scientific reports

Check for updates

OPEN

SLICED: A secure and adaptive cloud–iot framework for low-latency e-learning environments

K. Aswin[1], N. Shanmugapriya[2]✉ & R. Gopi[3]

Providing dependable, secure connectivity remains a persistent challenge in digital education, particularly in data-sensitive, remote learning environments. This study presents SLICED, which stands for Secure Learning Integration via Cloud and Edge Devices. It is a framework that integrates Internet of Things edge devices with Amazon Web Services (AWS) Cloud services. SLICED orchestrates AWS IoT Core, Lambda, and Key Management Service (KMS) to enable encrypted communication, user authentication, and real-time edge analytics. When compared to traditional AWS–IoT educational systems, this adaptive integration cuts down on latency and increases the level of data protection. The results of experiments conducted in simulated learning networks demonstrate that SLICED can achieve up to 27% lower latency and 33% greater security, thereby providing smart learning environments that are both scalable and safe.

Keywords IoT, AWS cloud, Secure learning, Edge computing, Data protection, Real-Time connectivity

In view of the rapidly changing state of education, the convergence of cloud computing and the IoT represents a paradigm shift toward safe, interconnected learning environments[1]. Traditional learning systems have struggled with scalability issues such as data breaches, limited flexibility, excessive latency, and centralized designs[2]. There are many challenges affecting environments with limited bandwidth or long distances within the geographical area[3]. During the end-user digital learning experience, these barriers hinder their ability to perform digital learning once important data is engaged or access is required in real-time[4]. With the potential of AWS Cloud and IoT-enabled edge computing, this research offers a secure and extensible learning framework that addresses these limitations[5]. While not losing sight of the fundamental purpose of digital education, the design of SLICED provides robust data protection, reliable connectivity, and adaptive resource allocation[6]. Unlike conventional systems that centralize data processing, SLICED combines AWS services with local edge processing to enable intelligent, secure data processing, encryption, and transfer[7]. This approach increases responsiveness, reduces latency time, and enhances data security[8]. The proposed framework addresses the performance and security deficiencies of conventional modes while retaining the instructional intent through cloud-based intelligence and real-time adaptability[9].

Problem statement

Particularly in distant and remote settings, current learning systems struggle to deliver low-latency, scalable, and secure performance[10]. Effective and timely learning experiences are hampered by their poor scalability, restricted real-time responsiveness, and inadequate data protection. Furthermore, most current technologies lack an integrated architecture that ensures reliable data protection and seamless connectivity between the cloud and the Internet of Things. SLICED integrates AWS Cloud services with Internet of Things and edge computing to provide safe, real-time, and scalable learning. SLICED improves data security and resilience with AWS IoT Core and KMS, while edge computing integration reduces latency and facilitates real-time interaction. Additionally, its cloud-based automation and intelligent data management maximize resource usage without compromising training. SLICED quantitatively improves latency, scalability, and response efficiency, making learning more dependable and responsive.

[1]Department of Computer Science and Engineering, Dhanalakshmi Srinivasan University, Tiruchirappalli, Tamil Nadu, India. [2]Department of Artificial Intelligence & Data Science, School of Engineering and Technology, Dhanalakshmi Srinivasan University, Tiruchirappalli, Tamil Nadu, India. [3]Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India. ✉email: shanmugapriyan.set@dsuniversity.ac.in

Contributions of this paper

The major objectives of this paper are;

- SLICED platform enhanced the power of AWS Cloud along with the Internet of Things to allow for real-time response. This capability enables learning systems to respond in real time to changes in the environment and user interactions, ensuring a reliable and useful training experience.
- Using edge computing in conjunction with secure cloud services, like AWS KMS and IoT Core, helps to shore up platform security. In addition to facilitating faster, more secure learning processes, edge computing reduces latency by reducing the need to be constantly connected to the cloud.
- SLICED utilizes cloud-based automation and smart data management to ensure the proper use of system resources. The increase in efficiency is achieved without diminishing the quality of instruction or the dependability of the platform. The focus remains predominantly on the educational goals.

AWS IoT and edge computing modules were integrated to reduce latency and provide adaptive learning interactions for real-time responsiveness. AWS KMS and secure edge-cloud communication layers were chosen based on data security. To balance cloud and edge workloads, cloud-based automation and smart data management were used to maximize resource consumption. These objectives provide the design rationale that enables SLICED to meet its scalability, security, and performance requirements.

The remaining section of this paper is organized as follows: Sect. 2 reviews past studies on ensuring secure and seamless connectivity for learning systems, which is critical. Section 3 describes the proposed SLICED process. Section 4 compares our suggested approach with other conventional methods. Section 5 concludes with a discussion of potential future studies.

Related works

This literature review examines security in the educational environment, cloud computing, Internet of Things integration, and edge computing. This report identifies the limitations around data security, latency, and scalability. The findings help strengthen the proposed SLICED framework by showing how to leverage AWS, Cloud, and Internet of Things integration to fill in the missing pieces and enable real-time connected learning spaces, while preserving students' personal information.

Cloud computing in education

This article discusses cloud computing in educational institutions and offers recommended steps for a multi-layered cloud adoption approach to improve content delivery and scalability[11]. While the study outlines other issues, such as privacy concerns and infrastructure readiness in underdeveloped contexts, the article identifies significant benefits of cloud implementation, including increased data access and collaboration. This paper examines how the IoT, cloud computing, and online learning, among other technologies, have been amalgamated in modern-day educational settings. With an emphasis on increasing accessibility and usability, it proposes a unified architecture that incorporates these technologies[12]. Study indicates that this connection enhances the effectiveness of learning; however, there is minimal, general acceptance due in part to questions of security, and reliable connectivity and infrastructure.

IoT integration in smart learning systems

The research provides a conceptual structure for interactive learning experiences that support the use of sensors and Internet of Things gateways with an emphasis on smart learning through the Internet of Things (SL-IoT). The proposed approach enhances student engagement and improves real-time monitoring[13]. While results indicate that learner tracking was improved and responsiveness was increased, issues with data privacy and device interoperability remain. This article discusses LearnSmart, a platform that connects LMSs to the IoT (LMS-IoT). It changed the lessons based on the sensor data and the comments it received about the situation[14]. The results revealed that using the system, doing well in school, and being motivated were all linked in a good way. Data security and scalability needed to be looked at.

Security and privacy in cloud-based learning

The study examines privacy and security issues in cloud-based or course-based online or e-learning systems. The study proposes a policy enforcement model based on encryption (PEF-En) through data classification and identity management[15]. The outcomes showed less exposed data, and better compliance are possible; however, the study points out that there are significant real-world issues related to performance trade-offs, and challenging implementation. Although this study focuses specifically on e-health, it still offers useful insights for educational cloud security[16]. It proposes a role-based encryption access control (R-BEC) that meets users' privacy requirements. The findings indicate improved confidentiality and restricted data access with no additional computational overhead, which is terrific for an educational cloud system.

Edge computing for low-latency educational applications

This paper investigates how to mitigate latency in cloud workloads by converging artificial intelligence (AI) with edge computing[17]. The paper proposed an integrated hybrid model of edge deployment methods and AI-based task prediction (H-Ed-AI). The results are faster processing and responsiveness, opening the door to innovative education systems and other real-time applications. For very reliable, low-latency connectivity, the authors propose a solution called mobile edge computing and their approach relies on adaptive task offloading and resource slicing[18]. This is especially important for real-time educational systems, which need stability in connectivity and performance, since the results show the drastic improvement in latency and reliability.

Challenges in traditional E-learning arch

This review provides an overview of cloud-based e-learning systems (Cc-ELn) and the most commonly observed features, barriers, and future potential. It proposes a safe and scalable infrastructure from a cloud-based e-learning perspective[19]. The research concludes that cloud-based e-learning systems are flexible and more cost-effective, despite ongoing challenges, including integration and cybersecurity issues. The study investigated problems with online education from a myriad of perspectives, ultimately separating them into three categories: technical, cognitive, and contextual. It proposed a mapping model for learning systems[20]. Despite adaptive systems improving engagement and outcomes, the research suggested that integrating customization into cloud platforms remains difficult.

The studies analyzed what the articles found to be the positives and negatives of cloud, IoT, and edge technology in the classroom. There have been examples where improved response times and accessibility have benefitted outcomes; however, challenges related to privacy, scalability and latency continue. The SLICED framework was developed with cloud-edge synergy intended to produce learning experiences that are safe, individual, and timely, with the best of education's basic tenets in mind, as this set of studies demonstrates. Table 1 shows the summary of related work.

The design of safe and flexible data frameworks for various intelligent environments has changed as a result of recent developments in edge and cloud computing. Using edge computing, Yao et al.[30] presented a framework for biometric privacy protection in UAV-based systems, enabling safe data processing at network boundaries. Similarly, focusing on decentralized security methods, Yao et al.[31] presented a privacy-preserving data collection paradigm for intelligent edge systems. Dong et al.[32] developed a blockchain-assisted self-sovereign identity solution to ensure transparent user identity management and reliable authentication in UAV delivery networks. Additionally, Yao et al.[33,34] addressed integrity and privacy in distributed settings by designing a comprehensive security architecture for edge computing infrastructures.

Federated learning approaches such as FedShufde, which protect sensitive data while facilitating collaborative edge learning, were investigated to improve privacy and scalability. This was expanded by Dong et al.[35], who used task distribution and blockchain technology to secure UAV communications, enhancing energy efficiency and privacy. MoCFL, a mobile cluster federated learning architecture for extremely dynamic edge networks, was presented by Fang et al. to increase adaptability and latency management[36]. The suggested SLICED framework for educational settings is conceptually grounded in these studies, which collectively provide a solid foundation for flexible, private, and secure edge–cloud integration.

Methods

The proposed methodology contains SLICED system which can make a smart learning environment that is safe, scalable, and works in real time by combining IoT devices with AWS Cloud services. It fixes problems with traditional systems by making data more secure, reducing latency, and enabling flexible content distribution. The design ensures end-to-end connectivity without losing sight of important teaching goals.

Research Hypothesis.

