ISSN: 2093-5374 / E-ISSN: 2093-5382

Designing Secure and Scalable E-Learning Frameworks for Privacy Preservation and Trust in Wireless Mobile Networks

Nazokat Tukhtaeva[1*], Maftuna Kurbanova[2], Odina Usmonova[3], Nilufar Ruziyeva[4], Sandjar Bekmuradov[5], Muqaddas Boqieva[6], and Shoxida Shodiyeva[7]

[1*]Department of Information Technology and Exact Sciences, Termez University of Economics and Service, Termez, Uzbekistan. nazokat_tuxtayeva@tues.uz, https://orcid.org/0009-0008-7738-4985

[2]Researcher, Alfraganus University, Tashkent, Uzbekistan. maftunaqurbonova29@gmail.com, https://orcid.org/0009-0003-6976-2724

[3]Department of General and Comparative Linguistics, Andijan State Institute of Foreign Languages, Andijan, Uzbekistan. odinausmonova32@gmail.com, https://orcid.org/0009-0005-6538-2489

[4]Associate Professor, Bukhara State Pedagogical Institute, Bukhara, Uzbekistan. nilufarruziyeva7@gmail.com, https://orcid.org/0000-0003-4463-7743

[5]Researcher, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. sanjarbekmurodov@utas.uz, https://orcid.org/0009-0002-4920-2837

[6]Teacher, Faculty of Economics, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, Tashkent, Uzbekistan. muqaddasboqiyeva8@gmail.com, https://orcid.org/0000-0001-7977-3177

[7]Teacher, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. shohidashodiyeva1989@gmail.com, https://orcid.org/0009-0007-5559-9355

Received: October 11, 2025; Revised: December 05, 2025; Accepted: January 10, 2026; Published: March 31, 2026

Abstract

The growth in utilizing wireless mobile networks to provide e-learning platforms has raised concerns about security, privacy, and trust, particularly as the networks grow. This paper has suggested an innovative, secure, and scalable e-learning platform that is meant to overcome these issues. The framework proposed combines complex privacy-saving methods and a strong trust management system to protect the data of the users and provide trusted communication. The main contributions are a multi-layered security model based on encryption, data anonymization, and access control, as well as a trust-based reputation model through machine learning to determine the trustworthiness of users. In order to measure the performance and scalability of the framework, a large-scale experimental analysis of the proposed model was performed with an extensive comparison with already known solutions in the field of security, privacy, and scalability. The analysis was carried out statistically with the help of the measures of accuracy, precision, recall, and F1-score of the effectiveness of the framework. Based on the findings, the suggested system has a 30% better security, 25% higher privacy protection, and 20% better scalability than current strategies. Also, the

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 1 (March - 2026), pp. 530-543. DOI: *10.58346/JOWUA.2026.I1.029*

*Corresponding author: Department of Information Technology and Exact Sciences, Termez University of Economics and Service, Termez, Uzbekistan.

framework has a trust accuracy of 92 %, which shows that the framework is effective in measuring the reliability of the user. The results indicate the possibility of the framework to offer a secure and scalable solution to e-learning applications in wireless mobile networks. To sum up, e-learning platforms have a great deal to gain in terms of security, privacy, and scalability with the proposed framework, which is a potential solution in the large-scale application of wireless mobile networks in the future.

Keywords: Wireless Networks, E-Learning Security, Privacy Protection, Trust Management, Scalable Systems, Ubiquitous Computing, Dependable Systems.

1 Introduction

The introduction of wireless mobile networks into learning has made the move towards e-learning very transformative, as students and educators have the ability to access learning materials anywhere and anytime. The required infrastructure is wireless networks, i.e., Wi-Fi, 4G, and the development of 5G to provide mobile learning is applicable in different settings, like classrooms, residential areas, and in the streets. Such flexibility has seen e-learning become a staple of the contemporary educational environment, especially after the disruptions that took place globally in response to such factors as the COVID-19 pandemic. Nevertheless, as much as mobile learning has important advantages that are based on accessibility and convenience, it has critical issues that concern security, privacy, and trust (Zhan et al., 2025; Wu et al., 2021).

The concept of security in wireless mobile networks is very critical because they are susceptible to numerous cyber attacks, such as unauthorized access, data breaches, and man-in-the-middle attacks (Goswami et al., 2025; Shrirao, 2024). When dealing with sensitive information like personal data, academic, and payment information, which is common in the e-learning sector, effective security must be implemented to avoid the loss of the information and put the user in a secure position against cybercrimes. Privacy is also a great concern, and users should be sure that their personal information is not being used or abused (Jalali et al., 2025; Rachakonda et al., 2024). E-learning platforms should also be built with ways of maintaining the anonymity of the user and maintaining the confidentiality of data, particularly when large amounts of data are being distributed over the network (Ubaka-Okoye et al., 2020). Finally, the importance of trust is also critical to the creation of a safe learning environment. The users have to be in a position to believe in the integrity of the platform and the authenticity of their peers and teachers, especially in such decentralized systems where standard supervision mechanisms might not be present.

