinary approaches in education. She also contributes to academic initiatives and mentoring programs that support academic excellence and institutional development. She is based in Termez, Uzbekistan.