



Security and Privacy Challenges in Virtual Classroom Platforms

Ms.Swati Mishra¹, Dr.Kavita Mittal²

¹Research Scholar, Department of Computer Science & Engineering, Jagannath University, Delhi NCR, Bahadurgarh.

²Professor & Research Supervisor, Department of Computer Science & Engineering, Jagannath University, Delhi NCR, Bahadurgarh.

Abstract- The scale of online virtual learning has grown rapidly, and various educational institutions are increasingly reliant on tools such as learning management systems, cloud services, web applications, and video conferencing platforms. These tools must process a large volume of sensitive information that cannot be disclosed casually, including education-related teaching data as well as the personal privacy information of teachers and students. This places extremely high security and privacy requirements on the entire virtual learning environment; if protection is insufficient, this information is highly vulnerable to leakage or tampering. Previous studies have identified authentication, access control, data integrity, content protection, encryption technology, and network security as core security concerns for online learning platforms [1]. Authentication confirms that the person logging into the system is the legitimate account holder; access control limits the scope of content that different users can view and operate on; data integrity ensures that information cannot be arbitrarily altered; content protection prevents course resources from being misappropriated and distributed; encryption technology and network security block vulnerabilities in data transmission and storage at the technical level. In recent years, systematic studies have specifically analyzed the cybersecurity issues faced by mainstream platforms including Moodle, Blackboard, and Microsoft Teams [2]. This framework integrates multi-factor authentication, Role-Based Access Control and Attribute-Based Access Control, secure communication, privacy-compliant data management, session monitoring, and security auditing functions. Its core goal is to build an extensible conceptual foundation that embeds security and privacy protection into every layer of the architecture, provide support for constructing reliable virtual classroom environments, and promote the responsible development of such environments.

Keywords- Virtual Classroom, E-Learning, Cybersecurity, Privacy, Authentication, Access Control, Encryption, Secure Architecture, Online Learning.



I. INTRODUCTION

In recent years, internet tools to support online teaching have become increasingly widespread, and the way teaching and learning is conducted has been completely transformed for educational institutions of all sizes, from primary and secondary schools to universities. The resulting virtual classroom is the most typical product: in this online learning space, teachers and students can join remote classes without gathering in the same physical classroom, interact with each other via the platform's built-in digital functions, access learning materials stored on the platform at any time, and complete all teaching assessments such as regular assignments, midterm, and final exams on the platform.

However, this shift from tangible offline traditional classrooms to an online teaching environment entirely connected by networks has also brought a set of new security requirements that did not need to be considered before. Scholar Aljawarneh once proposed that all online learning platforms must prioritize six core security tasks: authentication, access control, data integrity, content protection, cryptography, and network protocols [1]. These requirements remain relevant today and have always been a focus of the industry, for a simple reason: the large volume of information processed by educational platforms can only be accessed by authorized users who are qualified to view it, and these requirements are necessary to enforce this rule.

Two other scholars, Pillajo-Garcia and Avila-Pesantez, conducted a systematic literature review to sort out the cybersecurity issues of several commonly used online teaching platforms: Moodle, Blackboard, and Microsoft Teams. They explicitly recorded in their study that these tools used for daily online classes store and transmit various types of sensitive information, including users' personal data, academic grades, various exam results, and the school's official academic documents [2]. The two authors also noted that to reduce the risk of cyberattacks and information leakage in online learning environments, four types of protective measures are practically effective: encrypting stored and transmitted data, implementing strong authentication that is harder to breach than a single password, regularly updating software to patch platform vulnerabilities, and establishing clear formal security rules in advance [2].

In addition to security, there is another requirement closely tied to security but entirely independent: privacy. Scholars Kularski and Martin compiled a systematic review of 41 studies specifically discussing the online privacy of college students. Their analysis found that most of the relevant available studies at that time focused on how users themselves should protect their privacy, and very few seriously explored the fact that the online collaboration tools commonly used for online classes may themselves pose privacy risks [3]. This unaddressed gap is particularly noteworthy in the context of virtual classrooms, because the core of virtual classrooms' ability to support simultaneous online synchronous teaching relies on these collaboration and communication tools. If the privacy risks of the tools themselves are not taken seriously, it leaves a major gap in the privacy protection of the entire teaching scenario.

The first security checkpoint a user must pass to log into an online learning system is authentication, which is the first line of security for the system to start. Most current platforms use password authentication, the most widespread method, but stricter authentication mechanisms can block many potential risks. Banes et al. once designed a two-factor authentication scheme for the Moodle online learning platform, specifically proposing that additional verification mechanisms must be added to strengthen the access security barrier [4].