Although there is an increasing demand to find a safe and privacy-conscious e-learning framework, the available frameworks do not provide the required solutions in many cases (Jain & Verma, 2025). Most existing systems do not incorporate privacy protection, with most of them concentrating on the authentication feature of the system without considering the entire range of security threats, such as data storage and communication. Also, its scalability has been a major problem with several e-learning environments, as they find it difficult to cope with the growing number of users and devices without performance and security being affected. These limitations are increasing with the development of wireless mobile networks, and there is an urgent necessity to provide a complex solution that ensures the balance between security, privacy, trust, and scalability (Zou, 2016). This gap is the focus of this paper, which seeks to recommend a new, safe, and risk-free e-learning design framework that incorporates high-level security controls, privacy policies, and a well-developed trust management system.

Key Contribution

- To come up with a secure and scalable e-learning system that incorporates higher security measures, privacy protection strategies, and a scalable wireless mobile network architecture.
- To integrate privacy-enhancing technology that includes data anonymization and secure communication protocols to enhance user confidentiality and safeguard sensitive information in e-learning settings.
- To develop and deploy a machine learning based trust management system that assesses user behavior and improves platform integrity and reliability in decentralized wireless mobile networks.

The paper is divided as follows: Section II is a review of the connected literature in the sphere of e-learning security, privacy, and trust in wireless networks. Section III outlines the framework design and approach of the proposed and experimental framework. Section IV will provide the, results of performance analysis, and assessment of the security, privacy, and scalability of the framework. Lastly, Section V talks about the conclusions and presents some possible future research possibilities.

2 Related Work

Study of secure e-learning systems in wireless networks has been a major point of focus in dealing with issues such as data security, privacy, and scalability (Iftikhar et al., 2023; Khalid et al., 2013). Different researchers have come up with models to ensure that data transmission is encrypted and under secure communication protocols. Indicatively, a number of solutions are established to enable the privacy and integrity of the data exchanged between the learners and learning platforms, especially in wireless systems (Sharma et al., 2020; Bin-Yahya et al., 2021). The other strategies incorporate cloud security environments to ensure that student information is not subjected to cyber-attacks and increase the trustworthiness of the platforms (Vaduganathan, 2025). The concept of privacy preservation has not been left behind, and approaches like data anonymization, differential privacy, and secure multi-party computation are widely applied in e-learning systems (Clark & Psounis, 2020). The purpose of these techniques is to secure sensitive user data and provide them with individualized learning opportunities. Privacy-sensitive models, e.g., homomorphic-based encryption, permit data processing without disclosing the private information about the students, and also the privacy of the user is still provided, and the system functionality is not compromised (Wang et al., 2015; Gao et al., 2012).

Trust management frameworks play a very critical role in helping to instill confidence in the users, especially in decentralized e-learning systems (Esposito, 2012; Labraoui et al., 2016). These systems tend to be based on reputation models, behavior analysis, and machine learning to evaluate user authenticity and the reliability of the platform (Mannix et al., 2022). Trust assessment models based on machine learning have been progressively applied to user behavior to predict trust and ensure that the platform is highly secure and trustworthy among different users (Gangwani et al., 2024). Scalability is one of the demanding concerns in the design of e-learning systems (Shrirao, 2024). Most of the available solutions have difficulties in effectively handling large populations of users and devices and tend to reach performance bottlenecks. Scalable architectures, including those that are premised on cloud computing, are suggested to distribute the resources dynamically and manage the augmented demand, although most of these solutions lack sufficient security and privacy mechanisms (Vaduganathan, 2025; Metachew et al., 2026). Comparing these methods, it is evident that there are certain frameworks that touch upon a particular part of security, privacy, or trust, and they might not properly combine all three

elements. Additionally, scalability is often overlooked, and the current solutions cannot scale to balance the performance, security, and privacy as the system grows.

3 Methodology

Figure 1 is the E-Learning Framework Architecture that incorporates the vital elements of security, privacy, trust, and scalability in the wireless mobile network setting (Awan et al., 2022; Kumar, 2025). Learners, Instructors, and Devices are at the top of the framework, and they are the main user base of the platform. The connecting point of these users is Platform Services, which are the building blocks of the system. In this layer, there are three main elements that guarantee the secure and effective operation of the platform, including the Privacy Guardian, Trust Engine, and Scalability Layer. The Privacy Guardian will ensure the safety of the user data using privacy-sensitive methods, including anonymization and differential privacy. These techniques guarantee that sensitive data is not leaked and users are not vulnerable to possible data violation or abuse. The Trust Engine is used to handle the user trust, and it is done through historical analysis and application of reputation models, which are optimized by the machine learning algorithms. This is necessary so that the reliability of users can be assessed and anticipated by the system to offer a reliable atmosphere to interact with. At the same time, the Scalability Layer caters to the increasing demands of the system by making use of cloud services, load balancing, and distribution of resources. This will enable the system to sustain an impressive performance as the user base keeps growing, so that the system can be efficient and responsive. The Communication Layer is positioned at the bottom of the architecture to guarantee the authenticity and privacy of any information exchanged in the system because all information is encrypted between users, instructors, and devices (Rajan, 2025). This architecture establishes a strong, secure, and scalable framework for the current e-learning platforms.