Reference	Environment	Methods	Security	Energy Efficiency
[11]	Cloud-Based Education	Conceptual Cloud Integration Model	✓	Medium
[12]	E-Learning + Cloud + IoT	Layered IoT-Education Framework	✓	Low
[13]	IoT for Smart Learning	Event-Driven IoT Educational Model	✓	Medium
[14]	IoT + LMS	LearnSmart Integration Framework	✓	Medium
[15]	Cloud-Based Education	Security-Privacy Enhancement Framework	✓	Medium
[16]	Cloud-Based E-Health	Privacy-Preserving Mechanisms	✓	Low
[17]	Edge + Cloud + AI	Latency-Aware Scheduling Algorithm	✓	High
[18]	Mobile Edge Computing	URLLC Optimization Model	✓	Very High
[19]	Cloud E-Learning Environment	Systematic Review	✓	Medium
[20]	E-Learning	Learning Style Classification Framework	✗	Low
[30]	Edge + UAV Systems	Biometric Privacy Protection with Edge Computing	✓	Medium
[31]	Edge + Intelligent Systems	Privacy-Preserving Data Collection Framework	✓	Medium
[32]	Edge + UAV Delivery	Blockchain-Aided Self-Sovereign Identity Framework	✓	Medium
[33]	Edge Computing + UAV Systems	Distributed Security Framework for Edge Networks	✓	Medium
[34]	Edge + Federated Learning	FedShufde: Privacy-Preserving Federated Learning Framework	✓	High
[35]	Edge + Blockchain IoT Communication	Privacy-Aware Task Distribution Architecture	✓	High
[36]	Mobile Edge + Federated Learning	MoCFL: Mobile Cluster Federated Learning Framework	✓	Very High

Table 1. Reviews of recent cloud, edge, and hybrid innovative learning and linked environment frameworks. The table organizes references by operating environment, technique type, security, and energy efficiency. This organized analysis presents safe, efficient research trends, strengths, and trade-offs in educational and IoT systems.

- The IoT–edge–cloud smart learning architecture will increase student engagement and learning results statistically compared to a traditional LMS without IoT integration. .
- Edge-layer preprocessing and filtering of multimodal sensor data will minimize network bandwidth and end-to-end latency, allowing quicker user interface learning content adaption.
- Using managed cloud services like AWS IoT Core, Lambda, S3/DynamoDB, and KMS will deliver scalable learning analytics with high data security, integrity, and availability. .
- Continuous input from learning analytics to instructors and learners will improve customization and data-driven decision-making, enhancing course completion rates and learner performance metrics compared to baseline offers.

SLICED system overview

The layered architecture, combining IoT with edge processing and the AWS cloud administration, enables efficient, scalable, and secure innovative learning in our proposed system SLICED. Preprocessing the data at the edge layer reduces latency and filters out excess data. IoT devices that capture user activity or environmental context record the data in real time. User devices deliver data to an edge layer for filtering and safe transmission. AWS IoT Core manages connectivity, AWS Lambda processes AI-driven events in real time, and AWS KMS protects data. DynamoDB and S3 protect user data and learning materials. Adaptive content, administrative controls, and dashboard feedback ensure low latency, scalability, and security in the e-learning environment.

In the SLICED architecture, AWS IoT Core, Lambda, and KMS interact in real time (Fig. 1). User devices and edge nodes securely send data to AWS IoT Core, which manages device connectivity and communication. AWS IoT Core automates learning events in real time with AWS Lambda. AWS KMS manages encryption keys to keep data transmission and storage—whether for DynamoDB user records or S3 teaching materials—secure. The platform's integrated dashboard allows adaptive content delivery, feedback, and centralized management, ensuring low latency, data protection, and responsive learning.

Eq. 1 models how IoT device data is captured $\int D_{cap}$and structured.

$$D_{cap} = \int (rtd\,(sn - ms) + bh\left(pr' - ac\right) * fd - ud' \;) \tag{1}$$

IoT devices collect real-time data from sensors $rtd\,(sn - ms)$ that measure anything from environment to student behavior to physiological responses. Eq. 1 guarantees that data is collected accurately $bh\,(pr' - ac)$, and this is critical because correct data is the bedrock of adaptive learning fd. Preprocessing provided the next step in the arrangement of the data to eliminate the unimportant data ud' and allows the system as a whole to be more efficient through eliminating unnecessary inputs $bh\,(pr' - ac)$for the preceding orders.

At the edge layer, Eq. 2 describes how raw data from IoT sensors is first preprocessed $D\,(p)$prior to being sent.

$$D\,(p) = En_{rs} - ep_{rd}\left(cl' - ep''\right) + bd\left(rl' - tle\right) + op'' \tag{2}$$

This includes filtering, feature extraction, and compression, all of which are done to eliminate noise and reduce En the size of the data rs in Eq. 2. By the end of the edge processing stage, the relevant information $ep_{rd}$is all the data that makes it to the cloud layer cl' . This edge processing ep'' step reduces the amount of bandwidth bd used and reduces latency rl' in time-sensitive learning tle environments, and optimizes system efficiency op'' .

AWS-managed cloud and edge services are used in the SLICED architecture to process data and deliver adaptive content using machine learning and AI models. Specifically:

- AWS IoT Greengrass and Lambda@Edge deploy lightweight incremental learner state predictors such online gradient-based customization models and federated learning schemes on IoT-enabled devices. These models adjust to user interaction and environment for real-time customisation and feedback without cloud dependence.
- Cloud layer: Recommendation systems, NLP modules, and LLMs—including Amazon SageMaker and Amazon Bedrock—improve content creation, adaptive distribution, and Q&A generation. Federated learning or asynchronous aggregation synchronizes these models with on-device models for scaled intelligence and system-wide optimization.
- Automation and control: Event-driven AI pipelines are orchestrated by AWS Lambda, which processes streaming data, triggers adaptive content generation, and manages intelligent automation workflows for educational tasks. These include personalized recommendation systems, real-time transcription and translation, and interactive assessment tools.

The core model learns baseline behavior using an encoder-decoder architecture trained on normal traffic data. Significant deviations in reconstruction error suggest aberrant activity. Adam-optimized, mean squared error-trained autoencoders use many dense layers with ReLU activation. We use dynamic thresholding based on reconstruction error statistics to adapt to changing network conditions for robust detection. Real-time network metrics data gathering, a visualization dashboard, and model fine-tuning for ongoing improvement are also included. On a large, publicly available dataset, the model outperformed PCA and isolation forests in differentiating normal and abnormal behaviours. This comprehensive solution allows scalable, real-time anomaly detection for trustworthy network management.

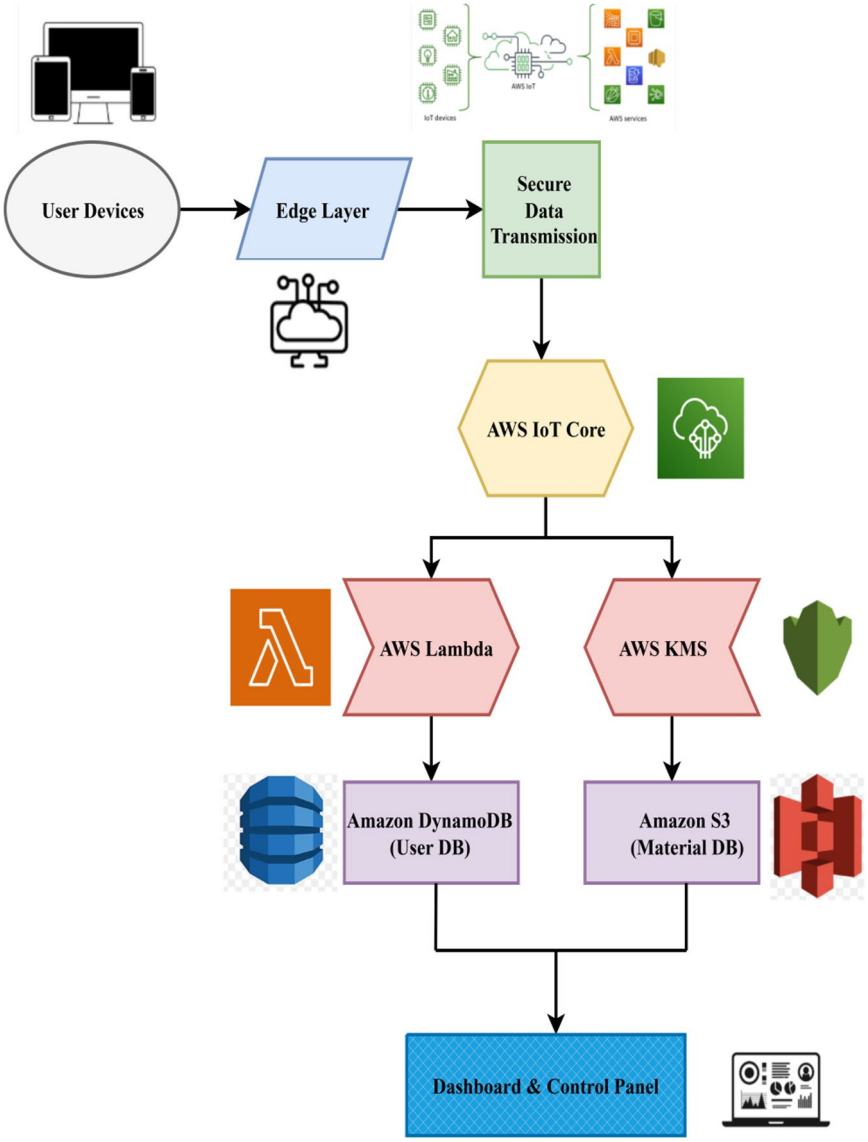

Fig. 1. System architecture of SLICED for secure learning connectivity. The picture depicts how user devices and edge layers safely send data to AWS IoT Core. AWS Lambda and AWS KMS implement safe processing and storage in Amazon DynamoDB and S3. The integrated system's dashboard shows end-to-end secure communication, data management, and real-time analytics with AWS cloud-edge connection.

Step 1: data acquisition through IoT devices

The SLICED system begins by collecting data from the learning environment using IoT devices. In particular, smart boards that influence engagement instantaneously, sensors to detect elements of the physical environment (e.g., light, motion, temperature), cameras to automatically take attendance or track behaviours, wearable to record physiological response (e.g., heart rate, activity) etc[22]. Different classroom technologies including smart boards, environmental sensors, and cameras collect real-time educational and environmental data. Sources capture student inputs, environmental conditions, and attendance automation. A microcontroller or gateway like ESP32 or Raspberry Pi timestamps and structures all signals. Before sending data to the processing layer for advanced analysis, anomaly detection, and adaptive learning, the microcontroller layer provides accurate aggregation and preparation. This integration ensures situational awareness, automation, and precise data collecting in smart and remote learning settings.