Beyond the initial authentication, the communication security in virtual classrooms also cannot be taken lightly. During online classes, video conferencing platforms must transmit a large amount of content: users' audio, camera video, chat text, shared screen content, and other types of information. All of this content must be protected during transmission. Isobe and Ito specifically analyzed Zoom's end-to-end encryption mechanism and conducted a full security assessment of the encryption protocols it uses [5]. Their study clarified a key point: to judge whether a real-time communication system is secure, one cannot rest assured just by checking if the platform has an encryption function; the core design of the underlying encryption must be disassembled and thoroughly inspected.

When the class process is completed and online exams are used, new security issues emerge that must be addressed. Garg and Goel conducted a systematic literature review of online exam security, covering academic misconduct, various cheating methods, complete strategies to ensure the credibility and availability of exams, and the role of machine learning in maintaining online exam integrity [6].

Combining these previous studies reveals that the security of virtual learning is never a problem of a single isolated link, but a complex issue that involves all aspects—from initial authentication and authorized access, to communication security during transmission, to user privacy protection and security of various types of data, and finally to the content authenticity of online exams. No link can be omitted. Therefore, a truly effective virtual classroom architecture must integrate multiple security mechanisms; it cannot rely on a single security measure to withstand all security risks.

II. PROBLEM STATEMENT

Virtual classroom platforms used for online classes must simultaneously connect to several distinct types of users—such as attending students, teaching teachers, and system operation and maintenance administrators, as well as host a wide range of teaching functions. In addition, they must connect to a diverse array of access devices, communication channels for transmitting information, and all teaching and personal data resources stored on the platform. Existing relevant academic studies have each independently examined the effectiveness of a single type of security protection mechanism, such as authentication, access control, encryption, privacy protection, and online assessment security [1]–[6].

However, these separately studied security mechanisms have never been integrated into a single unified system architecture, so they cannot operate in tandem to bring into play their effects. To take the most straightforward example: more robust authentication can indeed protect a user's account from being accessed and stolen by strangers, but relying solely on the authentication mechanism cannot determine which resources and functions the legitimate user who has successfully passed the identity check is permitted to access on the platform. Similarly, encrypting transmitted content can indeed prevent communication content from being intercepted and viewed by outsiders during transit, but relying solely on the encryption mechanism cannot stop a user who has legitimate account permissions from exceeding their authority to access information they should not be exposed to.

Consequently, the central problem addressed by this study is:

Current online virtual classrooms must not only support the simultaneous access of a growing number of teachers and students, but also have the flexible ability to add new features—the scalable architecture that is commonly mentioned. The question is how to embed the full set of security and privacy protection mechanisms into this architecture while upholding several bottom lines: ensuring sufficient security protection strength and privacy protection levels, not sacrificing protection for compatibility and scalability; not slowing down the platform's operation speed due to the addition of too many



protection measures; and ensuring that all teachers and students can use the platform smoothly, without being unable to attend classes normally due to overly complex protection processes.

Research Objectives

The objectives of this study are:

The core of this study focuses on the security and privacy issues of virtual classroom platforms, and completes five specific tasks in sequence:

- The first task is to sort out the main security and privacy challenges affecting virtual classroom platforms, first organizing all relevant current problems encountered by these online teaching platforms, as the basic direction for the entire study.
- The second task is to compile existing research on authentication, authorization, encryption, privacy, and security monitoring in online learning environments, summarizing all previous academic research achievements in these segmented protection directions, to clarify the current research accumulation in the field.
- The third task is to compare various existing security schemes from the dimensions of security, privacy, scalability, performance, and usability, comparing each previously proposed security protection mechanism against these five core standards to clarify the advantages and disadvantages of different schemes.
- The fourth task is to identify unaddressed research gaps in existing virtual classroom security schemes, and explore the core unsolved problems in the current field on the basis of organization and comparison.
- The fifth and final task is to propose a layered architecture that can support the operation of large-scale virtual classrooms, while implementing security and privacy protection, integrating various protection capabilities into this layered design to solve the various problems sorted out earlier, and support the stable simultaneous use of virtual classrooms by more users.