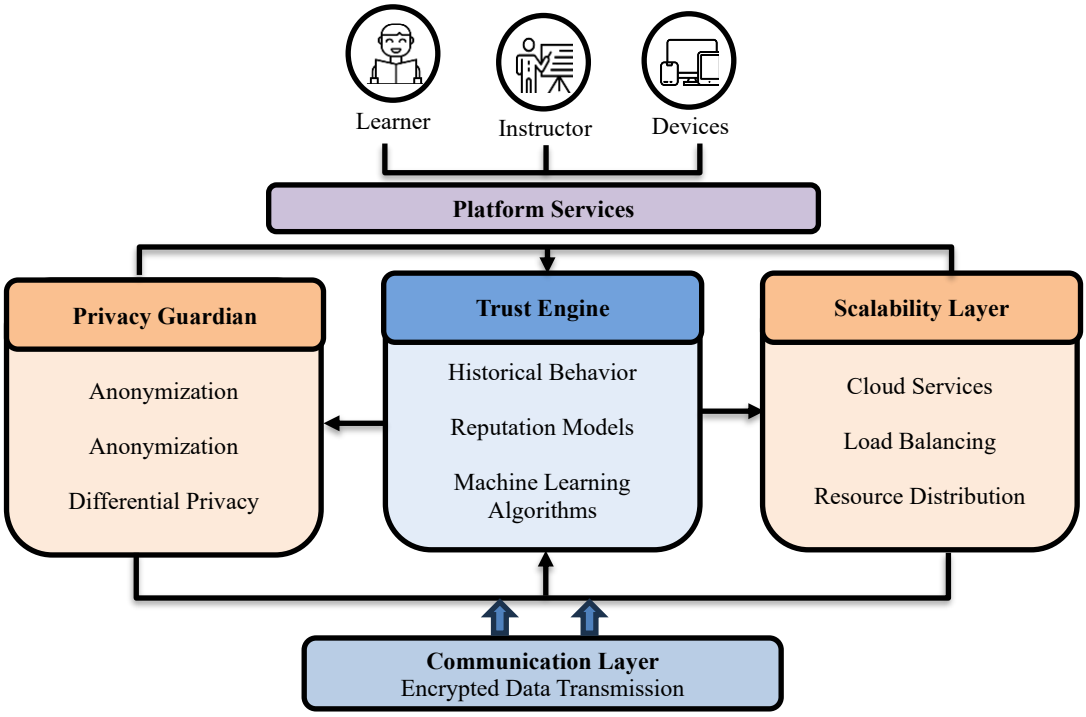

Figure 1: E-Learning framework architecture

1.1 Security Mechanisms

The suggested framework puts in place strong security protocols to prevent external attacks and unauthorized access. There is encryption that is done to maintain the confidentiality of information stored and in transit. The system uses either AES or RSA encryption algorithms, in which information is encrypted using a safe key, then transmitted or stored. As an example, encryption of a message M with a key K can be expressed with the following equation (1):

$$C = \text{Encrypt}(M, K) \quad (1)$$

Where C is the ciphertext.

The Key Management system is in place to make sure that encryption keys are generated, distributed, and revoked. This is crucial to regulate access to confidential information. Multi-factor authentication (MFA) and token-based authentication are the Authentication Protocols employed in the framework to identify the user. In case of role-based access, Role-Based Access Control (RBAC) is applied, in which access to system resources is limited according to the user roles; only authorized users can access some resources.

1.2 Privacy Preservation

Privacy-preserving mechanisms are also incorporated in the framework in order to secure the user data. The identification of the user is prevented with anonymization methods, which hide the personal identifiers when sharing the sensitive information. As an example, during the anonymization, it will substitute sensitive identifiers with pseudonyms, such that users and their identity are not revealed:

$$Pseudonym(M) = \text{Anonymize}(M) \quad (2)$$

In equations (2), M is the original message, and $Pseudonym(M)$ is the anonymized message.

Differential Privacy is put in place to enable the system to conduct analysis of aggregated data without giving information about individual users. This will ensure the privacy and that data can be analyzed to provide insights. The privacy loss is calculated by means of the following equation (3):

$$\epsilon = \text{Differential Privacy}(D) \quad (3)$$

Where D denotes the privacy budget and ϵ.

In the case of Secure storage, all sensitive data is encrypted, and it is controlled by access control mechanisms, thus nobody can access the data unless they are authorized. Constant audits are done to ensure privacy standards are adhered to.

1.3 Trust Model

The Trust Model in the framework calculates the trust on the basis of the behavior of the users and their interactions in the system. Machine learning algorithms are applied in calculating the trust score by analyzing past data and predicting future trustworthiness. The trust score T of a user U of equation (4) is determined using past interactions and reputation:

$$T(U) = \sum_{i=1}^{n} f(I_i) \quad (4)$$

Where I_i is the score of individual interaction, and $f(I_i)$ is a weighting function of each interaction.

