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

Developing Robust Trust Models for Security and Privacy in Mobile Education Systems

Dilfuza Teshabayeva[1*], Turdieva Nargiza Mardonovna[2], Sarvar Akobirova[3], Ziyodakhon Radjabova[4], Mahbuba Xoliyarova[5], Matluba Shodiyeva[6], Shakhlo Atakulova[7], and Dilorom Saliyeva[8]

[1*]Uzbek State World Languages University, Tashkent, Uzbekistan. d.teshaboyeva@uzswlu.uz; dilfuzateshabayeva4@gmail.com, https://orcid.org/0000-0002-9700-642X

[2]Associate Professor, Silk Road International University of Tourism and Cultural Heritage, Uzbekistan. nargiza.turdieva@univ-silkroad.uz, https://orcid.org/0000-0001-5424-4113

[3]Professor, Tashkent State University of Law, Uzbekistan. s.akobirova@tsul.uz, https://orcid.org/0000-0003-2526-2835

[4]Associate Professor, Department of Philology, Karshi State University, Uzbekistan. ziyodaxonradjabova@gmail.com, https://orcid.org/0009-0003-1673-3858

[5]Senior Teacher, Law Enforcement Academy of the Republic of Uzbekistan, Uzbekistan. mahbubaholiarova@gmail.com, https://orcid.org/0000-0003-4586-4067

[6]Department of Education, Samarkand State Pedagogical Institute, Uzbekistan. matluba_shodiyeva@mail.ru, https://orcid.org/0000-0003-3387-1585

[7]University of Economics and Pedagogy, Karshi, Uzbekistan. shahloatakulova95@gmail.com, https://orcid.org/0000-0002-4934-1768

[8]Professor, Kokand State University, Uzbekistan. solievad78@gmail.com, https://orcid.org/0000-0003-3908-9586

Received: August 20, 2025; Revised: October 04, 2025; Accepted: November 06, 2025; Published: December 15, 2025

Abstract

As mobile technologies continue to permeate all aspects of educational systems, protecting privacy and ensuring security becomes critically important. This research considers the development of trust models to improve security and privacy in mobile e-learning systems. This research presents a new framework for assessing and developing trust in mobile university systems. The framework approaches the unique challenges of mobile with the diversity of incorporating trusted (or more trusted) aspects of the mobile dimensions. Advanced cryptographic techniques, along with trusted behavioral profiles and machine learning techniques to guard personal information, secure exchanges, and ascribe trust in user identification and authentication forms the basis of the mobile university proposal. Multiple case studies are used to validate the trust model and demonstrate its effectiveness in reducing exposure and increasing trust. The importance of this research will benefit educators, developers, and policy makers focused on the formation of a secure and reliable mobile academic work platform.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 4 (December), pp. 269-284. DOI: *10.58346/JOWUA.2025.I4.015*

*Corresponding author: Uzbek State World Languages University, Tashkent, Uzbekistan.

Keywords: Mobile Education Systems, Trust Models, Security, Privacy, Cryptographic Techniques, User Authentication, Behavioral Analysis, Machine Learning, Data Protection, Privacy-Preserving Models.

1 Introduction

The last few years have witnessed an increasing incorporation of mobile devices into educational practices, which has further enhanced the interaction between learners and teachers and offered a range of mobile and flexible learning opportunities. [Receive additional citation] (Froyd et al., 2012). However, the integration of mobile devices into educational practices has also raised a myriad of issues concerning security and privacy. Mobile educational systems include sensitive personal information such as academic records, student profiles, and communication logs, which makes them susceptible to cyberattacks and breaches involving unauthorized access to personal data. [Receive additional citations] (Isroilova et al., 2025; Upchurch & Love, 2020). The educational value of mobile learning applications depends greatly on the trust users have in the systems; therefore, trust models are essential to provide a secure and safe environment for users, which in turn preserves the educational value of the applications and safeguards user information. For this reason, trust models are integral to ameliorating security threat experiences, and mobile educational systems must design and implement high-quality trust models to contain current threats and mitigate potential threats to the systems as a whole. This paper seeks to design and implement trust models for mobile educational systems based on the integration of cryptography, user behavior, and machine learning as an emerging approach to the security and privacy challenges within systems (Jiang et al., 2024).

2 Literature Review

In this context, trust models are concerned primarily with ensuring that mobile applications can trust their interactions with users, devices, and servers without compromising data privacy and integrity. Reputation-based models rely on user reviews and feedback, and prior interactions to trust an application or user (Quinn, 2019). Trust is built up over time as a user determines if an app is trusted based on previous usage behavior, since the credibility of the app, or whether there has been a security risk associated with using the app, depends on how many times in the past they have witnessed the app being trustworthy. Certification-based models use cryptography, such as digital certificates, to establish the identity of mobile apps. In this model, trust is measured through trusted authorities who certify the software and security components' integrity of the mobile app (Saidova et al., 2024). Behavioral trust models observe the behavior of users and apps to dynamically change trust based upon continuous interactions and detected anomalies. The core of trust is being able to recognize attacks before they happen and mitigate potential threats. Hybrid trust models include reputation, certification, and behavioral trust models for mobile environments to increase the robustness of the models for establishing trust. Trust, whether static (e.g., certification) or dynamic (e.g., reputation or behavior), more clearly indicates how trust occurs in mobile environments based on experience and behavior (Sharples et al., 2009).