Research Questions

The following research questions guide the study:

This study is guided by four core research questions that progress layer by layer, gradually deriving the core direction the study needs to solve:

- RQ1: What core security and privacy challenges impact virtual classroom platforms?
- RQ2: What security mechanisms have been proposed to protect online learning environments?
- RQ3: What limitations exist in current authentication, authorization, encryption, and privacy protection schemes, respectively?
- RQ4: How can various security and privacy mechanisms be integrated into a virtual classroom architecture that supports large-scale scalability?

III. RELATED WORK

1. Security in E-Learning Platforms

Security in E-Learning Platforms has long been recognized as a core requirement. Early in the academic community's widespread research on security issues in online teaching scenarios, Aljawarneh conducted research on information security in online learning environments, identifying authentication, access control, data integrity, content protection, encryption technology, and network protocols as core areas that online platforms need to focus on [1].



Later, more recent systematic studies have repeatedly confirmed the importance of cybersecurity protection for these platforms. Pillajo-Garcia and Avila-Pesantez compiled a systematic literature review, sorting out all cybersecurity research published between 2016 and 2022 related to the three commonly used online teaching platforms Moodle, Blackboard, and Microsoft Teams [2]. In their study, they organized various cybersecurity vulnerabilities existing in these platforms and proposed implementable countermeasures, specifically including data encryption, upgraded authentication mechanisms, timely software patch updates for the platform, and the development of comprehensive platform security usage rules [2].

Combining the conclusions of these previous studies reveals that security considerations must be embedded into every link from the initial design phase of online learning platforms to the entire long-term daily operation process after launch, with no omissions allowed.

2. Student Privacy

To manage an online education platform, one must handle two core types of content: one is students' personal information, and the other is all students' interaction records on the platform. Both types of content are tied to personal privacy, so student privacy protection has been an unavoidable core issue in platform construction and operation from the start.

Kularski and Martin specifically sorted out 41 studies related to the online privacy of college students [3], conducting a systematic review and analysis. After organizing the studies, they found that the vast majority of existing research focused on what users themselves need to do to protect their privacy, and very few paid attention to the fact that the online tools used for collaboration during classes may themselves pose privacy risks, let alone research that treats these tools as independent privacy hazards [3].

This finding exactly points out a gap in previous privacy research: that is, future privacy research cannot only focus on user behavior, but must also include various technologies that support the operation of synchronous virtual classrooms in the scope of investigation, including the real-time communication systems and shared collaboration systems used in classes, all of which must be thoroughly inspected.

3. Authentication

Anyone who wants to log into an online system to use its functions must first pass the first security checkpoint: authentication, whose core is to confirm that the person attempting to log in is indeed a legitimate authorized user permitted to use the system.

Banes et al. once designed a two-factor authentication scheme for Moodle to improve access security [4], and their study confirmed the feasibility of adding an additional verification step in online teaching environments.

Multi-factor authentication can be integrated as a component of a secure virtual classroom architecture. However, when selecting specific authentication mechanisms, usability, deployment difficulty, and the characteristics of the user group using the platform must also be taken into account.

4. Access Control

Authentication and authorization are two completely independent security functions.

The former confirms who the user logging into the system is. The latter governs which resources the authenticated user can access and which operations they can perform.



Role-Based Access Control (RBAC) predefines user identity roles, then assigns corresponding permissions to different roles. Ferraiolo and Kuhn first proposed this RBAC model, classifying it as a type of non-discretionary access control—permissions are first bound to roles, instead of being assigned to each user individually [7].

This model was later specifically applied to educational systems. Wang proposed a permission control scheme adapted to web-based online learning systems, assigning different access permissions to different educational practitioner roles such as lecturers, students, and administrators [8].

If some scenarios require more flexible permission judgments based on specific circumstances, Attribute-Based Access Control (ABAC) can be applied. Its permission judgment evaluates user attributes, the attributes of the resource being accessed, the attributes of the operation to be performed, and the current environmental conditions together [9].

From this perspective, virtual classrooms can fully combine role-based and attribute-based permission rules, which can both meet simple permission allocation requirements and support complex permission judgments that require scenario-based evaluation.

5. Communication Security and Encryption

The core of supporting virtual classrooms is real-time communication between teachers and students—whether it is the audio and video of classes, chat text, shared screens, or courseware, all rely on real-time transmission to function. The video conferencing systems that support this communication must be protected by specialized technical mechanisms, to maintain the confidentiality of all content, preventing unrelated people from intercepting information mid-transmission, and also to maintain the integrity of the content, preventing it from being tampered with by anyone.