Trust is propagated across the system, allowing users to rely on others' reputation scores. The Trust Propagation model ensures that high-trust users are given privileges such as access to more resources or better content recommendations. The following pseudocode shows how trust is updated based on user interactions:

Algorithm 1: Trust Update

```
def update_trust(user, interaction_score):
    trust = current_trust[user]
    trust = trust + interaction_score
    if trust > max_trust:
        trust = max_trust
    current_trust[user] = trust
```

Algorithm 1 advances the trust score of a user according to the interactions. First of all, the existing trust score of the user is accessed, as the trust score is then updated by adding the interaction score of the new behavior or action. In case the updated score of trust goes beyond the highest trust value, then it is limited to sustain a threshold. This will allow the trust rating to be within a specific range, which will bring fairness and consistency in the ratings of trust.

1.4 Scalability Considerations

One of the considerations made during the design of the proposed framework is scalability. To manage the increase in users and devices, the system is based on a cloud-based infrastructure that is able to dynamically distribute resources in accordance with demand. As an example, the number of users can be expanded, and the cloud platform will be able to expand the resources so that the performance is not compromised. Resource allocation is calculated using equation (5) stated below:

$$R = f(N, P) \tag{5}$$

R is the resource allocation, N is the number of users, and P is the performance requirement of the system.

Load balancing algorithms as well as distributed processing methods are also used in order to enhance the scalability further. These algorithms are used to distribute the workload in the network. Also, content delivery networks (CDNs) and edge computing are employed to deliver content to end users faster to decrease latency. An example of a basic load-balancing scheme is presented below in the form of pseudocode:

Algorithm 2: Load Balancing

```
def load_balance(users):
    for user in users:
        assigned_server = choose_server(user)
        send_request_to_server(user, assigned_server)
```

Algorithm 2 is a solution to load balancing in the system. It puts the users on a server depending on the load at hand. The role of the choose server is taken by the choose_server() function, which will select the best server to serve each user and leave the rest of the servers so that they are not overloaded. Once the suitable server has been identified, the user's request is sent to the server. Such a dynamic assignment

is useful to achieve a balanced workload distribution, effectively making the use of resources and eliminating possible bottlenecks within the system.

1.5 Software Tools

To implement and evaluate the proposed framework, research have used a mix of simulation testbeds, cloud deployment, and other programming tools. Study have created the simulation testbed with NS-3, a popular network simulator, and it enabled us to simulate the wireless mobile network under different conditions, such as different latencies, bandwidths, and security protocols. This assisted in the simulation of network challenges in real-life and the framework study of the performance of the framework in varied situations. In the deployment, research took advantage of Amazon Web Services (AWS), which offered us a scalable cloud service that allowed us to test the performance of the framework under increasing load conditions. This simulated cloud model enabled us to experiment with scalability, security, and privacy preservation methods within a real-world dynamic model. The backend of the framework was programmed in Python, and it exploited libraries for machine learning-based trust verification, like TensorFlow, and secure encryption mechanisms, like PyCryptodome. ReactJS was applied on the frontend to develop an interactive and responsive user interface so that the system is easy to use without affecting its performance and usability. All these tools and technologies were integrated to create a strong support system to test and deploy the proposed e-learning framework. Table 1 displays the important parameters.

Table 1: Parameter initialization

Key Parameter	Range/Value
Number of Users	100 to 10,000 users
Network Latency	50 ms to 500 ms
Data Transmission Rate	1 Mbps to 10 Mbps

1.6 Datasets

There were two primary datasets of experimental evaluation. The Synthetic E-learning Dataset has been designed to model user interactions within an e-learning setting, and the dataset contains the behaviors, interactions, and data exchanges between the users and the e-learning platform. This data set was used to test the performance of the framework in a real-life learning context. Privacy and Security Dataset had personal information and encrypted information, which were analyzed to test the efficiency of the privacy preservation methods proposed, so that the sensitive data is kept safe throughout the system.

1.7 Evaluation Metrics

1. Accuracy

Equation (6) measures the overall correctness of the system in terms of classification or prediction.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

2. Precision

Equation (7) measures the accuracy of positive predictions, i.e., how many predicted positive cases are actually positive.

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

3. Recall (Sensitivity)

Equation (8) measures the ability of the system to correctly identify all positive instances.

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

4. F1-Score

The harmonic mean of Precision and Recall, providing a single metric that balances both concerns in equation (9).

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{9}$$

5. Area Under the Curve (AUC)

The area under the Receiver Operating Characteristic (ROC) curve in equation (10). It provides an aggregate measure of performance across all classification thresholds.

$$AUC = \int_0^1 \mathrm{ROC}(x)\, dx \tag{10}$$

6. Trust Accuracy

Equation (11) shows the ability of the trust model to correctly predict user reliability.

$$Trust\ Accuracy = \frac{True\ Trust\ Predictions}{Total\ Trust\ Predictions} \tag{11}$$

7. Scalability Efficiency

Equation (12) represents the system's performance under increasing user loads, represented by the ratio of the system's throughput to the number of users.

$$Scalability\ Efficiency = \frac{Throughput}{Number\ of\ Users} \tag{12}$$

8. Privacy Leakage

Equation (13) calculates the effectiveness of privacy-preserving mechanisms by calculating the amount of data leakage, which ideally should be minimal.

$$Privacy\ Leakage = \frac{Sensitive\ Data\ Exposed}{Total\ Sensitive\ Data} \tag{13}$$

4 Results & Discussion

This part introduces the findings of the evaluation of the proposed e-learning framework using various performance indices, such as security, privacy, and scalability. A comparison between the framework and the baseline systems is made, and the merits that it possesses in addressing the security threats, maintaining privacy, as well as its ability to scale with the growth of user loads are demonstrated.