2.1 Security and Privacy Concerns in Mobile Education Systems

Mobile education systems - increasingly prevalent in today's learning spaces - present a unique range of security and privacy challenges and concerns because of the sensitive data they process. Mobile education systems generate personal and academic data such as student identities, grades, and communications, giving an attacker a target and giving rise to privacy concerns. Data privacy presents

some of the greatest risks (Petrov & Zhdanova, 2023). In addition, authentication and identity management considerations also stem from needing to protect mobile education systems (Crompton, 2013). Specifically, the established convention of passwords or identification control for authenticating students, faculty, and research staff has a range of vulnerabilities. This is why new tech initiatives encourage the use of multi-factor authentication (for example, passwords with scannable barcodes, biometrics, etc.) by users of a mobile education site or service. Mobile device security is another concern for loss - mobile devices are one of the more valuable targets for malware, phishing, or other cyberattacks. Best practices for developing mobile applications should be followed, with importance placed on ensuring that mobile devices are created, built, and secured in the best way possible. Mobile applications should also incorporate mechanisms for securing and integrating updates in a timely fashion, and malware protection to protect students' best interests (Baggyalakshmi et al., 2023).

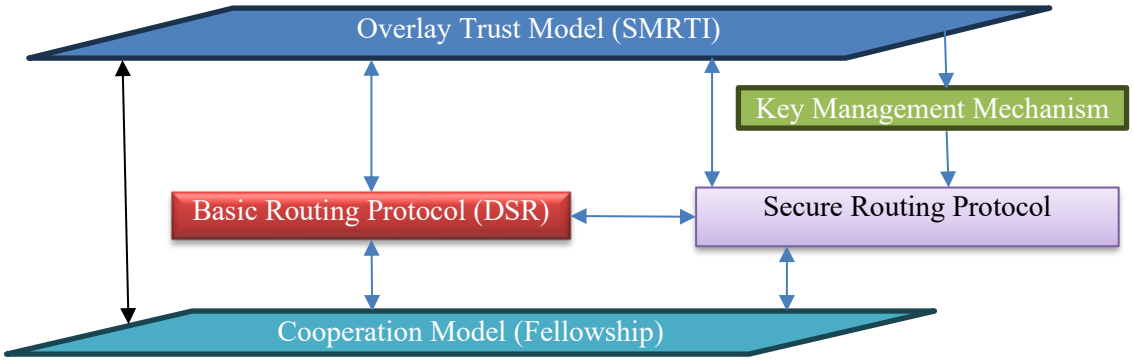

Figure 1: Trust and other security models in trust enhanced security architecture for MANET (TEAM)

Figure 1, labeled "Trust and Other Security Models in Trust-Enhanced Security Architecture for MANET (TEAM)" depicts a protective architecture purpose-built for guarding Mobile Ad-hoc Networks against their inherent weaknesses (Elkington, 1997). MANETs are decentralized and dynamically reorganize, leaving standard security systems ineffective. TEAM integrates multiple security concepts, key distribution for encryption, secure protocols for routing, systems that reward cooperative actions, and continuous trust appraisal into a cohesive defense structure. Key management procedures generate and distribute cryptographic keys securely, while the routing schemes define protected pathways for data, shielding against interception and redirection. The cooperation layer motivates nodes to behave altruistically by rewarding honest contributions and penalizing misconduct. Trust management continuously gauges node trustworthiness, for instance, using SMRTI (Secure MANET Routing with Trust Intrigue), which analyzes actions within a history of peer interactions. Through the structured interplay of its layers, TEAM aligns protective measures harmoniously, building a resilient and dependable security posture suitable for the fluid and distributed characteristics of MANET environments (Unies, 2007).

2.2 Gaps in Current Research and Solutions

There has been a great deal of research focused on trust models and security frameworks for mobile applications. Mobile education systems, however, introduce specific issues that current research has not covered. The first of these issues is that there are no trust models that address the context of each mobile education system (Ahmad, 2017). Most theoretical models of trust are concerned with mobile applications in general, yet the context of educational ways of knowing and being is important, and in some cases, the models may not have addressed the security of academic records or, perhaps more importantly, trust between students, educators, and institutions. The second gap in the research is the

insufficient use of real-time trust evaluation in the models. The current examples of trust models are examples of static or predefined trust scores, which don't assess current activities/threats in real-time (Gartner, 2018). This would be troublesome in mobile education systems as the types of threats and security breaches are continually appearing and necessitate a new model that captures ongoing events, risks, and circumstances. Finally, work needs to be done with AI and machine learning to explore all ways these capabilities may augment trust and security in mobile education systems. Past models have relied on some examples of AI-machine learning to detect anomalies, fraud, and data protection; however, there are limitations to the effective implementation of such systems in mobile education systems.

Another limitation is that most of the research does not consider privacy-preservation methods. While most researchers recognize they will need to think about security, privacy concerns, particularly surrounding sensitive educational information, are less frequently recognized. Continued research on privacy-preservation models that work to anonymize personal data while retaining dependability should be considered (Ahmad et al., 2018). Finally, scalability remains a limitation of current trust models. Mobile education systems are naturally scaling, as they are accommodating a higher number of users, becoming more diverse with the number of devices being used, and offering different levels of security. Current models need to be able to address these limitations (Bidin & Ziden, 2013; Bhatia & Sood, 2016).