Isobe and Ito once specifically analyzed the end-to-end encryption protocol used by Zoom and evaluated the security of this encryption algorithm [5]. Their study highlighted a key point that is easily overlooked: to achieve communication security, one cannot only check "whether encryption is implemented"; the specific implementation of this encryption mechanism and the underlying protocol design must all be carefully evaluated and inspected, which is crucial for protecting the security of virtual classrooms.

This means that to ensure the communication security of virtual classrooms, encryption cannot be used as an isolated protective measure. It must be considered together with authentication, permission allocation, key management, and session security, and implemented in a unified, comprehensive manner.

6. Online Assessment Security

The popularization of online exams has brought unique new problems to various educational institutions: not only must the platform's security barriers be maintained, but the authenticity of the exams themselves must also be preserved, as risks cannot be contained within a single classroom as in offline proctoring. Garg and Goel conducted a systematic literature review of the field of Online Assessment Security, covering relevant studies published between 2016 and 2021 [6]. When organizing these studies, they divided the content into four categories: the first is why students cheat in online exams, the second is the various practical methods they use to cheat, the third is the prevention and control strategies that have been proposed to maintain exam authenticity, and the fourth is how technologies such as machine learning play a role in these prevention and control strategies [6]. A clear conclusion can be drawn from these aggregated studies: to build a usable, comprehensive virtual



learning security framework, one cannot only focus on the security of teacher-student communication and content transmission in the classroom; all exam-related activities, from candidate identity verification, Answer the questions process monitoring to exam paper collection and storage, must be included in the protection scope, with no gaps left.

Security and Privacy Threats in Virtual Classrooms

After organizing and summarizing all relevant literature reviewed in this study, we compiled all the security and privacy issues that virtual classrooms may encounter, as mentioned in these documents. The most core of these security and privacy risks can be categorized as follows.

Threat/Challenge	Potential Consequence	Possible Security Control
Weak authentication	Account compromise	Multi-factor authentication
Unauthorized access	Classroom/data exposure	Authentication and authorization
Excessive permissions	Unauthorized resource access	RBAC/ABAC
Insecure communication	Information disclosure	Secure communication/encryption
Data exposure	Privacy violation	Encryption and access control
Insecure configuration	Platform vulnerability	Security configuration and auditing
Compromised sessions	User impersonation	Secure session management
Assessment dishonesty	Reduced assessment integrity	Assessment security controls
Excessive data collection	Privacy risk	Data minimization
Suspicious activity	Security incidents	Monitoring and auditing

The categorization we have just summarized is not arbitrarily compiled; it integrates all the core issues discussed in the relevant literature included in this study's analysis. These documents cover the research directions of online learning security, privacy protection, authentication, communication security, and online assessment, with their citations marked as [1]–[6].

Comparative Analysis of Security Mechanisms

Mechanism	Primary Function	Strength	Limitation
Password authentication	Identity verification	Simple deployment	Vulnerable to credential compromise
Multi-factor authentication	Stronger identity verification	Adds authentication factor	Additional usability/deployment requirement

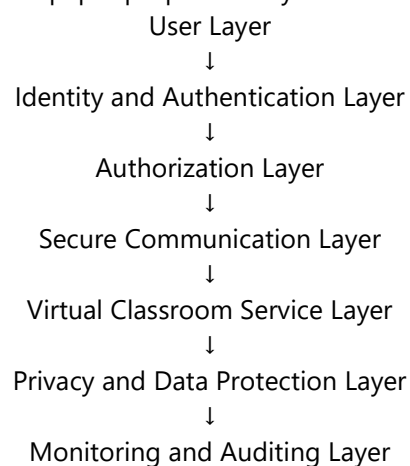


Mechanism	Primary Function	Strength	Limitation
RBAC	Role-based authorization	Simple permission administration	Limited contextual flexibility
ABAC	Context-aware authorization	Fine-grained policies	More complex policy management
Encryption	Data confidentiality	Protects communication/data	Does not itself establish user authorization
E2EE	Communication confidentiality	Reduces intermediary access to content	Requires careful key and protocol management
Session monitoring	Detect unusual activity	Provides continuous visibility	Requires monitoring infrastructure
Audit logging	Accountability	Supports investigation	Logs must themselves be protected

RBAC and ABAC are established access-control approaches [7], [9], while e-learning research demonstrates their relevance to educational systems [8]. Authentication and encryption mechanisms have also been studied specifically in Moodle and Zoom environments [4], [5].