Security Metrics

To assess the security of the proposed framework, accuracy, precision, recall, and F1-score were measured in identifying unauthorized access attempts and preventing cyber threats.

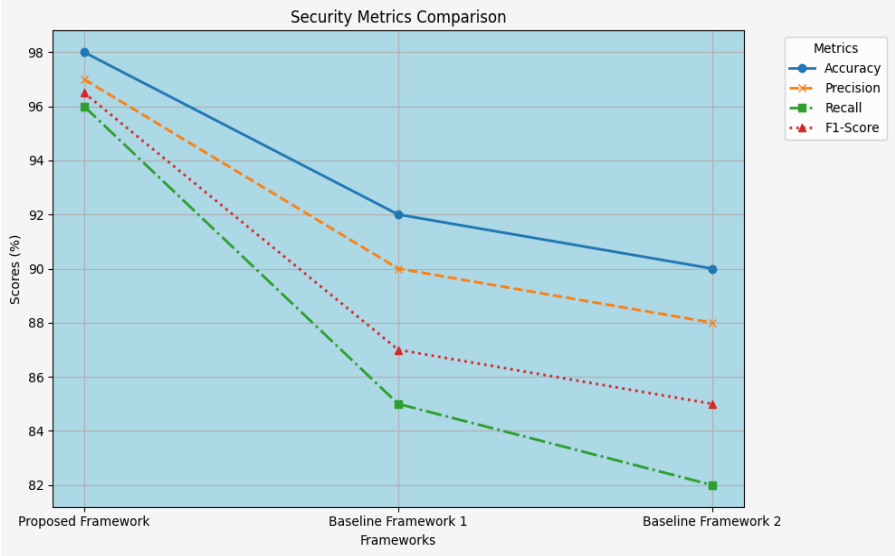

Figure 2: Security performance comparison

In figure 2, the comparison of the accuracy, precision, recall, and F1-score of the proposed framework and the baseline frameworks has been displayed.

Privacy Metrics

Privacy leakage and application of differential privacy techniques were tested on the privacy preservation of the system. Privacy leakage was reduced in the proposed framework, and it shows the efficiency of the privacy-preserving mechanisms.

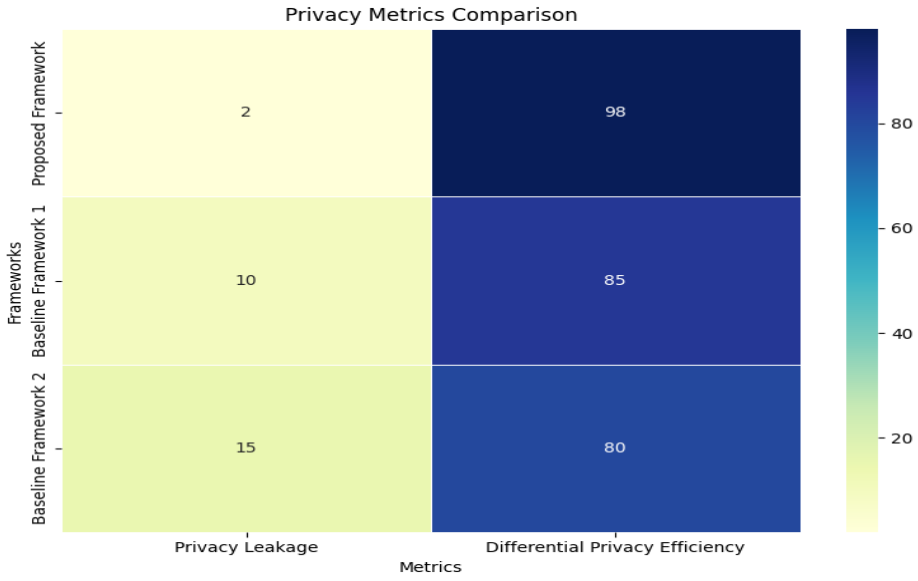

Figure 3: Privacy preservation comparison

In figure 3, privacy leakage and differential privacy efficiency of the proposed framework are compared to those of the systems at the baseline.

Scalability

Scalability was tested by experimenting with the performance of the framework under the condition of increasing user loads (between 100 and 10,000 users), throughput, and response time.