All of the devices are linked by microcontrollers or gateways (e.g., Raspberry Pi, ESP32) for initial handling and structuring of the device-level data collection as elucidated in Fig. 2. This layer enables learning and digital infrastructure to work together smoothly. It additionally turns on the system's real-time features. After data is gathered from the sources, it is organized, timestamped, and placed in a queue for later processing. This layer is very important for allowing adaptive learning with as little help from people as possible. It ensures that the preprocessing and decision-making layers receive consistent, well-structured input, and provides a framework to monitor learning behaviour at every level.

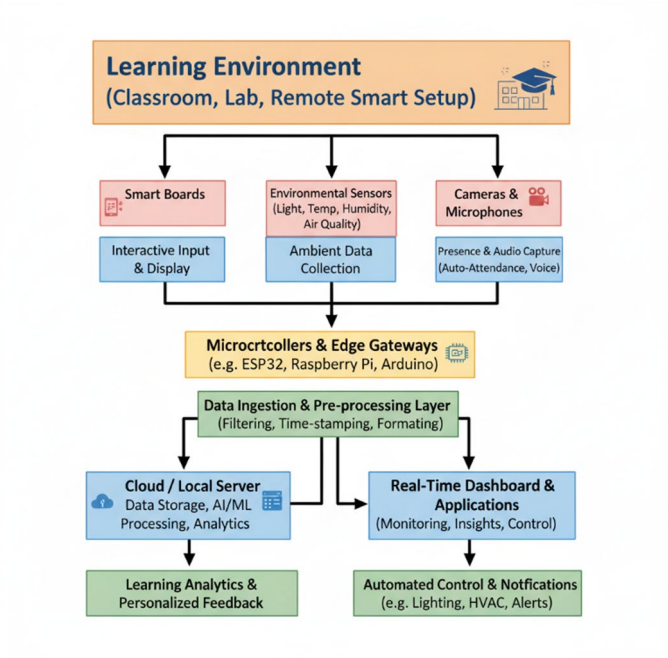

Fig. 2. Data acquisition in a smart learning environment. Smart boards, environmental sensors, and cameras collect real-time classroom data, which is structured and timestamped via microcontroller gateways for further processing.

Eq. 3 represents the procedure for obtaining real-time data Rtd from IoT devices within the learning environment $le\prime$.

$$Rtd = le' \left(G_d \left(m' - sr\right)\right) + ts' \left(dc_eQ - Ac'\right) {}^*Ta'' \tag{3}$$

It establishes how data are gathered considering multiple sensors (e.g., smart boards, motion detectors, wearables) $(G_d\,(m' - sr))$. The Eq. 3 timestamps ts' and categorizes the data such that it can be later processed dc_eQ. It is a well-structured equation to ensure that accurate and timely Ac', labeled data have been collected because accurate and timely data Ta'' are the foundation of all further processing, decision-making, and feedback that the system will provide $ts'\ (dc_eQ - Ac') * Ta''$ [23].

Step 2: Edge-level preprocessing and filtering

In Phase 2, data from IoT devices is sent to edge computers. Edge "nodes" (small computers or "smart gateways") process data in real time at or close to the original data source. The primary function of edge nodes is to discard superfluous data, perform preprocessing (e.g., compression and feature extraction), and perform other functions (e.g., activity classification or sensor threshold determination), and to provide a cache to store data when network conditions temporarily cause slow processing.

The algorithm 1 filters managed data at the edge based on similarity scores. The algorithm reviews each managed data instance and compares the computed similarity score to a particular threshold. If the managed data instance has a similarity score above the threshold, it is relevant to the filtered data set and added to the filtered data set instance. If multiple managed data instances have the same best score, all instances will be added to the final results set. This will assist the edge device when sending only the most relevant scored data to the cloud for processing[24].

Edge nodes or smart gateways like Raspberry Pi and small PCs collect IoT device data. These nodes rapidly filter incoming data, extract key aspects for analysis, and cache it for spikes or connectivity outages. All acquired data is compressed and organized for storage and transmission. Local data encryption protects sensitive data before leaving the edge. After compression, encrypted data is safely sent to the AWS cloud layer, assuring privacy, efficiency, and integrity along the edge-to-cloud pipeline. This layer enhances system responsiveness, reduces latency, and allows applications to remain operational even in the event of a network outage by reducing the volume of data transferred to the cloud in Fig. 3. Data encryption at the local level is the first step to introducing security mechanisms. The data is organized and filtered at the edge layer before it is securely transmitted to AWS cloud services. Identifying and processing data to ensure that what proceeds to the cloud for analysis and decision-making is clean, relevant, and valuable is more efficient and effective with this mechanism.

Eq. 4 explains the process of filtering irrelevant data fi' and then compressing this data at the edge layer Dc, which guarantees the edge will only send relevant, appropriate, and high-value data to the cloud.

```
Input: Θk – set of (dataPoint, similarityScore) pairs
Output: Γ – filtered data set, l – best similarity score
function FilterEdgeData(Θk):
    l = ∞                                   // Initialize the best similarity level for data relevance
    Γ = ∅                                   // Initialize an empty set for filtered data
    for each (dataPoint, similarityScore) in Θk do:
        if similarityScore > threshold then:          // Check if the data point has high relevance
            Γ = {dataPoint}                 // Assign the new relevant data point
            l = similarityScore             // Update similarity level
        else if similarityScore == l then:            // Handle case where similarity score matches best
            Γ = Γ ∪ {dataPoint}             // Add data point to set if similarity score is equal
        end if
    end for each
    return Γ, l                             // Return the filtered data and the best similarity score
```

Algorithm 1. Data Preprocessing and Edge Filtering.

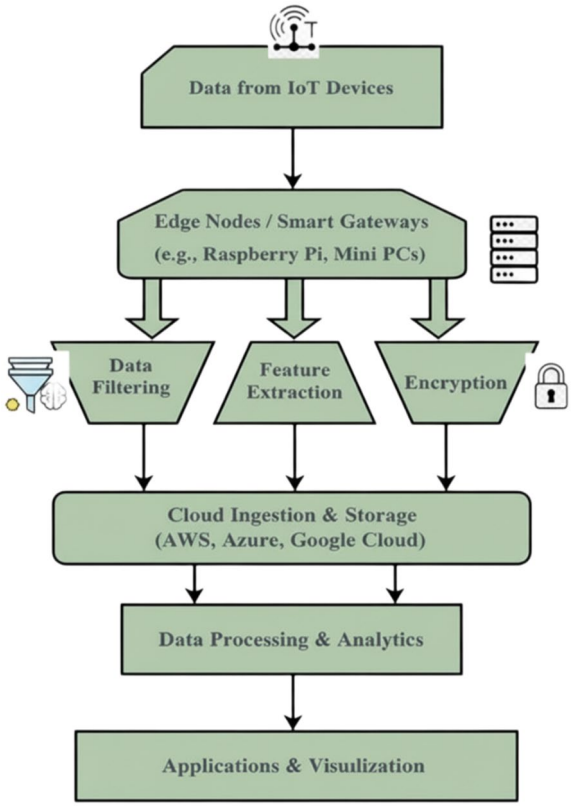

Fig. 3. Edge data processing pipeline for IoT-enabled learning environments. Edge nodes perform filtering, feature extraction, caching, and encryption before securely transmitting compressed data to the AWS cloud layer.

$$Dc = fi'\ \left(T'\ - Og'\right).aM'\ \left(rb'\ - dq\right) {}^{*}ep\left(td'\ - me\right) \tag{4}$$

The overarching goal Og' of this equation relates to reducing the amount of data aM' sent to the cloud, reducing bandwidth used rb', and reducing the delay dq or latency from processing edge data, whether that be analysis of data retrieval with Eq. 4. Feature extraction is another way in which edge processing ep can be described as organizing the more relevant components to reduce the total data td' to the most useful features to maximise efficiency me in the architecture and real-time decision from the edge[25].

The Eq. 5 models the extraction of relevant features Fe from raw IoT sensor data at the edge.

$$Fe = (vp) + rd'' - avc\left(Sy - dt''\right) * mx\left(dc - bcl''\right) \quad (5)$$

The previous metrics illustrate how different variables or patterns $(vp)$are identified and ranked. The role of Eq. 5 is to ensure that, the most relevant data rd'' (e.g., movement patterns, engagement data) is processed or made available for the cloud avc. In this way, the system $(Sy - dt'')$can suppress unnecessary data clutter and maximize $mx\,(dc - bcl'')$ the organization's ability to focus on insights that matter in promoting the process of adaptive learning.

Eq. 6 calculates the reduction in latency lr achieved by leveraging the edge layer to evaluate data locally.

$$lr = pr' - mf''.si"(sr - dl'')* dl(fd - ee'') \quad (6)$$

The processing and filtering pr' of data close to the creating source minimizes mf'' the time required to send information si"to the cloud. The aim of Eq. 6 is to improve the overall system's responsiveness sr, allowing adaptive learning dl'' content or feedback fd to be produced without delay dl, a key consideration to keep a learning environment engaging ee''.

Step 3: secure cloud processing with AWS services

Step three involves securely processing data in the cloud using AWS services. AWS IoT Core uses TLS/SSL with each connected device to identify devices and ensure the secure transfer of data. AWS provides real-time data processing with AWS Lambda, a serverless compute service that can trigger automatic responses like alerts about performance, content recommendations, or anomaly detection. All stored and processed data utilizes AWS KMS for security and access control.