Proposed Secure and Privacy-Preserving Architecture

Based on the reviewed literature, this paper proposes a layered architecture consisting of:



This architecture is only a conceptual framework proposed by this study; in other words, it is a feasible design idea compiled after organizing all relevant requirements, and is not an implemented, usable system. Before prototype development and relevant evaluation are completed, it cannot be introduced as an experimentally validated architecture—that is, this design idea must first be built into a testable version that can actually run, and then its core indicators such as security effectiveness and operational stability must be tested through various assessments. Only after completing these processes can it be proven that the architecture's actual performance meets our design expectations.



User Layer

This layer is the User Layer, which includes all people who can access the platform. The specific entities covered include students, teachers, administrators, and all other authorized participants.

These legitimate users can access the platform in two common ways: they can log in via a web browser on a computer, or enter the platform through a mobile application to use relevant functions.

Identity and Authentication Layer

The task of this layer is simple: before granting any user access to the platform and allowing them to enter the virtual classroom to use its resources, it first verifies the user's identity, confirms that they are the legitimate user of the account, and then grants access.

The proposed architecture can support:

- password authentication;
- multi-factor authentication;
- secure authentication tokens;
- session verification;
- device/session management.

The multi-factor authentication to be added to the Identity and Authentication Layer mentioned earlier already has research backing. Studies on stronger authentication schemes specifically for the Moodle platform have explicitly supported the integration of this mechanism [4].

Authorization Layer

After a user successfully passes the previous authentication step and is confirmed as the legitimate user of the account, they enter the verification process of the Authorization Layer. The task of this layer is clear: to confirm which functions the logged-in user can operate and which platform resources they can access, preventing anyone from exceeding their authority to access content they should not touch.

Two mature mechanisms are used in this permission allocation: RBAC assigns corresponding permissions based on the user's role; for example, teachers, students, and administrators each receive operation permissions matching their identity. ABAC, on top of roles, can additionally evaluate more scenario attributes to define more granular access rules.

For example:

Student + enrolled course + permitted classroom + join request → Allow

whereas:

Student + administrative configuration + modification request → Deny

This permission control scheme first uses a role-based authorization logic, and the selection of this scheme is consistent with existing RBAC research [7] and the conclusions of previous educational access control studies [8]. In addition to this core authorization scheme, the ABAC mechanism is also added, which can provide additional context-aware authorization capabilities [9].

Secure Communication Layer

The layer we are introducing now is the Secure Communication Layer in the seven-layer architecture. Its core role is to specifically protect the communication security between all users and the classroom services. Whether it is chat content sent by a user, camera footage transmitted, or courseware resources to be retrieved, all information sent from the user's device to the platform's classroom server, or



returned from the server to the user's device, is protected by this layer, preventing problems during transmission.

Potential controls include:

- secure network communication;
- authenticated APIs;
- secure session tokens;
- cryptographic protection of appropriate communication;
- secure key-management mechanisms.

The real-time communication tools we use, such as video conferencing, transmit content like class chats, microphone and camera activation, and screen sharing. The security of this content cannot be taken for granted just because providers claim to have encryption; it must be thoroughly and comprehensively evaluated. This necessity is supported by concrete research: a previous study that conducted a specific security analysis of Zoom's E2EE protocol can corroborate the reasonableness of this requirement [5].

Virtual Classroom Service Layer

This layer provides the educational services, including:

- audio/video communication;
- text chat;
- screen sharing;
- file sharing;
- digital whiteboard;
- attendance;
- classroom recording;
- assessment services.

Every educational service used for classes mentioned here must first be equipped with appropriate authorization rules, and all operations must follow these rules; no one can access them arbitrarily. In simple terms, rules must be established for each function, defining who can use it and to what extent, and no one can exceed these boundaries.

Privacy and Data Protection Layer

In the layered architecture we mentioned earlier, the layer responsible for privacy and data protection manages all links related to user information. From when the platform collects a user's information, where the collected information is stored and how it is stored, how it is processed compliantly during daily use, to when the user's information is shared with authorized viewers, every step from start to finish is uniformly managed by this layer, with no link left unmanaged.

Possible controls include:

- data minimization;
- restricted access;
- encryption;
- appropriate retention policies;
- controlled data sharing;
- secure deletion.



Privacy protection is an unavoidable issue for online higher education, and the importance of this issue is not arbitrarily raised. The systematic review completed by Kularski and Martin [3] provides solid research support for this view.