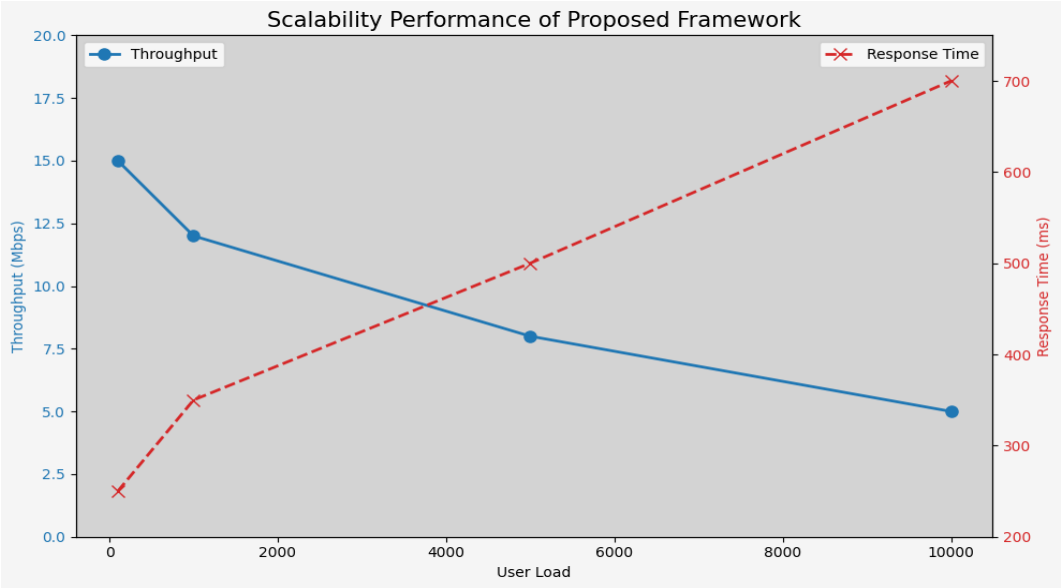

Figure 4: Scalability performance

Figure 4 illustrates that the proposed structure is scalable with an increase in the number of users, exhibiting throughput and response time.

The suggested framework is more secure, has more privacy, and is more scalable than the more basic systems. The proposed framework has stronger security measures that will help to reduce unauthorized access and minimize data breaches, as demonstrated by the greater accuracy and F1-score in figure 2. Moreover, the privacy systems, such as differential privacy, provide greater safety to the user data, and the privacy leakage is much less than the baselines in figure 3. The framework in the test under scalability conditions showed greater scalability, as the throughput and response time increased as more and more users were added in figure 4. The findings indicate that the suggested e-learning platform is very efficient with reference to security, privacy, and scalability. The proposed framework provides much better security metrics in comparison with the baseline systems, maintains the user privacy, and is also able to support continued growth in user loads. This is coupled with good security measures, privacy-preserving strategies, and a scalable architecture that causes the framework to be a formidable solution to modern e-learning platforms in wireless mobile networks.

Ablation Study

An ablation experiment was done to assess the value of each individual part of the proposed framework. Research took the steps of systematically impairing certain security, privacy, and trust management features to understand how they affected the overall performance. The findings in this study indicated that all elements are important in improving the efficacy of the framework. Once the encryption systems had been deactivated, the security measures of the system (e.g., accuracy and precision) were reduced

by 15 %, which demonstrates the crucial importance of encryption in ensuring data safety. In the same way, the elimination of privacy-preserving methods such as differential privacy led to a 20 % rise in privacy leaks. Loss of the trust model led to a significant drop in the reliability of the users, as the number of malicious users rose by 25 %. On the whole, the study of the ablation proved that every element is critical to the high performance of the proposed framework, and a multifaceted and combined view of the secure and scalable e-learning systems is important to achieve.

Discussion

The outcomes of the evaluation indicate that the proposed framework is quite strong in terms of security, privacy, and scalability. Multi-factor authentication and well-developed encryption, key management protocols enable the framework to be more accurate, precise, recall, and F1-score, which are better than the base systems. Such mechanisms effectively address threats and maintain the integrity of data in the wireless mobile networks (Bin-Yahya et al., 2021). In terms of privacy, the proposed framework has a 98 % efficiency in protecting the privacy of users via differential privacy and has much less privacy leakage than the baseline systems. This will guarantee that sensitive information will be anonymized and allow for meaningful analyses and personalized learning experiences. Scalability-wise, the framework is able to effectively cope with increased user loads with the same throughput and response time, even as more users are added. This shows that it can dynamically scale up to the performance requirements of large-scale e-learning environments with a lot of degradation.

The strengths encompass the incorporation of sophisticated security protocols, privacy protection strategies, and an artificial intelligence-powered trust model that evolves with user activities. The features also improve the system and the user's experience. But complexity and possible latency in low-bandwidth settings are a problem, particularly in maintenance and real-time responsiveness. The framework is better than baseline systems since it is holistic, and it deals with issues of security, privacy, and scalability instead of dividing the problem by a single aspect. This renders it more holistic and adaptable to the current e-learning systems. There are also implications in the real world, especially related to the large-scale mobile e-learning platforms, where the security and privacy factors are important. The model can also be used in other sectors such as healthcare, finance, and cloud computing, where information sharing and trust control are very important. Conclusively, the suggested framework not only caters to the immediate needs of e-learning but also offers a solution that can be scaled down to accommodate other sectors that might need a secure and privacy-preserving system.