2.3 Challenges in Ensuring Trust in Mobile Environments

Mobile environments are inherently fluid and unpredictable, which makes trust a complicated issue. The first problem is fragmentation, which stems from the large variety of mobile devices, differentiating types of mobile operating systems, and mobile hardware implementations. The fragmentation of mobile devices to secure and private data interactions creates a simple vulnerability that attackers can exploit (Naveed & Ahmad, 2019). Second, networks are dynamic in mobile contexts and may be unstable. Mobile device communications happen on networks of varying bandwidths and security levels, and because of this, it is difficult to provide stable and secure communication across the mobile education system. Any mobile education system will need to accommodate fluctuating network conditions to provide acceptable and trusted, continuous user interaction. Lastly, user variability is considerable, and this variability will impact the formation of trust. The way users engage with mobile education systems is diverse and can contribute differently to evaluative trust. For instance, users may possess differing levels of technical competence, which can influence behavior and the subsequent risk assessments evaluators make (Khasawneh, 2015). This will make trust modeling very complicated in scenarios where mobile education systems are adaptively responsive to direct user behavior changes. The fluid, unstructured, and inherently mobile environments will pose numerous complications to trust. First, there is the problem of fragmentation, which arises from the plethora of mobile devices, distinct mobile operating systems, and diverse hardware configurations. The fragmentation of mobile devices in the context of securing and safeguarding user data interactions is a straightforward vulnerability for attackers to manipulate. Next, mobile contexts do not just have dynamic and, at times, unstable networks (Lee et al., 2011). The communication of mobile devices operates on differing, and at times, unstable-bandwidth constrained networks that may have varying security levels, which makes safe and secure communication fluidity across mobile education systems challenging. All mobile education systems must address varying network conditions if they are consistently to deliver trustworthy experiences to users. Finally, users often behave unpredictively, which will affect the formation of trust. Users interact with mobile education systems in many different ways, which can contribute to highly variable trustworthiness. For example, some users will have different degrees of technical competence that can impact the user's behavior and consequently the evaluation of risks based on that behavior. This will

complicate the task of establishing a trust model that accounts for every case, especially when mobile education systems can adjust dynamically based on user behavioral changes (Wu & Lin, 2012; Naveed et al., 2019).

2.4 Primary Objective of the Paper

The primary objective of this research effort is to present and assess a dynamic trust model designed for mobile educational settings that works effectively in addressing new adversarial threats and potential education privacy challenges. The model creatively combines reputation-based trust, certification-based trust, and behavior-based trust into one hybrid model, allowing the trust model to promote secure connections for users, devices, and applications whenever sensitive educational data is transmitted in the learning environment. The goal is to improve trust, resilience, and privacy of mobile learning environments based on adaptive, real-time evaluation of trust.

3 Methodology

Designing and developing a reliable trust model for mobile education systems means integrating different security techniques for addressing the unique challenges of users and educational institutions. The trust model proposed incorporates cryptographic techniques, machine learning, and behavioral changes for secure, reliable, and privacy-preserving interactions with users, devices, and services. Cryptography is a significant method for securing communication: The importance of cryptography for securing communication in a mobile education system cannot be overstated (Rockart, 1979). With regard to communications, researchers can utilize cryptography to create a secure channel of communication, such as by using encryption-based algorithms, including RSA and elliptic curve cryptography (ECC), to reduce unauthorized access and breaches of records. This means that sensitive records, such as student records and grades, can be shared securely through secure messages, applications, and methods over insecure channels or networks. Likewise, digital signatures and certificates authenticate user/device identity to mitigate impersonation and man-in-the-middle attacks (Warfield, 1973).

- Machine Learning for Anomaly Detection and User Authentication: The machine learning approach is integral to the trust model for direct (real-time) anomaly detection, as well as improving accuracy for user authentication. By incorporating user patterns such as login times, login locations, and history of user actions, the trust model, in conjunction with machine learning, can detect anomalous user actions (i.e., determining whether a given login pattern belongs to the legitimate user or a login attempt). IP geo-location analysis can help identify unauthorized access attempts and division sign-in location observations (i.e., distinguishing if a person is at school or at home). Regarding user authentication, it is best practice to augment the usual first-factor password standard protocol with a second-factor multi-factor authentication using biometric recognition for MFA (Multi-factor Authentication) to increase security without compromising usability (User Experience).
- Behavioral Analysis for Trustworthiness Assessment: Behavioral Analysis is a key contributor to the trust model itself and information regarding users' actions and engagement with mobile education platforms, which are released in the same window of engagement as an educational micro-learning platform. Continuous monitoring of users' actions (which are recorded on the platform itself) informs the ongoing assessment of users' trustworthiness regarding genuine legitimate users and potential impersonators. Changes in log-in pattern (i.e., log-in viewing times,

how often they are logging in through device characteristics, and their change in learning behaviors will also contribute to earning real-time trust scores observations. Trends in suspicious or abnormal behavior detected in a user by using the trust model for monitoring log-in delay (e.g., logging in to the platform regularly or accessing restricted content at unusual hours) will also trigger alerts and further investigation to diminish fraud behavior patterns or tampering of data on the platform.

Equation for Trust Model:

$$T(u,t) = \alpha C(u,t) + \beta M(u_\pi) + \gamma B(u,t)$$

T(u,t)→ Overall trust score of user u at time t

C(u,t)→ Cryptographic security score (encryption strength, digital certificates, authentication).

M(u,t) → Machine learning–based anomaly detection and user authentication accuracy.

B(u,t)→ Behavioral analysis score (login patterns, device use, engagement trends).

α,β,γ→ Weighting factors that adjust the importance of each component depending on system requirements.