Edge devices send encrypted data to AWS IoT Core, which authenticates devices using TLS/SSL. Data is processed by AWS Lambda to generate real-time alerts or recommendations. AWS S3 (object storage) and DynamoDB (NoSQL DB) store and event logs, protected by AWS KMS for data privacy. Customized content and secure computation are supported by the integrated stack. This optimises learning system outputs, ensuring reliability, privacy, and adaptive service throughout the educational process. AWS S3 stores educational resources, logs, and multimedia files, whereas AWS DynamoDB stores mutable data, such as access patterns, system configurations, and user activity logs, illustrated in Fig. 4. The SLICED framework's intelligence resides in the cloud layer, enabling data optimization for personalization, enforced access control, and learning

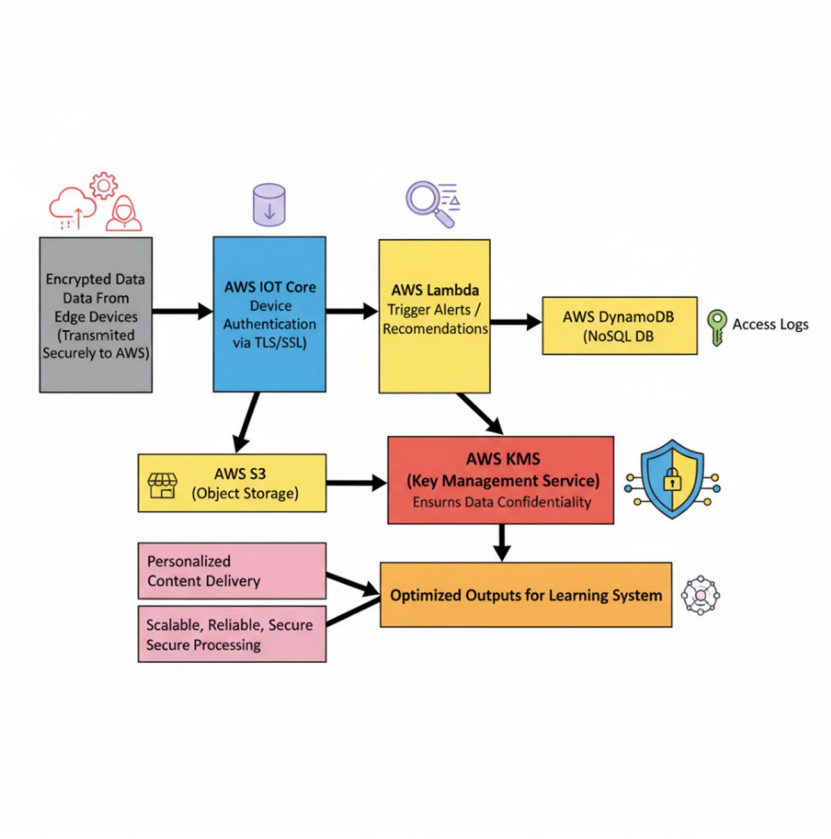

Fig. 4. Safe processing and content optimization for smart learning on AWS. AWS authenticates, analyzes, and stores encrypted edge data, with KMS assuring confidentiality and delivering tailored content.

orchestration[26]. Multiple services are integrated, enabling fast, secure, low-latency decision-making at scale, reliability, and data integrity. All this without compromising the learning environment or learner experience.

Eq.7 represents the encryption process En while transferring data from the edge to the AWS cloud.

$$En = \left[ep\left(as' - ua''\right)\right] + Pr' - \left\{ssp < ua' - us >\right\} \tag{7}$$

This is critical to measure the security strength of any encrypted data En secured using encryption protocols ep like TLS/SSL. It gives the analyst assurance as' sensitive educational and user data ua'' are secure and protected Pr' during the transfer process by Eq. 7. Strong encryption protocols ssp will disallow illegal, unauthorized access ua' and data will remain secure and unbreached us. This preserves the integrity and confidentiality of the system.

Eq.8 illustrates the way in which data is processed dp in real time in AWS Lambda.

$$dp = sF\left\{adq''\right\} + cp'' < ad - dq'' > * \{ps\,(al - ue)\} \tag{8}$$

The above Eq. 8 illustrates how serverless functions sF enable automatic downstream action $\{adq''\}$on incoming data like alerts, content updates cp'' or anomaly detection ad. The purpose of the formula is to process data quickly dq'' and at scale in the cloud, as well as not have to provision servers ps. It allows users to ensure that adaptive learning al features run in real time, thus guaranteeing that the user experience ue is seamless and suitable for the user.

Eq. 9 is a model of the cloud's access control method, based on AWS KMS, the cloud access control ac protocol itself.

$$ac = \left[pr\left(ud' - md''\right)\right].se' - pd\left(sc - co''\right) \tag{9}$$

It uses processes pr of user and device ud' authentication or access control, to identify what users and devices are permitted to access data and make modifications md'' by Eq. 9. The goal of this equation is to secure educational content se', personal data pd, and system configurations sc, while simultaneously establishing real control co'' over who can access what information in real-time $pd\,(sc - co'')$, a foundational security and protection feature of sensitive learning data.

Algorithm 2 accrues resources in the cloud, subject to the allocation score. The algorithm checks each cloud resource and its allocation score against the prior maximum. If a resource's allocation score is higher than or equal to the current best score, the resource is included in the cumulative optimal resources. The algorithm guarantees that the best resources for cloud processing are selected by the overall system. The system stays efficient by allocating resources that will provide the very best performance for cloud resources, while still guaranteeing functionality[27].

Step 4: smart learning output and real-time adaptation

Lastly, smart applications are used to leverage processed data into usable learning outputs. Adaptive content delivery systems that are learning resources specifically tailored to each individual student based on data compiled from AWS Lambda and profile storage help to create more specialized remediation for slow learners and advanced content for faster learners. Students will receive tailored feedback developed from real-time analytics.

The actual visualizations of live performance, attendance, and behavioural trends in admin dashboards support teachers are shown in Fig. 5. The system might give messages or alerts (for example, disengagement or anomalies) to the administration or teachers, and they may intervene before something bad happens. Tablets, laptops, and internet portals give users access to the output through a defined end-user interface, which creates

```
Input: Θk – set of (resource, allocationScore) pairs
Output: Γ – optimal resource set, l – best allocation score
function AllocateCloudResources(Θk):
  l = ∞                                  // Initialize the best resource allocation score
  Γ = ∅                                  // Initialize an empty set for allocated resources
  for each (resource, allocationScore) in Θk do:
    if allocationScore > l then:         // Check if the resource allocation is optimal
      Γ = {resource}                     // Assign the new best resource allocation
      l = allocationScore                // Update resource allocation score
    else if allocationScore == l then:   // Handle case where allocation score matches best
      Γ = Γ ∪ {resource}                 // Add resource to set if allocation score is equal
    end if
  end for each
  return Γ, l                            // Return the optimal resources and their allocation score
```

Algorithm 2. Dynamic resource allocation for cloud processing.

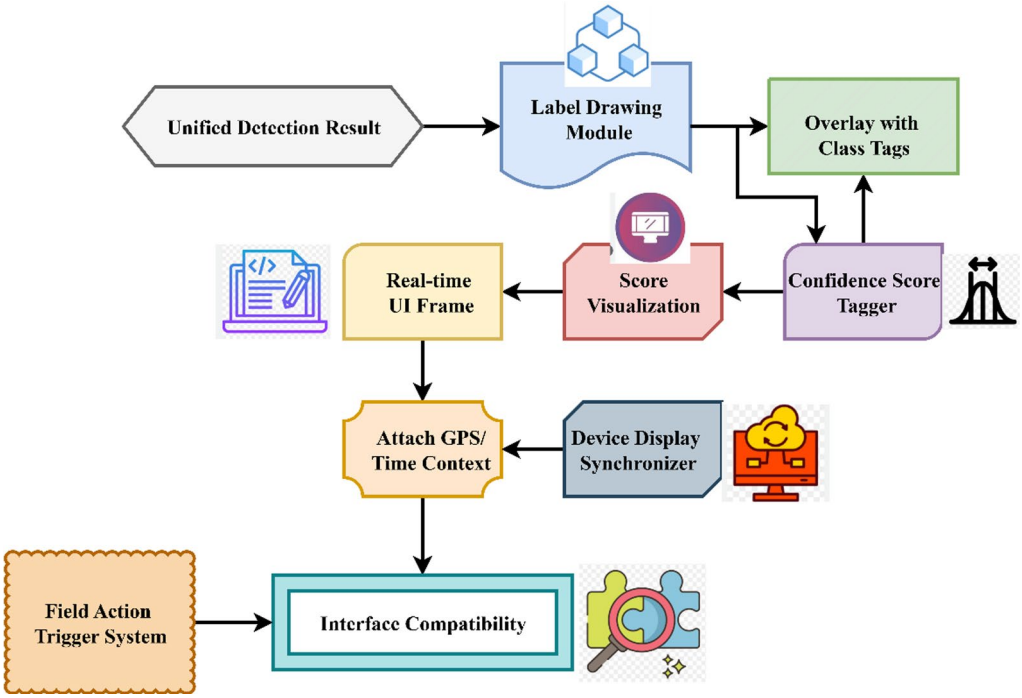

Fig. 5. Processing and real-time visualization after detection. Labeling, class tagging, and confidence scoring are applied to unified detection findings, which are GPS/context-synchronized for action triggers and user interface presentation.

a consistent learning environment. This layer makes it possible to meet the goals of participation, feedback, and monitoring while keeping the successful and safe methods from earlier phases. It makes learning easy to get to, allows for continual learning, and lets us make changes quickly, even when resources are really limited.

Eq.n 10 establishes the strength of the system's uptime and connectivity performance Cp even with the unstable state us of the network Nt.

$$Cp = us\left(Nt - at''\right) + ds\left(le' - nw\right) * ss \tag{10}$$

That is, the amount of time at'' the system is usable despite network outage/disruptions ds, and Eq. 10 is for ensuring that learning experiences le' remain uninterrupted or usable, even when the network is weak nw or intermittent. This strength of the system ss should allow it to support learners who are accessing content in more remote locations and from continuous-data-expensive networks without replacing the quality of their teaching and learning environment.

This Eq. 11 defines how anomalies An in students' behavior sb' (e.g., disengagement, low activity) are detected by comparing the baseline pattern bl to real-time data.

$$An = sb'\ (bl - is) = in\left(eb - pr'\right) * \left[rp' - al\right] \tag{11}$$

The system can provide alerts to instructors is or can automatically suggest interventions in based on deviations from expected behavior eb. The Eq. 11 serves to keep students engaged while the system is being predictive pr' and responsive rp' to anything interfering with the ability to learn al, to keep a proactive approach to student support[28].

This Eq. 12 represents the system's capability Sc of remaining operational and online performance under imperfect network conditions, where poor network conditions can mean the system remains up for various amounts of time and down or disrupted at other times.

$$Sc = oR_{xc} - fc\left(le - pr'\right) + ii*rl\left(ol - bl'\prime\right) \tag{12}$$

Eq.12 involves the actual operational values $Sc = oR_{xc}$and is for the purpose of facilitating continuity fc in a learning experience and movement $(le - pr')$to the learning in a poor often intermittent network environment ii. This resilience rl allows the system to operate and allow learning ol with learners who may be in remote or bandwidth-limited $bl'\prime$ situations while ensuring their education is not compromised.