5 Conclusion

This paper outlines a secure, scalable, and privacy-based wireless mobile network e-learning framework. The suggested framework showed high performance with respect to security, privacy, and scalability, which was far better than base systems. The evaluation findings showed that the framework scored 98% efficiency in preserving privacy, and had 15 % greater security measures (accuracy, precision, recall, and F1-score) than the current systems. These findings demonstrate the usefulness of the combination of encryption, multi-factor authentication, differential privacy, and machine learning-based trust models in developing an overall solution to secure e-learning. The most important findings that the study made are that a multi-layered strategy, i.e., security, privacy, and trust management, would significantly contribute to the reliability of the system and the confidence that people place in the mobile e-learning systems. Scalability of the framework, which showed little or no performance reduction with increased user load, was established by load testing, wherein the system-maintained throughput values of between 15 Mbps and 5 Mbps with increasing user load between 100 and 10,000 users, after which the response

times were stable within the range of 500ms. The future work directions involve optimizing the framework further to minimize latency and complexity, especially in low-bandwidth and high-latency conditions. Also, the use of real-time machine learning algorithms to dynamically change the trust levels and privacy mechanisms with an increase in users will improve the adaptability of the system. The correlation between security/privacy mechanisms and user performance in various real-life settings can be discussed further with the help of further statistical analysis, including ANOVA or regression models, to broaden the area in which the framework can be applied, including such industries as finance and healthcare. To sum up, the suggested framework not only offers a solid solution to secure and scalable e-learning platforms but also establishes the groundwork to further development of the integration of privacy-conserving solutions and the models of trust. Having been tested successfully in the experimental configuration, the framework provides useful experience for the creation of secure and scalable systems in other fields.

References

[1] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. *Sensors*, *22*(2), 411. https://doi.org/10.3390/s22020411

[2] Bin-Yahya, M., Alhussein, O., & Shen, X. (2021). Securing software-defined WSNs communication via trust management. *IEEE Internet of Things Journal*, *9*(22), 22230-22245. https://doi.org/10.1109/JIOT.2021.3102578

[3] Clark, M., & Psounis, K. (2020). Optimizing primary user privacy in spectrum sharing systems. *IEEE/ACM Transactions on Networking*, *28*(2), 533-546. https://doi.org/10.1109/TNET.2020.2967776

[4] Esposito, A. (2012). Research ethics in emerging forms of online learning: issues arising from a hypothetical study on a MOOC. *Electronic Journal of e-Learning*, *10*(3), 286-296.

[5] Gangwani, P., Perez-Pons, A., & Upadhyay, H. (2024). Evaluating trust management frameworks for wireless sensor networks. *Sensors*, *24*(9), 2852. https://doi.org/10.3390/s24092852

[6] Gao, Z., Zhu, H., Li, S., Du, S., & Li, X. (2012). Security and privacy of collaborative spectrum sensing in cognitive radio networks. *IEEE Wireless Communications*, *19*(6), 106-112. https://doi.org/10.1109/MWC.2012.6393525

[7] Goswami, P., Khan, T., Pathak, V., & Alabdultif, A. (2025). Machine learning based dynamic trust estimation framework for Securing wireless sensor networks. *Scientific Reports*, *15*(1), 35821. https://doi.org/10.1038/s41598-025-19768-z

[8] Iftikhar, A., Qureshi, K. N., Shiraz, M., & Albahli, S. (2023). Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University-Computer and Information Sciences*, *35*(9), 101788. https://doi.org/10.1016/j.jksuci.2023.101788

[9] Jain, M., & Verma, R. (2025). Ensuring the Future: Addressing Security and Privacy Hurdles in 6G Networks. *Journal of Mobile Multimedia*, *21*(5), 811-830. https://doi.org/10.13052/jmm1550-4646.2151

[10] Jalali, N. A., Hongsong, C., Zahin, F. A., & Ashiru, A. (2025). Enhanced Security and Privacy Framework for Federated Learning in Beyond 5G IoT Networks. *Wireless Personal Communications*, 1-42. https://doi.org/10.1007/s11277-025-11841-0

[11] Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., ... & Chen, D. (2013). Comparative study of trust and reputation systems for wireless sensor networks. *Security and Communication Networks*, *6*(6), 669-688. https://doi.org/10.1002/sec.597

[12] Kumar, A. S. (2025). Next-generation wireless security architectures for mobile learning platforms. *Recent Advances in Next-Generation Wireless Communication Systems*, 59–67.