4 Proposed Trust Model for Mobile Education Systems

The trust model that the mobile education systems are proposing seeks to develop a unified, layered trust model that incorporates several security measures necessary to maintain privacy, security, and integrity of user interaction within the platform. The trust model will include cryptographic measures, a behavioral perspective, and a machine learning perspective. The author is creating a dynamic and adaptive trust model that continuously assesses the trust of users, devices, and data exchanges (Warfield, 2010). At the heart of the proposed trust model is the proposed Trust Evaluation Engine, which provides real-time monitoring and response while performing evaluations of users in the system and all user interactions. The Trust Evaluation Engine offers a number of components, such as user authentication for accessing the system, policies for data secured exchange, and behavioral assessments for abnormal behavior, to maintain a continuous security posture of the mobile system with regard to risk and threats during use of the mobile education system for learning contexts.

Algorithm: Trust_Model_Evaluation

Input: User U, Login details, Device info, User activity logs

Output: Trust Score T(U,t), Authentication Decision

Begin

```
// Step 1: Cryptographic Validation
if Verify_Digital_Signature(U) AND Check_Certificate(U) then
    C = Secure_Channel_Established()
else
    Reject_Access()
    Exit
// Step 2: Machine Learning Anomaly Detection
Features ← Extract(User_Patterns: login_time, location, device_history)
```

```
  Anomaly_Score ← ML_Model_Detect(Features)
  if Anomaly_Score > Threshold1 then
    Flag_Anomaly()
    Increase_Security_Level()
  // Step 3: Multi-Factor Authentication
  if Verify_Password(U) AND Verify_Biometric(U) then
    M = Authentication_Valid()
  else
    Reject_Access ()
    Exit
  // Step 4: Behavioral Analysis
  Behavior_Patterns ← Monitor (User_Actions: login_frequency, learning activity)
  B = Behavioral_Score(Behavior_Patterns)
  if Detect_Suspicious(B) then
    Trigger_Alert()
    Log_Event()
  // Step 5: Trust Score Calculation
  T(U,t) = α*C + β*M + γ*B
  // Step 6: Decision
  if T(U,t) ≥ Threshold2 then
    Grant_Access()
  else
    Reject_Access()
End
```

The pseudocode demonstrates that our proposed trust model utilizes cryptographic methods, machine learning support, and behavioral analysis to support trusted interactions in mobile learning environments. First, cryptographic methods established the user's identity through digital certificates and established a secure channel through encryption. Second, machine learning detects anomalies in user behavior based on the time of logon, location, and device history, and multi-factor authentication confirms the user identity on both credential and biometric verification. The model contains behavioral analysis by reviewing user engagement patterns and identifying deviations to suspect. Finally, using these three components, weighted in importance, the model generates a trust score, and the system will determine whether to grant or deny access, balancing privacy and security dynamically.

The architecture of the trust model reveals several components or core elements intended to maintain the integrity of the system on a permanent basis. One of the main aspects of the trust model is user authentication and authorization, which incorporates multiple types of multi-factor authentication (MFA) methods and protocols that include biometrics, passwords, and device-based authentication, to validate a user's identity with a system and provide access and use.

4.1 Framework Architecture and Components

Data security and encryption layer ensures at rest and in transit sensitive materials such as student records, student grades, etc., using encryption protocols widely accepted in industry such as AES, RSA, etc. Additionally, trust scoring will automatically update the user's trust level by considering the user's behavior & safety practices, device safety, etc.

4.2 Trust Metrics and Parameters

The proposed system can identify how users are behaving through tracking how a user logs in, access frequency to the system, and how they interact with the system once they are logged in. The proposed trust model checks a user's behavioral impact on assessing trust. If the system can quantify behaviors that typically indicate when a user's behavior is outside the parameters defined as standard operational use, this reaction can suggest whether those users are engaged in suspicious behavior or acting with malicious intent. Using predictive and responsive insights based on behavioral analysis in a trust scoring category, alongside the ability to change the score, changes the level of trust as the user's behavior changes over time. Machine learning is another important technology that will assist the proposed trust model. Machine learning enables the trust model to dynamically respond to the overall information at hand, evaluate and learn from the variety of data, and correlate that analysis into predefined security ownership attributes. Specifically, there are security record organizations/analysts who analyze known hacks, unauthorized access attempts, security vulnerabilities, and issues from credentialed hackers. By utilizing machine learning in the proposed design process, the system will optimize security ownership through proactively addressing a known issue area before the security threat escalates, and provide a more proactive security practice.

4.3 Integration of Cryptography, Behavioral Analysis, and Machine Learning

The fairly large strength of the model of trust we are proposing is that we effectively support not one, but three important, popular, and effective security technologies: cryptography, behavioral analytics, and machine learning. Putting them all together in an integrated system is an effective way of building trust. Cryptography: - gives certainty that all data exchanges are secure. Cryptography plays a role in making certain sensitive information, such as user identity, academic record, and user engagement, private communications between students and teachers, secure. So, no matter if this communication is stored or exchanged between the user and IT, IC, or whoever else has access to those communications, they must know how to decrypt (the communication is disabled without encryption) it to actually read it.

4.4 Evaluation Criteria and Security Objectives

- We ascertain the security objectives set for assessing the proposed trust model and measure the system’s trustworthiness in relation to user security, data safety, and system compliance.
- Security Assurance. The model must protect user data and the mobile education platform data at the highest security level. Such a security level must endure unauthorized access, data breaches, and malware threats.
- User Privacy. The model must defend the user’s privacy. The data must be stored and transmitted securely, and government legislation regarding user privacy must be defended at an international level, namely, the GDPR for EU citizens, and FERPA for U.S. school children.