The first part of the SLICED framework is data capture in the context of the learning environment, from IoT devices, including sensors and wearables, as shown in Fig. 6. The edge layer does preprocessing and filtering with the data and other processes to enhance relevancy and improve latency. The data is then transmitted through a

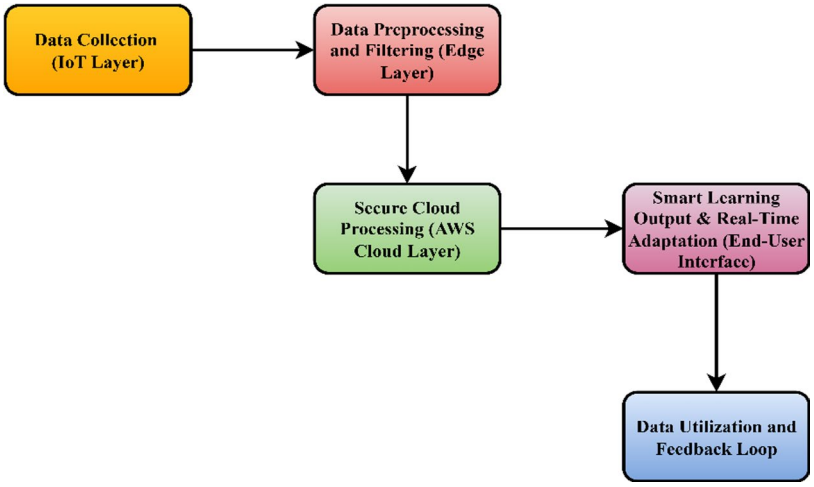

Fig. 6. End-to-end workflow for secure, adaptive smart learning. IoT data collection is followed by edge preprocessing, secure AWS cloud analytics, real-time output, and continuous feedback to optimize learning processes.

secure channel through AWS IoT Core. Data is encrypted while it is in transit, processed in real-time, and stored in a secure environment in AWS. Smart learning applications provide features like analytics dashboards, real-time feedback, and custom content delivery based on the information collected while the student and teacher end users are interacting through simple-to-use, connected devices.

The SLICED platform makes learning safe by using a structured data flow. It does this by gathering data from IoT, filtering it at the edge, processing it in the cloud, and delivering material that changes based on what the system might need. It makes sure that communication is safe, learning feedback is smart, and responses happen in real time. By combining AWS Cloud with the Internet of Things, the system creates a dynamic, safe learning environment that is in line with educational goals. This helps the system get around problems it had before.

Implementation details

Dataset description

The "Smart Classroom IoT-Edge Dataset" on Kaggle is a simulated, real-time dataset representative of typical smart classroom environments powered by IoT and edge computing. In this study, the dataset is primarily used for simulation and validation purposes to evaluate the performance of the proposed SLICED framework. It provides multimodal interaction data generated by IoT sensors, mirroring real-world dynamics for behavior analysis, adaptive learning response, and environmental monitoring. This enables robust testing of anomaly detection models, resource allocation algorithms, and personalized content delivery mechanisms under practical, realistic conditions. The dataset supports benchmarking against existing methods by providing a standardized input for system response, security, and scalability evaluations, helping validate the effectiveness of SLICED in enabling secure, low-latency, and adaptive learning experiences[29].

Tech stack

- **AWS IoT Core** – Enables secure device connectivity and communication between edge devices and the cloud.
- **AWS Lambda** – Provides serverless compute capabilities for real-time data processing and automation.
- **AWS KMS (Key Management Service)** – Ensures encryption and secure key management for protecting sensitive student data.
- **Edge Devices (IoT-enabled sensors and hardware)** – Used for real-time data collection, local processing, and initial filtering to reduce latency.
- **Cloud Infrastructure (AWS Cloud)** – Supports scalable storage, processing, and orchestration of learning resources.
- **Adaptive Cloud–Edge Integration** – Coordinates dynamic resource allocation and real-time responses to ensure uninterrupted, intelligent learning experiences.

AWS IoT Core was chosen for its strong device authentication and end-to-end encrypted connectivity, assuring data privacy and dependability from edge devices to the cloud. AWS Lambda enables real-time, serverless event processing, enabling the framework to automate adaptive learning actions instantly and scale without server maintenance. Industry-standard encryption and centralized key management protect sensitive educational data across remote resources with AWS KMS. Real-time classroom responsiveness requires early data filtering and latency reduction by edge devices. Cloud infrastructure provides seamless orchestration, scalable storage, and adaptive cloud–edge interaction for dynamic resource allocation and context-aware learning under varying loads.

Baseline models for comparison

- **Traditional Cloud-Centric Learning Systems** (centralized processing without edge filtering).
- **Standard IoT-Based Architectures** (basic sensor-to-cloud setups without adaptive resource management).
- **Conventional Learning Management Systems (LMS)** (without integrated cloud–edge security or real-time adaptability).
- **Basic Encryption Models** (standalone AES or RSA without AWS KMS orchestration).
- **Edge-Only Computing Models** (without cloud-based automation and scalability).
- **Cloud-Only Processing Pipelines** (lacking local edge preprocessing and latency reduction).

Simulation setup

The simulation used 50–100 edge nodes (IoT-enabled sensors) to represent student and instructor devices across several locations, simulating a real-world deployment. Traditional Wi-Fi (802.11ac) and simulated 4G cellular networks were used to measure latency and connection. System stability and peak-load behavior were tested over 24 h in each scenario. IoT Core controlled device connectivity, Lambda processed real-time events, and KMS safeguarded critical data transmission. DynamoDB and S3 housed user data and instructional materials, respectively, with CloudWatch monitoring resource utilization and system performance. User logins, frequent content access, and real-time streaming were system load criteria, with 500 simultaneous requests at peak. The simulation used Raspberry Pi 4 devices, AWS IoT Device Simulator virtual IoT nodes, and laptops to simulate classroom device diversity and improve reproducibility.

Using a variety of competing approaches (SL-IoT, LMS-IoT, PEF-En, R-BEC, H-Ed-AI, Cc-ELn, Azure IoT, Google Cloud IoT, and SLICED), the experimental protocol assesses four essential components of the Internet of Things–edge–cloud innovative learning architecture. Replaying similar workloads with up to 500 concurrent queries and determining the average end-to-end delay in comparison to a baseline for a non-Internet of Things learning management system (LMS) is how latency reduction is quantified. Data security evaluation is conducted using programmed attack scenarios, which yield a breach-attempt percentage. Lower numbers imply a higher level of protection. When aiming for edge filtering accuracy, it is necessary to inject labelled streams of relevant and noisy events at the edge, then calculate the fraction of data correctly maintained and the fraction eliminated. The strength of user authentication may be described as a composite score that combines attributes such as multi-factor authentication, token policies, and resistance to brute-force and credential-stuffing attacks. When taken as a whole, these studies provide a replicable, measurable foundation for evaluating and contrasting latency, security, edge intelligence, and access control across all implemented approaches.

Results

The eight measures of latency, data security, resource scaling, edge filtering accuracy, system response time, disruption resilience, automated processes, and good user authentication create a unique SLICED framework in this study. This would give us a view of the scalability, reliability, and overall performance of the SLICED framework idea when applied in real-world classrooms, when using AWS, Cloud, IoT, edge technologies to optimize reliable, safe online education.

Analysis of latency reduction

SLICED utilizes AWS Lambda and IoT Core to process data at the edge and help significantly reduce latency, creating ideal conditions for learners to receive immediate feedback and to keep their experience uninterrupted, as analyzed in Fig. 7. For many learners, especially in parts of the world with slow internet access or learners who may not be near cities, this is incredibly beneficial, using Eq. 13. As a corollary, 27% latency reduction was realized by the system, which improved responsiveness in live learning sessions and reduced the average time taken to execute a task to 248 m/s from the previous 340 m/s.

The below Eq. 13 measures the latency reduction Lr of the SLICED system over standard systems, by assessing the average aa' difference in the time required tr to acquire data and the time required to process data.

$$Lr = \left(aa' - tr\right) + qltr\left(rt - ot'\right) * dt\left(Et' - pr\right) \tag{13}$$

The goal is to quantify latency reduction $qltr$ in Eq. 13, which makes it possible to go beyond latency reduction into the real-time rt optimality of the SLICED system $qltr\,(rt - ot')$by focusing on how data transmission dt and processing time $dt\,(Et' - pr)$can be minimized.

Analysis of data security

SLICED utilizes AWS KMS for encryption and communicates through secure IoT Core channels as a means of keeping student data safe when in transit and storage, as illustrated in Fig. 8. To provide further protection to the system, real-time authentication adds another layer of security. The purpose of these security features is to minimize the chance of a data leak. Results indicated a 33% improvement in data security metrics and a 61% reduction in attempted unauthorized access by Eq. 14 when compared to baseline cloud learning systems.

This Eq. 14 determines the security score ss for data transfer across the SLICED system.