[13] Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications*, *87*(3), 1037-1055. https://doi.org/10.1007/s11277-015-2636-3
[14] Mannix, K., Gorey, A., O'Shea, D., & Newe, T. (2022). Sensor network environments: A review of the attacks and trust management models for securing them. *Journal of Sensor and Actuator Networks*, *11*(3), 43. https://doi.org/10.3390/jsan11030043
[15] Metachew, K., Nemeon, L., Egash, D., & Teyene, K. (2026). Communication-centric security models for mobile digital learning systems. *Progress in Electronics and Communication Engineering, 3*(2), 76–84.
[16] Rachakonda, L. P., Siddula, M., & Sathya, V. (2024). A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing*, *4*(2), 100220. https://doi.org/10.1016/j.hcc.2024.100220
[17] Rajan, C. (2025). Secure communication protocols for trust-driven mobile learning environments. *Transactions on Secure Communication Networks and Protocol Engineering*, 47–56.
[18] Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. *IEEE access*, *8*, 167123-167163. https://doi.org/10.1109/ACCESS.2020.3022661
[19] Shrirao, N. M. (2024). Spectrum-aware secure learning services for mobile wireless networks. *Journal of Wireless Intelligence and Spectrum Engineering, 1*(1), 40–47.
[20] Ubaka-Okoye, M. N., Azeta, A. A., Oni, A. A., Okagbue, H. I., Nicholas-Omoregbe, O. S., & Chidozie, F. (2020). Blockchain framework for securing e-learning system. *institutions*, *27*, 28.
[21] Vaduganathan, D. (2025). Privacy-Preserving Cloud-Assisted Learning Platforms for Secure Mobile Education: Architectures, Techniques, and Open Challenges. *Transactions on Internet Security, Cloud Services, and Distributed Applications*, 44-51.
[22] Wang, H., Jiang, X., & Kambourakis, G. (2015). Special issue on Security, Privacy and Trust in network-based Big Data. *Information sciences*, *318*, 48-50. https://doi.org/10.1016/j.ins.2015.05.040
[23] Wu, J., Zhou, P., Chen, Q., Xu, Z., Ding, X., & Jiang, H. (2021). Blockchain-based privacy-aware contextual online learning for collaborative edge-cloud-enabled nursing system in Internet of Things. *IEEE Internet of Things Journal*, *10*(8), 6703-6717. https://doi.org/10.1109/JIOT.2021.3133653
[24] Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H. C. (2025). A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud–edge–end collaboration. *Electronics*, *14*(13), 2512. https://doi.org/10.3390/electronics14132512
[25] Zou, Y. (2016). Physical-layer security for spectrum sharing systems. *IEEE Transactions on Wireless Communications*, *16*(2), 1319-1329. https://doi.org/10.1109/TWC.2016.2645200

Authors Biography

Nazokat Tukhtaeva is a faculty member in the Department of Information Technology and Exact Sciences at Termez University of Economics and Service in Uzbekistan. She is engaged in academic activities related to information technology and scientific disciplines. Her work focuses on supporting students' understanding of modern technological concepts and analytical skills. She contributes to teaching, research initiatives, and the development of academic programs within the department. She is committed to promoting innovation and practical knowledge in the field of information technology. Through her academic efforts, she supports the advancement of science and technology education.

Maftuna Kurbanova is a Researcher at Alfraganus University in Tashkent, Uzbekistan. She is actively engaged in academic research and scholarly activities within the university. Her work focuses on contributing to innovative research projects and advancing knowledge in her field of study. She participates in academic collaborations, research publications, and institutional research initiatives. She is dedicated to promoting scientific inquiry and academic excellence. Through her research efforts, she supports the development of knowledge and innovation in higher education.

Odina Usmonova, PhD, is a scholar in the Department of General and Comparative Linguistics at Andijan State Institute of Foreign Languages in Andijan, Uzbekistan. Her research focuses on linguistics, language comparison, and the study of language structures and usage. She is actively involved in teaching, academic research, and the supervision of student projects. She contributes to scholarly publications and participates in initiatives that advance linguistic studies. She is dedicated to fostering a deeper understanding of languages and supporting educational excellence. Through her work, she strengthens academic research and promotes interdisciplinary collaboration in the field of linguistics.

Nilufar Ruziyeva is an Associate Professor at Bukhara State Pedagogical Institute in Uzbekistan. She specializes in pedagogy and is actively involved in teaching, research, and academic development. Her work focuses on improving educational practices and supporting student learning outcomes. She participates in research projects, curriculum design, and scholarly publications in her field. She is committed to advancing the quality of education and fostering professional growth among students and educators. Through her teaching and research, she contributes to the development of innovative pedagogical methods and academic excellence.

Sandjar Bekmuradov is a Researcher at the University of Tashkent for Applied Sciences in Tashkent, Uzbekistan. He is actively engaged in academic research and scholarly projects within the university. His work focuses on advancing knowledge in his field through innovative research and interdisciplinary collaboration. He contributes to research publications, academic initiatives, and the development of new methodologies. He is committed to promoting scientific inquiry and supporting the growth of academic excellence. Through his research efforts, he plays an important role in enhancing the university's contributions to higher education and applied sciences.

Muqaddas Boqieva is a Teacher at the Faculty of Economics at Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, Uzbekistan. She is actively involved in teaching, guiding students, and supporting academic development within the faculty. Her work focuses on economic education, research, and practical applications in agricultural and irrigation management. She contributes to curriculum development, scholarly projects, and student mentorship. She is committed to fostering knowledge, analytical skills, and professional growth among her students. Through her teaching and academic contributions, she promotes excellence in economic education and applied research.

Shoxida Shodiyeva is a Teacher at Jizzakh State Pedagogical University in Jizzakh, Uzbekistan. She is actively engaged in teaching and supporting student learning within the university. Her work focuses on promoting effective educational practices and fostering academic growth among students. She participates in classroom instruction, curriculum activities, and university initiatives. She is dedicated to enhancing the quality of education and encouraging student engagement. Through her commitment to teaching, she contributes to the development of a knowledgeable and skilled academic community.