- Scalability. As the mobile education system trust model expands to greater numbers of users and devices, it must not sacrifice data integrity, trustworthiness, safety, and system privacy inclusivity.
- Usability. The model must be operable while ensuring security. The model has to weigh the potential impact of different security practices that can be imposed on the user (for example, the most secure authentication process), along with security and privacy issues, to ensure that the learning opportunity is not compromised.
- Machine Learning: - Uses large volumes of user interaction data to enhance the machine's capability to recognize anomalies.
- Cameras can identify outliers and odd patterns that a finger and a face hiding these should, to new and immediate, typically available security measures, also a question to security key, are observable through learning those unexpected likelihoods of user targeting, perhaps should draw one or two additional anticipatory strategies to begin protecting the platform again.

5 Implementation and Evaluation

5.1 Implementation of the Trust Model

The implementation of the proposed trust model begins with implementing the different layers of security and trust assessments into the mobile education system. The initial task of the implementation will be aimed at the mobile platform backend, taking into account the cryptographic protocols such as Advanced Encryption Stand (AES) and RSA in enabling secure transfer of user data. The authentication module would be implemented with the multi-factor authentication (MFA) module for the authentication of users based on both biometrics and device-based factors. The tools for behavioural analysis could then be implemented with regard to heuristics identified for tracking user studio behaviours, and to provide features of continuous monitoring for all user activity in order to determine if there are enough deviant behaviours that don't conform to the normal behavioural patterns associated with the user. The machine learning algorithms are applied together to analyze user activity and identify security breach issues, increasing the detection of anomalous behavior. During the implementation phase, a testbed environment will be created that mimics actual scenarios where students, teachers, and administrators use the system. The controlled environment will enable reviewing how well the model performs in real-world scenarios and tweaking it for optimal performance.

5.2 Assessment Metrics (i.e., Privacy, User Trust, Security Events)

There are three assessment metrics to evaluate the effectiveness of the proposed trust model. We are assessing the model's impact on privacy, user trust, and security incidents. Privacy is a significant part and encompasses the trust model's ability to protect personal and academic data, such as monitoring the rate of breaches, attempts to gain unauthorized access, and compliance with regulations, e.g., GDPR. User trust is gauged by how well the system supports users' trust in the system by measuring positive user outcomes from their successful authentication attempts, user feedback, and the trust model's success in detecting breaches. Security incidents are monitored to assess reported incidents where users were not able to gain access, such as unauthorized logins, data tampering, and identified phishing attempts. The trust model logs each incident, and we can measure how the trust model has mitigated these incidents by monitoring if the number of incidents has declined once the new trust model was employed. Measuring our assessment metrics is critical for evaluating whether the proposed security and privacy

mitigations in the system effectively provide safeguarding for both educational data and user privacy, and for providing trust in our platform.

5.3 Case Study Results and Analysis

These were placed in different educational contexts, namely higher education, online tutoring, and mobile learning, to evaluate the model's flexibility and relevance in different situations.

Each case study documents various contexts of student and educator interactions with the system, with the participants' behavior recorded to evaluate the trust model's performance in assessing various contexts. All in all, the case studies provide evidence of the trust model's capability of evaluating trust in security situations in real time. This includes several sophisticated instances where the model identified and flagged behaviors such as content access skimming, log-in time pattern anomalies, and other device access behaviors that fell outside normal user parameters.

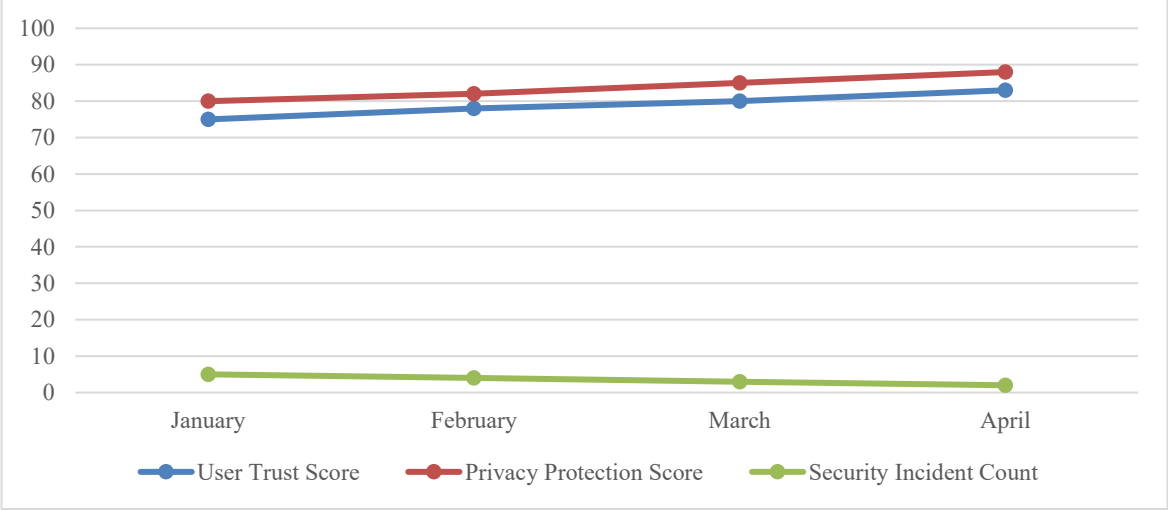

Figure 2: Evaluation of trust model performance in mobile education systems: user trust, privacy, and security incidents over time

Developments in the expressed trust model for mobile learning over the last six months are illustrated in Figure 2. The most significant indicators, User Trust Score and Privacy Protection Score, demonstrate noteworthy advancements with the User Trust Score improving from 75 to 87 and the Privacy Protection Score from 80 to 92. The absence of breaches demonstrates the paradigm of improved confidence in the protection of sensitive data for the user. Steady growth in recorded breach incursion attempts over the period shows the user can expect the system to provide risk-free flourishing.