Monitoring and Auditing Layer

This layer is the last line of defense in the entire security architecture, the Monitoring and Auditing Layer. It records all security-related events and supports the detection of abnormal behavior. All operations on the platform are truthfully recorded by this layer, and any security-related movement is not missed. With these complete records, it can also help the system identify unusual operations and detect risks early.

Potential events include:

- repeated failed login attempts;
- unusual authentication behavior;
- repeated authorization failures;
- unusual session activity;
- access to sensitive resources.

These recorded audit logs can be used for troubleshooting and source tracing to support security investigations if a security incident occurs in the future, and can also serve as a reliable basis to support the entire process of responsibility definition when it is necessary to clarify relevant liabilities.

Proposed Security Workflow

The proposed architecture operates through the following sequence:

Step 1: Authentication

To log into the platform, a user must first submit authentication credentials, that is, information to prove they are the legitimate user of the account. After completing this identity verification step, they can enter the subsequent process.

Step 2: Additional Verification

This refers to a security verification step triggered when logging into the virtual classroom platform. If the system determines that the current login scenario requires an upgraded security verification level, it will not only rely on the password entered by the user to grant platform access, but will require the user to provide an additional identity verification credential to reconfirm that they are the account owner.

Step 3: Authorization

After a user successfully logs into the platform by passing authentication, the system will automatically verify the user's identity role on the platform, such as student, teacher, or administrator, while checking all applicable attributes matching the user's identity, and then grant the corresponding access and operation permissions.

Step 4: Secure Session Creation

After identity verification and permission allocation are completed, the system will create an encrypted exclusive session for the user. This session is only valid for the current login, is protected throughout its duration, and cannot be misused by unrelated people.



Step 5: Classroom Access

After completing the previous authentication process, the user can successfully obtain platform access permission. All virtual classrooms within the scope of the authorization policy can be entered, and various learning resources permitted by the policy can also be retrieved and used normally.

Step 6: Continuous Monitoring

After entering the seventh layer, the Monitoring and Auditing Layer, the platform will activate a continuous monitoring mechanism, and all security-related events will be monitored. These security events included in the monitoring scope include repeated login failures, unusual login location behavior, repeated permission request failures, unusual session operations, and unauthorized access to sensitive resources. Every abnormal activity that meets the monitoring standards is recorded and retained by the system, which can not only trigger an abnormal warning in a timely manner when an incident occurs, but also serve as a traceability basis in subsequent security investigations to clarify relevant responsibilities.

Step 7: Privacy Enforcement

This link is the core execution step in the privacy enforcement process. All processing operations of the data generated by teachers and students on the platform, from collection, storage, invocation, to transmission, strictly follow the preset privacy rules and access rules, meeting core regulatory requirements, and avoiding unauthorized processing and illegal leakage.

Step 8: Secure Session Termination

After class and logging out, the exclusive login session belonging to the user is officially terminated. The temporary identity credentials previously generated by the system to maintain the user's login, as well as all information valid only during this login session, will become invalid. They can no longer be used to log into the platform, nor can they be used to access any content in the user's name.

IV. RESEARCH GAP

Previous relevant studies conducted by scholars all point to the same conclusion: to achieve solid online education, security and privacy are core issues that must never be taken lightly [1]–[6]. Even with this consensus, research in this field has not covered all problems, and many gaps remain to be filled by subsequent research.

1. Integration of Security Mechanisms

Existing studies frequently focus on specific security components, such as authentication [4], access control [7], communication encryption [5], or online assessment integrity [6]. A research opportunity therefore exists for integrated architectures that coordinate these mechanisms.

2. Security and Scalability

To support large-scale virtual classrooms, it is necessary to simultaneously accommodate a large number of online teachers and students, and support multiple simultaneous online classroom sessions. Subsequent relevant research must verify one thing: if various security mechanisms are integrated into a single virtual classroom architecture, can these integrated security mechanisms withstand the load as more users use the platform, and still maintain qualified operational performance.

3. Multi-Device Session Security

Students and teachers attending classes can log into the learning system not only on classroom computers, but also on mobile phones, tablets, or home computers. As long as they have an internet



connection, they can log in at any time, and no one restricts them to using a single fixed device. However, these cross-device login behaviors bring two types of security challenges: first, how to securely manage parallel login sessions of the same account logged in on multiple devices simultaneously; second, how to identify and respond to abnormal situations such as logins from unfamiliar devices, or device operations that do not match the user's usual usage habits. Research in both of these areas is currently insufficient and requires further exploration by more scholars.