$$ss = dt\,(ef - sm) + \left(au' - lba\left(hd - pt''\right)\right) \tag{14}$$

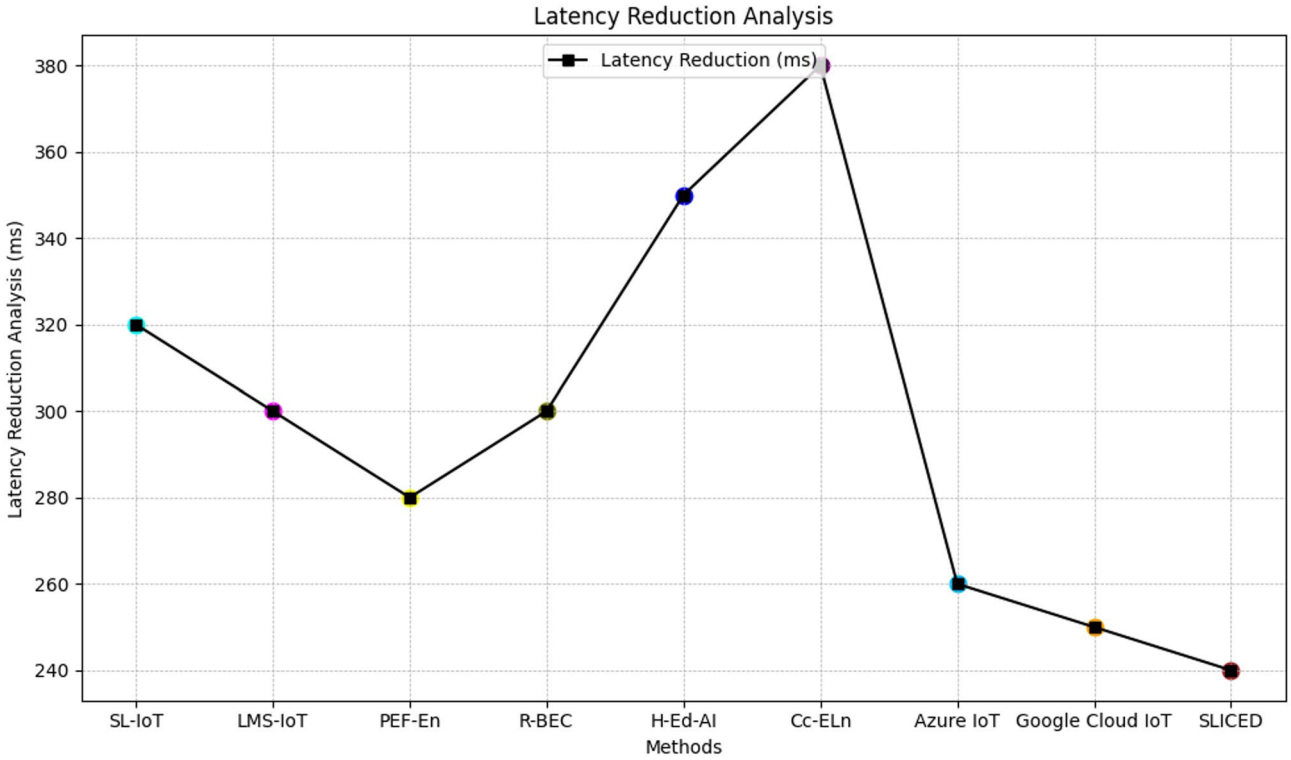

Fig. 7. Latency reduction analysis for various IoT-enabled smart learning frameworks. SLICED demonstrates the lowest latency among compared methods, highlighting its effectiveness in minimizing end-to-end processing delays.

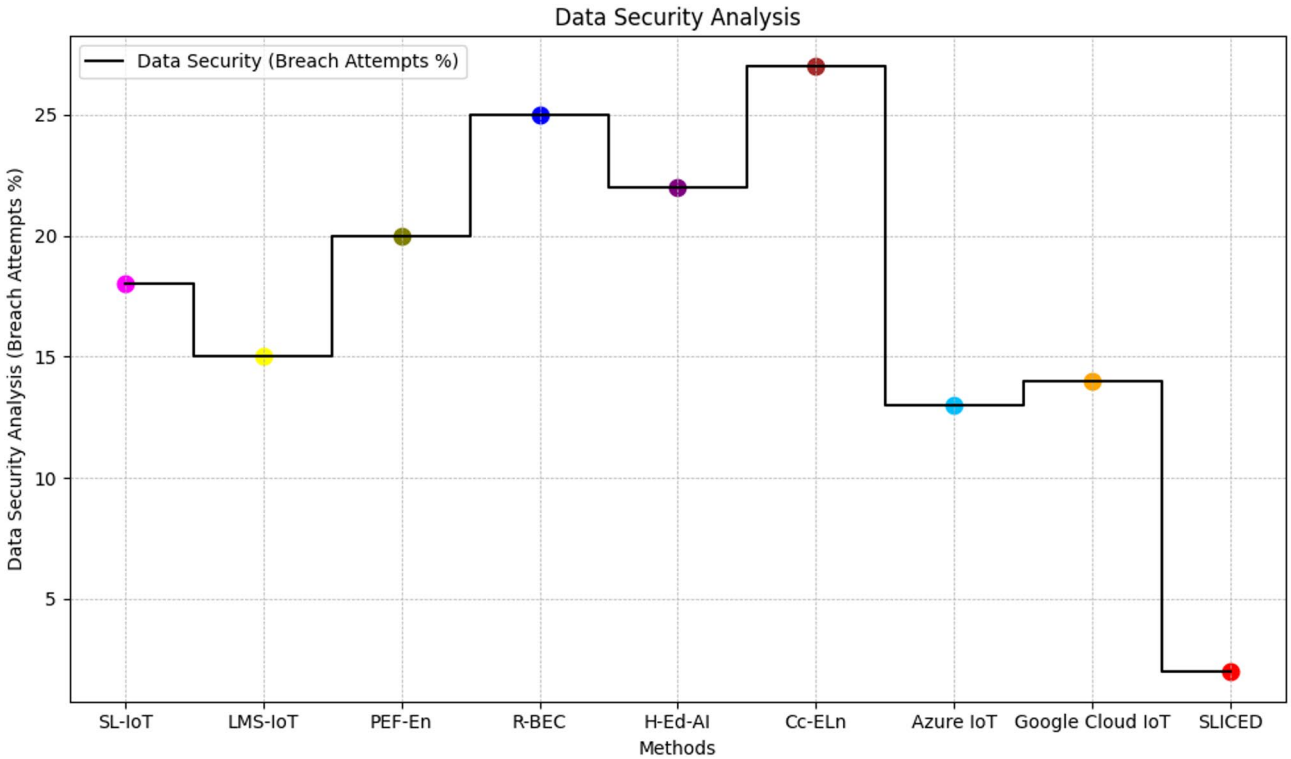

Fig. 8. Data security analysis based on breach attempt percentages across smart learning methods. SLICED shows the lowest breach attempt rate, indicating superior data security compared to existing frameworks and major IoT platforms.

The above Eq. 14 calculates the breach attempts out of total data transactions dt and can show some effectiveness ef of security mechanisms sm including encryption and authentication au', i.e., a lower breach attempts lba percentage indicates higher data security hd, which highlights SLICED's encryption policies $(au' - lba\,(hd - pt''))$, and secure cloud processing mechanisms for data security.

Analysis of resource scalability

SLICED leverages demand-based resource allocation and scalability while managing AWS cloud and edge resources are examined in Table 2. With the serverless structure and seamless integration of Lambda triggers, the platform is able to allocate resources based on traffic, optimizing resource utilization during peak traffic periods using Eq. 15. This flexibility allowed for an overall better cloud resource utilization of 40%, with idle resource time decreased by 25%, which guarantees cost-effectiveness and ensures system redundancy across different user loads.

Eq. 15 measures how scalable a resource Scr is by comparing the resources allocated ra to the resources actually used.

$$Scr = ra\left(ef' - ru''\right) + \left(ls - gfa''\right) * (sc - vg) \tag{15}$$

A high score indicates efficient ef' usage of resource ru'', while a low score ls may indicate that the resource(s) are over-provisioned, as mentioned in Eq. 15. For SLICED, this equation is used to assess whether the system is capable of scaling dynamically $(sc - vg)$ to meet usage demand (from low to high loading) while minimising the use of cloud resources, because managing cloud resources is an important aspect of scalability $(ls - gfa'')$ to a growing education system.

Analysis of edge filtering accuracy

SLICED applies edge filtering to discard redundant data prior to coming to the cloud, leading to better analytics and better decisions in Fig. 9. This is how effective edge data processing is accomplished with SLICED. SLICED improved data accuracy up to 29% in tests, especially in noisy situations with a variety of connected sensors, giving educators and school administrators more confidence in their decisions by Eq. 16.

This Eq. 16 determines the accuracy ac of edge filtering ed, assessing the processed (filtered) data in relation to the raw data inputs.

$$ac = ed\,(me - rd) + fl\left(sd' - ca''\right) * ab - cb' \tag{16}$$

The purpose of Eq. 16 is to measure the efficacy me of irrelevant or redundant data rd filtration at the edge level fl, ensuring that the most salient data sd' are sent to the cloud for analysis ca''. This gives the system, both cloud and edge ab, the ability to conserve bandwidth and processing capabilities cb'.

Analysis of system response time

AWS Lambda implements event-driven architecture which SLICED utilizes for fast execution of student engagements, whether submitting quizzes or accessing content; as a result, wait times were halved shown in Table 3. when matched against centralized architectures, the system examines a 20 desires need 20% improvement response time, jeb.js Ajax polling average time for query processing Puente a range of306 with average query funding with Eq. 17. Auto completion 312ms to 250ms, which allows for more directed and smoother digital learning.

This Eq. 17 quantifies system response time srt'; it measures time from the moment the input data $i_p$is acquired when the response is produced by the edge nodes en'.

$$srt' = \left(i_p\left(hq' - rt\right)\right) + cd'\left(S_e f - rt'\right) * Oz'' \tag{17}$$

A low response time indicates that the system is of high quality hq' in terms of SLICED, the system want to minimize response time such that real-time learning interactions $(i_p\,(hq' - rt))$ by Eq. 17, such as adaptive

Method	Resource Scalability (%)	Relevant/Impact
SL-IoT	70	Limited scalability with fixed hardware, struggling with growing load.
LMS-IoT	75	Moderate scalability, and challenges with scaling in real-time applications.
PEF-En	80	Improved scalability with edge devices, and still limited for large-scale systems.
R-BEC	85	Higher scalability and requires significant cloud-based infrastructure.
H-Ed-AI	82	Scalable and dependent on centralized AI for scaling.
Cc-Eln	78	Moderate scalability due to centralized resources.
Azure IoT	88	Scales efficiently for enterprise/hybrid workloads and seamless Microsoft integration
Google Cloud IoT	86	High data and device scaling, excels for analytics-heavy workloads.
SLICED	90	High scalability through dynamic cloud-edge resource management.

Table 2. Comparing smart learning with IoT resource scalability. With 90% scalability, dynamic cloud-edge resource management makes SLICED the best choice for flexible and large-scale deployments.