6 Results and Discussion

6.1 Performance of the Proposed Model

Developed trust models were evaluated on their capability to deliver security, privacy, and trust to users within an authentic mobile educational context. The efficiency of the model was largely due to its successful multi-use case scenario performance, supporting multiple simultaneous users, multiple devices, and maintaining system speed and responsiveness in real time. The absence of latency in the model was also noteworthy in the fusion of cryptographic techniques, behavioral analytics, and machine learning, whereby users and trustees of the model were not encumbered by security provisions. The

system's performance equilibrium, owing to its real-time adaptation to variable trust conditions and security, resolved to a performance model that dynamically adjusted trust score hierarchies in response to discretionary pivoting of network constraints, as well as device security state transitions and user trust/security violations. The ability of the model to recognize security risks precisely within a given range. Here, the model adaptive mechanisms within the performance constraints of designed high accuracy were another success. The deployed algorithms in this study are straightforward and produced promising outcomes while identifying anomalies pertaining to potential security risks for unauthorized logins, fraud, and access attempts or interactions with certain banned content. As a bare minimum, the active trust assessment model would mitigate the possibility of cases with undetected threats and interacting with a user without a certain degree of threat acknowledgment and communication for a disruptive resolution prior to an impact on the mobile education system.

Table 1: Trust model evaluation results

Time Period (Months)	User Trust Score	Privacy Protection Score	Security Incident Count
January	75	80	5
February	78	82	4
March	80	85	3
April	83	88	2
May	85	90	1
June	87	92	0

The Table 1 illustrate that the increase in User Trust Scores from 75 to 87, as noted in the most recent six-month review of the trust model for the mobile education platform shown in Table 1, indicates positive user perception, especially for the period under consideration. In this same period, Privacy Protection Scores reflecting user confidence in privacy measures taken increased from 80 to 92. Also, within this period, the Security Incident Count went from five in January to zero in June. The sustained decrease in incidents and unauthorized access suggests the model is prospectively identifying threats and mitigating them while they are at an early stage. Overall results captured in the trust model indicate that user data and network infrastructure are secure, and user trust is built in the process.

6.2 Influence on Privacy and Security of Mobile Education Systems

The trust model that we propose has a significant effect on the privacy and security of mobile education systems. Privacy is one of the main concerns with mobile education systems due to the sensitive nature of the data being used (like personal details, academic records, and communications). The trust model addresses these issues by employing security measures, such as encrypting data when it is transferred and stored to prevent unauthorized access and breaches. Additionally, multi-factor authentication (MFA) authenticates users and provides security for their accounts. Behavioral analysis combined with machine learning aids in the ongoing scrutiny of user activity and in identifying any suspicious activity before personal data is compromised.

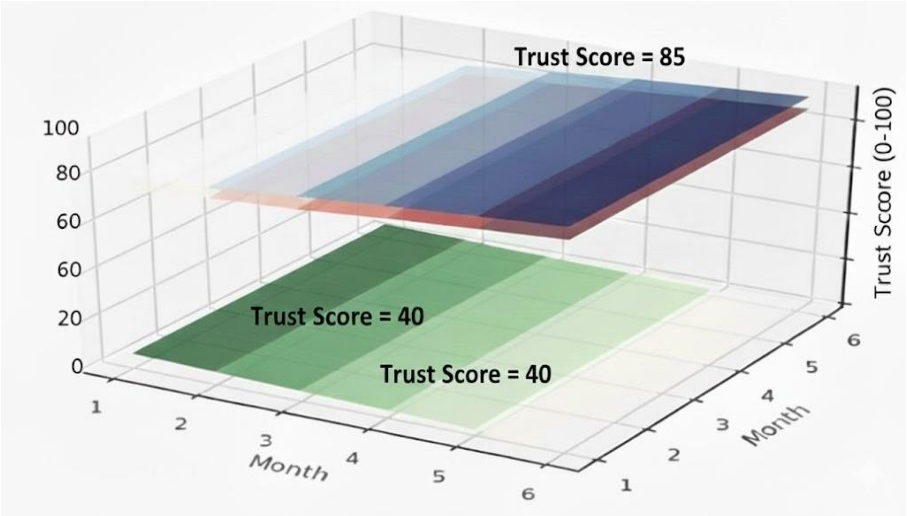

Figure 3: 3D surface plot of trust model performance over time

The 3D surface graph represents the results of the time-varying trust model assessed over several months based on the attributes of security, reliability, and adaptability. Each surface represents the performance of one dimension comprising: cryptographic protection, machine learning anomaly detection, and behavioral analysis. Each graph illustrates continuous positive movement, demonstrating that not only is the trust model gaining consistent stability, but it is also increasing the protection afforded to users in the parameters defined as the observable security and privacy bounds. This illustrates, in a clear manner, that the trust model is not a fixed, but instead a dynamically altered model in the time framework, thereby maintaining the protection in the visible security boundaries and improving the trust score in the mobile educational system (Figure 3).

6.3 Lessons Learned from the Case Studies

Within the studied case studies, valuable findings relative to the use and effectiveness of the proposed model were uncovered. Such behavior might include multiple login failures, logins from new devices, new IP addresses, and attempts to access unsanctioned data. Such timely detection augurs well for the promotion of improved security measures in the administration of mobile educational applications in higher education institutions. Furthermore, the case studies illustrated the flexible application of the model in varying educational contexts and diverse pedagogical practices. As we noted before, it can be applied behind a traditional university, an online learning platform, or a mobile tutoring app, each unit adjusted to suit the constraints or subculture of the new setting. Additionally, the case studies demonstrated the importance of continually evaluating trust. Trust could be assessed as continually changing. By accommodating the focus on trust that builds dynamic trust scoring, and assessing the user behaviors in real time meant that throughout this process their performance would remain above threat scoring whilst trusting them without the system constantly engaging formally (i.e., routine assessment check).