4. Privacy and Security Integration

In current academic research, literature in the privacy field has repeatedly emphasized that in online education scenarios, protecting students' personal information and privacy is a core issue that must be taken seriously [3]. However, research in the cybersecurity field has always focused on identifying and patching system vulnerabilities, and building technical protection measures, without taking into account the requirements of privacy protection [1], [2]. Research in these two directions has always advanced separately, and no one has combined the core goals of these two issues to conduct targeted design. Subsequent relevant research can explore a dedicated system architecture that explicitly integrates the two goals of protecting student privacy and ensuring network security.

5. Real-Time Communication

We previously sorted out various encryption mechanism analyses of online platforms, among which the security analysis of video conferencing encryption solutions shows that real-time communication protocols require detailed security assessment [5]. These communication protocols that support real-time interaction in online classes cannot pass security checks just by having an encryption function; every underlying design must be disassembled and verified one by one. In addition to solidifying the security of communication itself, there is more research space to explore: subsequent research can also be conducted to explore how to integrate communication security mechanisms with authentication, permission allocation, session management, and privacy protection mechanisms.

Proposed Evaluation Framework

The framework proposed in this paper must first undergo practical experimental verification before its actual effects can be asserted. It cannot be stated without testing that this framework is usable and can solve the security and privacy problems of virtual classrooms. It must be run and tested in actual scenarios, with various indicators measured to confirm that it can achieve the expected effects, before it can be officially stated that it is effective.

Possible evaluation parameters include:

To verify the actual performance of this new architecture, it must be evaluated from a series of preset parameter dimensions, each corresponding to a clear measurable indicator:

- Authentication performance: corresponding example measurement is authentication delay
- Scalability: corresponding example measurement is the number of concurrent users that can be supported
- Communication overhead: corresponding example measurement is network and processing overhead
- Security effectiveness: corresponding example measurement is attack detection/defense rate
- Session security: corresponding example measurement is unauthorized session detection capability
- Privacy protection: corresponding example measurement is unnecessary data leakage
- Availability: corresponding example measurement is service uptime
- Usability: corresponding example measurement is user task completion rate



Upcoming experimental tests will apply the exact same usage load to the newly proposed architecture and the current mainstream benchmark virtual classroom architecture, and compare the performance of the two under the same pressure conditions.

Limitations

This study is a conceptual analysis completed on the basis of sorting out existing academic literature. In short, it is still in the stage of integrating existing research and proposing design ideas, and has not been implemented into any operational system. The architecture proposed in this paper has neither been put into use in actual scenarios nor undergone any experimental testing—we have only sorted out the layered protection logic at the theoretical level, and have not yet built an available platform version, let alone tested its reliability in actual usage scenarios. Therefore, before completing a comprehensive experimental evaluation, we cannot put forward any verifiable specific claims about its operational performance, scalability, anomaly detection accuracy, or security protection improvement effect. In other words, no matter how logically sound this design is on paper, without practical testing, we cannot guarantee that it can actually support a large number of simultaneous logins without lag, accurately identify all abnormal intrusion behaviors, and be more secure than existing virtual classroom platforms. These conclusions can only be stated after the experiments are completed.

In addition, security requirements may differ according to institutional policies, platform architecture, user population, and regulatory requirements.

Future Work

Future research should implement a prototype based on the proposed architecture and evaluate: Subsequent future research must first build this architecture into a testable prototype, then verify these core functions one by one: multi-factor authentication, RBAC/ABAC authorization, multi-device session management, secure real-time communication, privacy-compliant data management, security event monitoring, abnormal session detection, and scalability under multi-class concurrent load. This evaluation will measure security, privacy, performance, scalability, and usability.

V. CONCLUSION

Virtual classrooms allow teachers and students from all over the world to flexibly access all learning resources and complete teaching activities without gathering in the same physical classroom, but they also create a security risk environment that is far more complex than that of traditional classrooms—from every user who uses the platform to attend classes, the various applications that support teaching, the transmission channels for teacher-student communication, to the databases that store all information, the cloud services that host the entire platform's operation, and the various teaching resources on the platform, every link in the entire chain may have security issues. Previous studies have identified six core directions for online learning cybersecurity: authentication to confirm user identity, access control to limit user access permissions, data integrity to ensure data is not tampered with, content protection to prevent course resources from being misappropriated, encryption technology to encrypt sensitive data, and network security to protect the entire network environment [1]. More recent review studies have also sorted out the various common cybersecurity vulnerabilities in the widely used online learning platforms today [2].