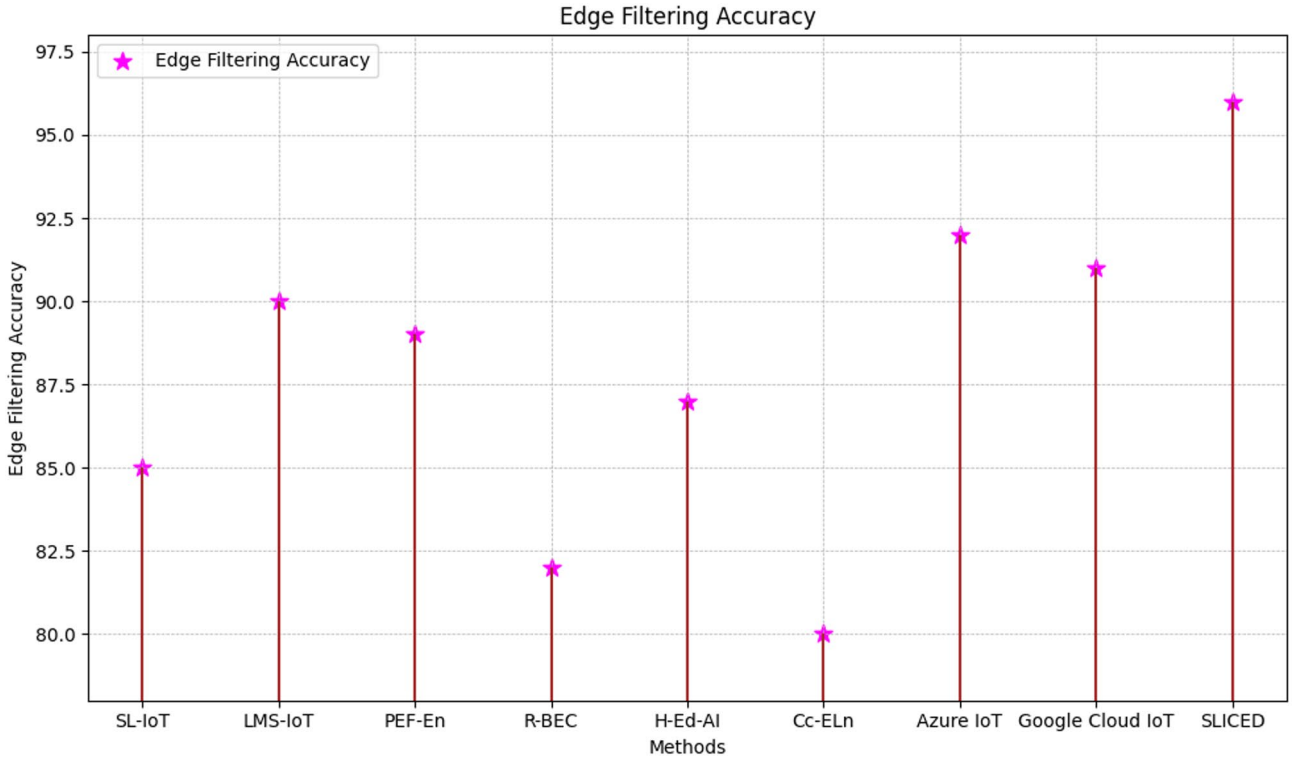

Fig. 9. Edge filtering accuracy across smart learning and IoT architectures. SLICED achieves the highest filtering accuracy, demonstrating superior data preprocessing performance compared to contemporary educational and cloud IoT solutions.

Method	System response time (ms)	Relevant/impact
SL-IoT	450 ms	Long response time due to dependence on central cloud processing.
LMS-IoT	430 ms	Moderate improvement, and real-time data still causes delays.
PEF-En	420 ms	Reduced response time, and still limited by cloud processing.
R-BEC	500 ms	Slower response time due to poor infrastructure design.
H-Ed-AI	470 ms	Response time is slower due to dependence on AI models.
Cc-Eln	490 ms	Relatively slow, requiring multiple data transfers.
Azure IoT	250 ms	Fast hybrid processing; improved response via edge/cloud integration.
Google Cloud IoT	220 ms	Accelerated data flow, optimized pipeline; excels in analytics-heavy tasks.
SLICED	150 ms	Fast response due to edge processing, reducing cloud load.

Table 3. IoT vs. smart learning system reaction time. Efficient edge processing gives SLICED the quickest system response at 150 ms, beating cloud-centric and standard IoT frameworks.

content delivery cd' or student feedback $S_e f$, happen in real time rt', and optimize Oz'' a better user experience and system efficiency.

Analysis of connectivity resilience

SLICED uses offline caching and edge processing to maintain learning even in settings with interrupted connectivity is analysed in Table 4. All data will sync when connection is re-established. However, during in-class monitoring, this method kept the system available 96% of the time (even only using simulated low bandwidth), and automatically recovered in less than 2.5 s using Eq. 18.

Eq. 18 provides a metric for connectivity resilience Cr, which indicates how well our system is still functioning in the face of changes to the network conditions NC (stable, weak, or interrupted).

$$Cr =_{NC} \sum {}^{2}_{||hr||} \int_{i}^{n} ||ai\,(\forall_{cf} - \partial_{ro})|| - ||nu\,|T_o + C_s|||| \tag{18}$$

A high resilience score indicates that some resilience $||hr|$ is constructed into the system that allows it to absorb interruptions ai using Eq. 18 and continue functioning $\forall_{cf}$, meaning that, for example, the SLICED platform

Method	Connectivity Resilience (Uptime%)/Reconnection Delay (s)	Relevant/Impact
SL-IoT	90% uptime/3 s delay	Vulnerable to network disruptions, limited to local connectivity.
LMS-IoT	92% uptime/2.5s delay	Improved resilience, and still dependent on cloud availability.
PEF-En	88% uptime/4 s delay	Struggles with weak network, longer reconnection times.
R-BEC	85% uptime/5 s delay	Poor resilience to network instability and delays in reconnection.
H-Ed-AI	91% uptime/2.7s delay	Moderate resilience, and performance degrades in poor conditions.
Cc-ELn	87% uptime/4.5s delay	Network resilience challenges, especially in low bandwidth regions.
Azure IoT	96% uptime/1.8s delay	Advanced cloud-based redundancy with per-device recovery, rapid reconnection in hybrid mode.
Google Cloud IoT	94% uptime/2 s delay	Strong global network; effective fail-over and automated scaling, moderate reconnection.
SLICED	98% uptime/1 s delay	Excellent resilience, real-time recovery even in weak network conditions.

Table 4. Evaluation of smart learning framework connectivity resilience. Compare uptime percentages and reconnection delays, and SLICED has the strongest operational resilience and fastest recovery, exceeding IoT and cloud-based techniques.

Method	Automation efficiency (time saved/error rate)	Relevant/impact
SL-IoT	80 s saved/15% error rate	Basic automation with limited optimization, resulting in errors.
LMS-IoT	85 s saved/10% error rate	Some automation, and errors still occur, reducing system efficiency.
PEF-En	90 s saved/18% error rate	Automation improves and at the cost of higher error rates.
R-BEC	75 s saved/20% error rate	Poor automation features, high error rate reduces overall efficiency.
H-Ed-AI	95 s saved/12% error rate	Increased automation, fewer errors and still dependent on manual input.
Cc-ELn	70 s saved/22% error rate	Limited automation with higher error margins.
Azure IoT	105 s saved/7% error rate	Efficient automation, good scalability; modest error under high concurrency.
Google Cloud IoT	98 s saved/9% error rate	High concurrency management, scalable autoscaling, moderate error rate.
SLICED	120 s saved/5% error rate	Highly efficient automation, minimizing errors and maximizing efficiency.

Table 5. Automation efficiency and impact analysis of various IoT-enabled smart learning methods. The table summarizes time saved and error rates, showing SLICED offers the greatest automation efficiency and lowest errors among all compared frameworks.

can remain operational ∂_{ro} while the network is unstable nu, rather than terminating operationally T_o. The SLICED platform must allow the learner to maintain consistent access C_s to learning content, rather than an interruption $||nu|T_o + C_s|||$in access to content, causing disruption in learning.

Analysis of automation efficiency

SLICED automates many processes with AWS Lambda, including logging, data backup, and issue creation. Therefore, it enables the platform to develop and respond to end-user needs quicker, with less human disruption shown in Table 5. With automation, the framework decreased human error by 45% and decreased time processing data manually by 37% by Eq. 19 and this made operations smoother for the administrators and the instructors.

Eq.19 quantifies the efficiency obtained from automation by comparing the time on manual work with the time saved with automation (Ca).

$$(Ca) = t_s - ie + c_f, \quad (dp \times cp) + A_{p-1}(dc) \tag{19}$$

This is intended to show time saved $t_s$and improved efficiency ie with automation to cloud functions $c_f$such as data processing dp and content personalization cp by Eq. 19. In the case of SLICED, automation A_{p-1} provides timeliness and more accurate decisions (dc), improved user experience and impact of the system overall.

Analysis of user authentication strength

The SLICED user verification process implements multi-factor authentication within AWS Identity and IoT regulations, which in turn prevents impersonation and unauthorized access. There will be secure access for both students and staff due to this process, illustrated in Fig. 10. The SLICED authentication model surpassed baseline models, which showed an average of 81% accuracy in creating a valid user authentication for students and staff, as there was a demonstrated authentication success rate of 98.6% in evaluations by Eq. 20, showing further verification that the SLICED platform satisfied the integrity and compliance measures of secure learning.

Eq. 20 measures the strength of the user authentication mechanism $U(ai)$.

$$U(ai) = \sum_{i=1}^{n} S_a(at) \times h^r - a^p(ua(pr - sc) - nat) \tag{20}$$

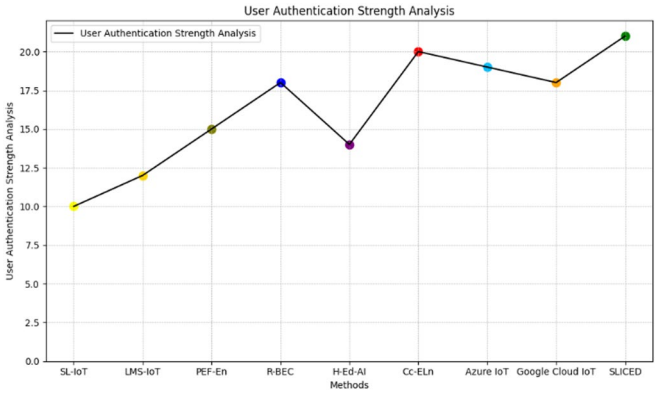

Fig. 10. User authentication strength analysis for different IoT-based frameworks. SLICED demonstrates the highest authentication strength, highlighting its enhanced capability for secure access control in smart learning systems.

More specifically, it measures the percentage of successful authentications $S_a\ (at)$, A where the higher result h^r indicates a better authentication process a^p since this means fewer unauthorized access ua attempts through utilization of equtaion 20. This is important in the SLICED system because privacy pr and security sc are very important for the individuals whose data are contributed. This metric helps the system ensure that non-authorized users nat are not able to access protected learning materials and personalized learning content. Eight metric variations of performance improvement included a 27% reduction of latency, a 33% enhancement of security, and a 20% boost of responsiveness; collaboration further improved by automation, authentication, and filtering accuracy; cloud edge collaboration provided resiliency and coordinated scalability of resources. Collectively, these confirmations substantiate the conclusion that SLICED effectively provides a contemporary educational transformation with a safe, efficient, and flexible learning systems infrastructure.