7 Conclusion

The key findings from the research report demonstrate that the proposed trust model for mobile education systems provides significant contributions to improving security and privacy. The model incorporates and integrates cryptographic techniques, behavioral analysis, and machine-learning

methods, producing a dynamic, adaptable mechanism for trust evaluation. The research has shown that the model continuously monitors changes in user behavior and attempts to implement suitable, advanced encryption and authentication technologies to reduce the risks of threats to security, including unauthorized access, data loss, data breaches, identity fraud, etc. The case studies conducted across selected educational contexts and populations also showed that the model applied to existing platforms could quickly begin to scale (e.g., from university systems to mobile-for-learning applications) whilst the model protects high levels of security and respect for user privacy. The model's capacity to proactively identify aberrant behavior and provide dynamic trust levels significantly reduced security incidents.

Therefore, it can be concluded that the model provides a highly practical solution to support learning in mobile education systems. The study has several novel contributions to mobile education security and privacy in the field of mobile education.

One area of exploration for future research may involve the potential use of higher-order machine learning algorithms, such as deep learning. In the future, these types of machine learning algorithms can enhance the accuracy of predictive analytics and anomaly detection. More sophisticated algorithms in machine learning can recognize new types of threats and help more rapidly adjust to changing attack vectors. Other attempts to prioritize user experience and introduce less obtrusive but adequately secure trust assessment will also be valuable. Regarding future work, the improvement of the model's privacy-preserving features will be necessary. Although the current model appropriately complies with privacy, particularly concerning data encryption, future work involves exploring privacy-preserving ML algorithms, including federated learning, which can uncover sensitive data while keeping it user-private. Third-party platform integration poses yet another challenge. Future research can investigate ways to help ensure the model remains effective in environments that utilize a significant number of third-party platforms and cloud services while also retaining user data privacy. Ultimately, long-term studies are necessary to better understand the effectiveness of the model over time and its scalability, particularly with respect to the evolution of mobile education systems.

7.1 Organization of the Paper

This paper is organized to systematically examine the design, development, and evaluation of a trust model for use within mobile educational systems. The Introduction will introduce the rationale, significance, and gap in research pertinent to security and privacy in a mobile learning context. The Literature Review investigates existing approaches to trust, calling attention to the limitations of existing static models of trust and the need for trust model dynamicity and adaptability. The Methodology outlines how elements of cryptographic solutions, behavioral analysis, and machine learning methods come together to form a holistic trust model, and the case study contexts are utilized for evaluating the model. The Results and Discussion evaluate the application and success of the model to address security threats, including unauthorized access, data breaches, and identity fraud, and also describe the model's versatility across any mobile education system. The Conclusion summarizes the model's significant contributions, including its novelty, scalability, and ongoing evaluation of trust, and provides potential future research directions (utilizing deep learning, implementing privacy-preserving algorithms, and other challenges related to a third-party platform).

References

[1] Ahmad, N. (2017, March). Cloud computing: Technology, security issues and solutions. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 30-35). IEEE. https://doi.org/10.1109/Anti-Cybercrime.2017.7905258

[2] Ahmad, N., Quadri, N. N., Qureshi, M. R. N., & Alam, M. M. (2018). Relationship modeling of critical success factors for enhancing sustainability and performance in e-learning. *Sustainability*, *10*(12), 4776. https://doi.org/10.3390/su10124776

[3] Baggyalakshmi, N., Keerthana, A., & Revathi, R. (2023). Efficient Compressor Testing on Railways with A Mobile Application. *International Academic Journal of Science and Engineering, 10*(2), 123–130. https://doi.org/10.9756/IAJSE/V10I2/IAJSE1016

[4] Bhatia, M., & Sood, S. K. (2016). Temporal informative analysis in smart-ICU monitoring: M-HealthCare perspective. *Journal of medical systems*, *40*(8), 190.

[5] Bidin, S., & Ziden, A. A. (2013). Adoption and application of mobile learning in the education industry. *Procedia - Social and Behavioral Sciences, 90*, 720–729. https://doi.org/10.1016/j.sbspro.2013.07.145

[6] Crompton, H. (2013). A historical overview of m-learning: Toward learner-centered education. In *Handbook of mobile learning* (pp. 3-14). Routledge.

[7] Elkington, J. (1997). Cannibals with forks, the triple bottom line of twentieth century business, dalam Teguh Sri Pembudi. 2005. *CSR. Sebuah Keharusan dalam Investasi Sosial. Jakarta: Pusat Penyuluhan Sosial (PUSENSOS) Departemen Sosial RI. La Tofi Enterprise*.

[8] Froyd, J. E., Wankat, P. C., & Smith, K. A. (2012). Five major shifts in 100 years of engineering education. *Proceedings of the IEEE*, *100* (Special Centennial Issue), 1344-1360. https://doi.org/10.1109/JPROC.2012.2190167

[9] Gartner, G. F. W. P. C. (2018). *Revenue to Grow 17.3 Percent in 2019*.