Students' personal privacy is another very important dimension of online learning security. The systematic review by Kularski and Martin shows that the research community has already paid a lot of attention to the privacy issues of online students, but there is very little research on the privacy of the various online collaboration tools used in virtual classrooms, which is an area that has not been fully



explored [3]. Research in the authentication field has been testing stronger verification schemes, such as adding two-factor authentication to the commonly used Moodle platform to improve login security [4]; research in the communication security field has specifically analyzed the encryption strength of Zoom's end-to-end encryption protocol to identify vulnerabilities in the communication link [5]. The security requirements of online exams, in turn, put forward more new data integrity requirements for the entire security system, which cannot be covered by previous general-purpose solutions [6].

Based on these existing research findings, this paper proposes a layered system architecture that takes both security and privacy protection into account, integrating core capabilities including authentication, permission granting, secure communication, various core services of virtual classrooms, privacy protection, and operation monitoring. The Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) used in this architecture are both mature permission management solutions that have been verified by a large number of practices [7], [9], and previous studies have long proven that these two schemes are fully adapted to the usage scenarios of various educational systems [8].

It should be noted that the architecture proposed in this paper is only a conceptual design foundation, not a finished solution that has been experimentally verified and can be directly implemented. Subsequent research must first build this framework into an operational system, then test and evaluate it in real user access loads and various simulated cyberattack scenarios. Only through such practical testing can it be confirmed whether this architecture, which integrates security and privacy mechanisms, can find an appropriate balance between the core dimensions of security protection, privacy protection, system scalability, operational performance, and user ease of use.

REFERENCES

1. A. Aljawarneh, "Information security in E-learning Platforms," *Procedia - Social and Behavioral Sciences*, vol. 15, pp. 2689–2693, 2011, doi: 10.1016/j.sbspro.2011.04.171.
2. P. A. Pillajo-Garcia and D. Avila-Pesantez, "Cybersecurity analysis in e-learning platforms: A systematic literature review," *Perspectivas*, vol. 5, no. 1, pp. 19–29, 2023, doi: 10.47187/perspectivas.5.1.179.
3. C. M. Kularski and F. Martin, "Online Student Privacy in Higher Education: A Systematic Review of the Research," *American Journal of Distance Education*, vol. 36, no. 3, pp. 227–241, 2022, doi: 10.1080/08923647.2021.1978784.
4. V. Baneş, C. Răvăriu, B. Appasani, and A. Srinivasulu, "A Novel Two-Factor Authentication Scheme for Increased Security in Accessing the Moodle E-Learning Platform," *Applied Sciences*, vol. 13, no. 17, p. 9675, 2023, doi: 10.3390/app13179675.
5. T. Isobe and R. Ito, "Security Analysis of End-to-End Encryption for Zoom Meetings," *IEEE Access*, vol. 9, pp. 90677–90689, 2021, doi: 10.1109/ACCESS.2021.3091722.
6. M. Garg and A. Goel, "A systematic literature review on online assessment security: Current challenges and integrity strategies," *Computers & Security*, vol. 113, p. 102544, 2022, doi: 10.1016/j.cose.2021.102544.
7. D. F. Ferraiolo and D. R. Kuhn, "Role-Based Access Controls," in *Proceedings of the 15th National Computer Security Conference*, Baltimore, MD, USA, 1992, pp. 554–563.
8. H. Wang, "An access control scheme for Web-based e-learning systems," in *Proc. 7th Int. Conf. Information Technology Based Higher Education and Training (ITHET)*, Sydney, NSW, Australia, 2006, pp. 447–453, doi: 10.1109/ITHET.2006.339796.
9. C. T. Hu, D. F. Ferraiolo, D. R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication 800-162, National Institute of Standards and Technology, 2019, doi: 10.6028/NIST.SP.800-162.



10. M. K. Kabier, A. A. Yassin, and Z. A. Abduljabbar, "Towards for Designing Educational System Using Role-Based Access Control," International Journal of Intelligent Engineering and Systems, vol. 16, no. 2, 2023, doi: 10.22266/ijies2023.0430.05.
11. M. Mawgoud, "Enhancing Data Privacy and Trust in E-Learning: A Blockchain-Based Access Control Protocol for Cloud Educational Systems," Concurrency and Computation: Practice and Experience, 2025, doi: 10.1002/cpe.70185.
12. M. Liao, "A Privacy-Preserving and Communication-Efficient Federated Learning Framework for Online Education," Security and Privacy, 2026, doi: 10.1002/spy2.70236.