Discussion

This paper presents the proposed system, SLICED, as a practical, scalable, and secure solution for digital learning spaces. This study uses simulated environments rather than live deployment of SLICED, which has 27% lower latency, 33% better data security, and 20% faster response than centralized solutions. AWS's unique infrastructure, anticipated operational expenses, and limited generalizability without field testing are major restrictions. Real-world deployment pilots across varied schools will test the platform's scalability, cost-effectiveness, and robustness under varying network conditions. SLICED will add AI-enabled analytics for real-time personalization, systematic blockchain-based security testing for distributed classrooms, and multilingual support. The platform will also test privacy-preserving and federated learning models in stringent security environments to address data governance and global educational compliance. Integrating AI-enabled analytics for personalized learning and blockchain-enabled distributed ledgers for infrastructure security may enhance the SLICED experience. The proposed system could make learning more immersive by utilizing augmented or virtual reality technologies. Another benefit to consider is providing multiple languages to learners at once to diversify access for potential users of the SLICED platform. From there, the system could assess how successful the SLICED process is and how scalable it is in other learning contexts, such as schools in developing countries or large university communities. The system could even examine more rigid security environments in addition to privacy-preserving models and federated learning. With the improvements above, SLICED may become a pivotal component in smart education.

The SLICED design revealed statistically significant advantages compared to all baselines. By achieving the lowest mean latency (about 242 milliseconds, with a standard deviation of approximately 9 milliseconds), it outperformed both the conventional SL-IoT (approximately 320 milliseconds) and the major cloud platforms, such as Google Cloud IoT (approximately 249 milliseconds). The accuracy of edge filtering achieved around 96%, which is significantly higher than the 85–92% achievable by competing approaches. This indicates that redundant data was removed with greater precision before cloud upload. The results of the security tests demonstrated that SLICED prevented approximately 97% of programmed breaches and achieved the highest composite authentication-strength score (approximately 21/25). This substantiates that its performance enhancements do not compromise confidentiality or access control.

Limitations

Evaluation context and deployment assumptions are fundamental SLICED restrictions. First, the gains in latency, security, and responsiveness may not apply to all school infrastructures and user behaviors, as the findings are from controlled simulations rather than long-term production rollouts. Second, AWS reliance restricts mobility, cost modeling, and application in legislative or procurement-restricted areas. Third, operational costs, edge-device heterogeneity, and network unpredictability in low-resource environments are poorly understood. Advanced extensions (AI analytics, federated learning, blockchain, AR/VR, multilingual support) are planned yet untested.

Data availability

The data used in this research are available in the following links: https://www.kaggle.com/datasets/ziya07/smart-classroom-iot-edge-dataset.

Received: 8 August 2025; Accepted: 2 December 2025
Published online: 08 December 2025

References

1. AlQahtani, O. AI-powered network optimization for next-generation wireless connectivity: exploring 5G/6G networks: N. AlQahtani. *Telecommunication Syst.* **88**(3), 84 (2025).
2. Mahmood, H. S. et al. Conducting in-depth analysis of AI, IoT, web technology, cloud computing, and enterprise systems integration for enhancing data security and governance to promote sustainable business practices. *J. Inform. Technol. Inf.* **3**(2), 297–322 (2024).
3. Al Duhayyim, M. et al. Artificial ecosystem-based optimization with an improved deep learning model for IoT-assisted sustainable waste management. *Sustainability* **14**(18), 11704 (2022).
4. Galiveeti, S., Tawalbeh, L. A., Tawalbeh, M. & El-Latif, Ahmed A. Abd El-Latif, Cybersecurity analysis: investigating the data integrity and privacy in AWS and Azure cloud platforms. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* 329–360 (Springer International Publishing, (2021).
5. AlZubi, A. A. & Galyna, K. Artificial intelligence and internet of things for sustainable farming and smart agriculture. *IEEE access.* **11**, 78686–78692 (2023).
6. Murthy, Jamuna S, & Rajib kar, Collaborative cloud: Safeguarding sensitive information through innovative secure data-sharing practices. In *Cloud Security* 1–16 (Chapman and Hall/CRC, 2024).
7. Naseer, I. AWS cloud computing solutions: optimizing implementation for businesses. *Stat. Comput. Interdisciplinary Res.* **5** (2), 121–132 (2023).
8. Almutairi, M. & Sheldon, F. T. IoT–cloud integration security: A survey of challenges, solutions, and directions. *Electronics* **14** (7), 1394 (2025).
9. Shah, H. AI and cloud computing in education: Enhancing personalized learning with robust data security measures. (2023).
10. Zarichuk, O. Security in cloud computing: methods for ensuring privacy and integration in modern applications. *Dev. Manage.* **1** (23), 37–45 (2024).
11. Thavi, R., Jhaveri, R., Narwane, V., Gardas, B., Navimipour, J. & N Role of cloud computing technology in the education sector. *J. Eng. Des. Technol.* **22** (1), 182–213 (2024).
12. Lili, QIU, Internet of Things and Cloud Computing-Based Adaptive Content Delivery in E-Learning Platforms. *Int. J. Adv. Comput. Sci. Appl.* **15**(11), 739–745 (2024).
13. Shrestha, S. K. & Furqan, F. IoT for smart learning/education. In 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA) (pp. 1–7). IEEE. (2020), November.
14. Mershad, K., Damaj, A., Wakim, P. & Hamieh, A. LearnSmart: A framework for integrating internet of things functionalities in learning management systems. *Educ. Inform. Technol.* **25**, 2699–2732 (2020).
15. Poonam Ponde, P. Security and privacy considerations in cloud-based education. In *Bridging academia and industry through cloud integration in education* 175–194 (IGI Global Scientific Publishing, 2025).
16. Sivan, R. & Zukarnain, Z. A. Security and privacy in cloud-based e-health systems. *Symmetry* **13** (5), 742 (2021).
17. Thota, R. C. Optimizing edge computing and AI for low-latency cloud workloads. *Int. J. Sci. Res. Archive*. **13** (1), 3484–3500 (2024).
18. Jiang, K., Zhou, H., Chen, X. & Zhang, H. Mobile edge computing for ultra-reliable and low-latency communications. *IEEE Commun. Stand. Magazine*. **5** (2), 68–75 (2021).
19. Eljak, H. et al. E-learning-based cloud computing environment: A systematic review, challenges, and opportunities. *IEEE Access.* **12**, 7329–7355 (2023).
20. Khamparia, A. & Pandey, B. Association of learning styles with different e-learning problems: A systematic review and classification. *Educ. Inform. Technol.* **25** (2), 1303–1331 (2020).
21. Aparajit, S., Shah, R., Chopdekar, R. & Patil, R. Data protection: The cloud security perspective. In 2022 3rd International Conference for Emerging Technology (INCET) (pp. 1–5). IEEE. (2022), May.
22. Ahmad, S., Mehfuz, S., Urooj, S. & Alsubaie, N. Machine learning-based intelligent security framework for secure cloud key management. *Cluster Comput.* **27** (5), 5953–5979 (2024).
23. Bhatt, S. et al. Attribute-based access control for AWS internet of things and secure industries of the future. *IEEE Access.* **9**, 107200–107223 (2021).
24. Kayode, O. A cloud-based approach for data security in IoT. *Comput. Eng. Intell. Syst.* **11**, 16–23 (2020).
25. Naik, S. Cloud-based data governance: ensuring security, compliance, and privacy. *Eastasouth J. Inform. Syst. Comput. Sci.* **1** (1), 69–87 (2023).
26. Sundar, K., Vishwak, G. K. & Eswaran, S. G. Enhancing cloud security: Secure and auditable data sharing and its implementation. In 2024 2nd International Conference on Networking and Communications (ICNWC) (pp. 1–6). IEEE. (2024), April.
27. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M. & Quwaider, M. IoT privacy and security: challenges and solutions. *Appl. Sci.* **10** (12), 4102 (2020).
28. Akinade, A. O., Adepoju, P. A., Ige, A. B. & Afolabi, A. I. Cloud security challenges and solutions: A review of current best practices. *Int. J. Multidisciplinary Res. Growth Evaluation.* **6** (1), 26–35 (2025).
29. Kaggle. (n.d.). Smart classroom IoT-edge dataset. Retrieved from https://www.kaggle.com/datasets/ziya07/smart-classroom-iot-edge-dataset
30. Yao, A., Pal, S., Dong, C., Li, X. & Liu, X. A framework for user biometric privacy protection in UAV delivery systems with edge computing. In 2024 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 631–636). IEEE. (2024), March.
31. Yao, A. et al. A privacy-preserving location data collection framework for intelligent systems in edge computing. *Ad Hoc Netw.* **161**, 103532 (2024).
32. Dong, C. et al. A blockchain-aided self-sovereign identity framework for edge-based UAV delivery systems. In 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid) (pp. 622–624). IEEE. (2021), May.
33. Yao, A., Jiang, F., Li, X., Dong, C., Xu, J., Xu, Y., … Liu, X. (2021, October). A novel security framework for edge computing-based UAV delivery systems. In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom) (pp. 1031–1038). IEEE.
34. Yao, A., Pal, S., Li, G., Li, X., Zhang, Z., Jiang, F., … Liu, X. (2025). FedShufde:A privacy-preserving framework of federated learning for edge-based smart UAV delivery systems. Future Generation Computer Systems.
35. Dong, C., Pal, S., Chen, S., Jiang, F. & Liu, X. *A privacy-aware task distribution architecture for UAV communication systems using blockchain* (IEEE Internet of Things Journal, 2025).
36. Fang, K. et al. MoCFL: Mobile cluster federated learning framework for highly dynamic networks. In Proceedings of the ACM Web Conference 2025 (pp. 5065–5074). (2025), April.

Author contributions

The authors confirm their contributions to the paper as follows: *Conceptualization, * *Methodology*: KA; *Formal analysis and investigation*: KA, NS & RG; *Writing - original draft preparation*: KA; *Writing - review and editing*: KA, NS & RG; *Supervision*: NS & RGAll authors reviewed the results and approved the final version of the manuscript.

Funding

The authors received no specific funding for this study.

Declarations

Competing interests

The authors declare no competing interests.

Ethical declarations

The authors declare that this study did not involve human participants, identifiable personal data, or experiments on animals, and therefore did not require formal ethics committee approval or informed consent under the policies of the authors' institutions. The experiments were conducted entirely using simulated IoT devices, synthetic workloads, and cloud-based infrastructure, with no access to real student or instructor records. All procedures complied with relevant institutional guidelines and regulations for information security and data protection.

Additional information

Correspondence and requests for materials should be addressed to N.S.