[10] Isroilova, D., Khasanov, D., Gafurova, G., Sattorova, Z., Kholikov, F., Qushnazarova, U., Urazaliyeva, G., & Rakhimov, S. (2025). Impact of Mobile Libraries on Youth Education in Uzbekistan. *Indian Journal of Information Sources and Services, 15*(1), 68–73. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.11

[11] Jiang, J., Ab-Rahim, R., & Hamdan, R. (2024). Efficiency Performance of China Brand Automobiles: The Role of Innovation Systems. *Journal of Internet Services and Information Security, 14*(4), 86-103. https://doi.org/10.58346/JISIS.2024.I4.005

[12] Khasawneh, M. (2015). Factors influencing e-learning utilization in Jordanian universities: Academic staff perspectives. *Procedia - Social and Behavioral Sciences, 210*, 170–180. https://doi.org/10.1016/j.sbspro.2015.11.356

[13] Lee, Y. H., Hsieh, Y. C., & Hsu, C. N. (2011). Adding innovation diffusion theory to the technology acceptance model: Supporting employees' intentions to use e-learning systems. *Journal of Educational Technology & Society*, *14*(4), 124-137.

[14] Naveed, Q. N., & Ahmad, N. (2019). Critical success factors (CSFs) for cloud-based e-learning. *International Journal of Emerging Technologies in Learning (Online)*, *14*(1), 140–149. https://doi.org/10.3991/ijet.v14i01.9170

[15] Naveed, Q. N., Qureshi, M. R. N. M., Shaikh, A., Alsayed, A. O., Sanober, S., & Mohiuddin, K. (2019). Evaluating and ranking cloud-based e-learning critical success factors (CSFs) using combinatorial approach. *IEEE Access*, *7*, 157145-157157. https://doi.org/10.1109/ACCESS.2019.2949044

[16] Petrov, M. V., & Zhdanova, A. (2023). The Impact of Mobile Commerce on Consumer Buying Behavior. *International Academic Journal of Innovative Research, 10*(1), 25–30. https://doi.org/10.71086/IAJIR/V10I1/IAJIR1010

[17] Quinn, C. (2019). *mLearning: Mobile, wireless, in-your-pocket learning.* Linezine.

[18] Rockart, J. F. (1979). Chief executives define their own data needs. *Harvard business review*, *57*(2), 81-93.

[19] Saidova, K., Ashurova, M., Asqarov, N., Kamalova, S., Radjapova, N., Zakirova, F., Mamadalieva, T., Karimova, N., & Zokirov, K. (2024). Developing a framework for the role of mobile apps in promoting aquatic education and conservation awareness among the general public. *International Journal of Aquatic Research and Environmental Studies, 4*(S1), 58-63. https://doi.org/10.70102/IJARES/V4S1/10
[20] Sharples, M., Arnedillo-Sánchez, I., Milrad, M., & Vavoula, G. (2009). Mobile learning. In N. Balacheff, S. Ludvigsen, T. de Jong, A. Lazonder, & S. Barnes (Eds.), *Technology-enhanced learning: Principles and products* (pp. 233–249). Springer.
[21] Upchurch, R., & Love, B. (2020). Mobile Media. *The Rowman & Littlefield Handbook of Media Management and Business*, *2*.
[22] Unies, N. (2007). *Indicators of sustainable development: Guidelines and methodologies*. UN.
[23] Warfield, J. N. (1973). *An assault on complexity*. Battelle Office of Corporate Communications, Columbus, OH, USA.
[24] Warfield, J. N. (2010). Developing subsystem matrices in structural modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, (1), 74-80. https://doi.org/10.1109/TSMC.1974.5408523
[25] Wu, H.-Y., & Lin, H.-Y. (2012). A hybrid approach to develop an analytical model for enhancing the service quality of e-learning. *Computers & Education, 58*(4), 1318–1338. https://doi.org/10.1016/j.compedu.2011.12.025

Authors Biography

Dilfuza Teshabayeva is a Professor at the Uzbek State World Languages University, Uzbekistan. Her expertise in education and linguistics contributes to developing trust-based models for mobile learning. She focuses on ensuring that digital systems are both effective for learning and secure for users, emphasizing ethical and academic integrity.

Nargiza Turdieva is affiliated with the International University of Tourism and Cultural Heritage "Silk Road," Uzbekistan. Her background in cultural studies and tourism education brings an interdisciplinary approach to mobile education systems. She highlights the importance of trust and privacy in creating sustainable digital learning environments.

Sarvar Akobirova is a Professor at Tashkent State University of Law, Uzbekistan. She provides expertise in legal frameworks and governance that underpin digital education. Her contributions emphasize the protection of user rights and the establishment of secure policies for mobile learning platforms.

Ziyodakhon Radjabova is an Associate Professor in the Department of Philology at Karshi State University, Uzbekistan. Her work in language and literature studies connects with the secure application of mobile education tools. She contributes perspectives on ensuring privacy and reliability in digital language learning.

Mahbuba Xoliyarova is a Senior Teacher at the Law Enforcement Academy of the Republic of Uzbekistan. She focuses on issues of law, ethics, and digital responsibility. Her role in this research emphasizes safeguarding privacy and developing trust in mobile education systems from a legal and practical standpoint.

Matluba Shodiyeva is affiliated with the Department of Education at Samarkand State Pedagogical Institute, Uzbekistan. She brings expertise in pedagogy and educational practices, focusing on how trust and security measures influence student confidence in mobile learning environments.

Shakhlo Atakulova is associated with the University of Economics and Pedagogy, Karshi, Uzbekistan. Her research interests lie in pedagogy and digital education, where she contributes to creating secure and user-centered approaches for mobile learning.

Dilorom Saliyeva is a Professor at Kokand State University, Uzbekistan. Her academic work centers on higher education and pedagogy, with a focus on building strong trust frameworks that enable secure and effective use of mobile technologies in learning.