International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I5P134

Volume 74 Issue 5, 540-562, May 2026
© 2026 Seventh Sense Research Group®

Original Article

TransExa-Fog: A Fog-Edge-Cloud Architecture for Low-Latency, Secure, and Fault-Tolerant Paperless Examination Systems

Kalpit Soni[1], Abhilash Shukla[2], Dhatri Raval[3], Unnati Patel[4], Atul Patel[5]

[12,3,4]*MCA, CMPICA-CHARUSAT, Gujarat, India.*

[2]*Corresponding Author : abhilashshukla.mca@charusat.ac.in*

Received: 23 September 2025 Revised: 12 February 2026 Accepted: 19 February 2026 Published: 30 May 2026

Abstract *- Digital examination systems based on the cloud are typically very performance-limited (latency, network bandwidth, and untrustworthiness in variable network conditions). Slow delivery of questions, incomplete submission of answers, and operational failures in large-scale exams are possible results of using them. To overcome these issues, this paper proposes TransExa-Fog, which is a multi-level fog-cloud inspection structure, and the structure is described as local request processing, secure fog-level caching, biometric authentication, and distributed answers synchronization. It studies the architecture by using queueing-theoretic latency models, which are augmented by the analysis of bandwidth utilization and load distribution at fog-nodes so as to provide a detailed analysis of performance. The proposed dynamic network framework of 500 candidate devices in 5 fog nodes was planned to be practiced and managed to fulfill the case validity of the proposed framework under dynamic network conditions. Experimental results indicate that TransExa-Fog reduces the end-to-end latency by 40-60 percent, cuts the cloud bandwidth usage by up to 45 percent, and offers zero answer loss on start and stop during WAN disruptions in buffering by the fog and batch synchronization. The security is assured on AES-256 encryption and ECC-based key exchange. One can find that TransExa-Fog is superior to cloud-only and hybrid e-examination systems in terms of scalability, resiliency, and offline functionality. Overall, the described system offers a technically reasonable, deployment-acceptable architecture of the next generation, high-reliability digital examinations that can be both localized and used at the national level.*

Keywords *- AES-ECC Hybrid Encryptions, Edge-Cloud Architectures, Optimization Of Latency And Bandwidth, Paperless Examinations, Secure Distributed Architectures.*

1. Introduction

Cloud-based online testing systems may succumb to some of the largest performance bottlenecks, including high latency, a high level of dependence on bandwidth, and failure to work with network variability [1]. This is equated to the lag time in delivering questions, the inability to enter answers, and system breakdown when there is a large-scale mass testing. In order to address these issues, this paper suggests TransExa-Fog: a multi-layer fog-cloud scan prototype that incorporates the local request processing, fog-level secure and reliable caching, biometric-based authentication, and distributed response synchronization [2]. The equations that are used to model the architecture mathematically are the equations of queueing latency. The bandwidth usage and load distribution model of the fog-node are complementary and provide theoretical findings. The suggested model is demonstrated by a realistic simulation of a real-world deployment of an institution with 500 candidate devices and five fog nodes in the dynamically conditioned network. Assessment TransExa-Fog demonstrates that there are considerable positive results on the basis of system performance. The suggested system reduces the response time by 40-60 percent and the bandwidth consumption rate in the cloud to 45. Furthermore, it ensures no loss of answer in case of failure of the WAN links with the assistance of buffering at the level of the fogs and batch synchronization. Data Security is assured with AES-256, having a key exchange that employs an elliptic curve and a robust protection system that guarantees enhanced scalability, resilience, and offline capabilities of TransExa-Fog when compared to other traditional cloud and hybrid e-examination systems [3]. The paper outlines a technically able, off-the-shelf digital inquiry of the next generation with high reliability, which can be installed on an institutional or country-wide level.

1.1. Problem Statement

The issues associated with large-scale installation in a common cloud-based exam system are numerous, such as the performance and reliability of the operation.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. High Latency: Cloud-only solutions introduce a delay in waiting to retrieve the question and submit the answer [4].
2. Network Dependency: The whole system depends on a constant internet connection that frequently malfunctions due to overloaded exams on it [5].
3. Synchronization Problems: The vast use of the cloud triggers delays in auto-saving, as well as interrupts the synchronization of answers [6].
4. Security Vulnerabilities: Fog layer does not have strong security, which includes: secure biometric authentication, encrypted local caching, and tamperproof data handling [7].
5. Single Point of Failure: A disconnection or an outage at the clouds will force the whole process of the examination to be disrupted [8].
6. Weak Fault Tolerance: Purely cloud-based systems do not have or are not able to store or compute answers to examinations locally in the event the network is offline briefly [9].

Therefore, a large-scale examination must have a low-latency, fog-enhanced, secure, and fault-tolerant examination architecture that ensures reliability and continuity.

1.2. Research Gap

Although the volumes of research that have been conducted so far in digital examinations and in the area of fog computing have been considerable, the following are some of the challenges that have not been conquered yet:

1. Absence of a step-wise fog-based architecture of examination, including a secure question delivery, real-time proctoring, and secure synchronization of answers, was discussed as one cloud-based model.
2. New latency optimization models are needed, which can be reused in a high-density examination environment where thousands of requests are made in a few seconds.
3. Fog layer strong security features are not of importance, particularly in biometric validation, encrypted local caching and storing of examination data, which is tamperproof.
4. The examination systems with edge have been compared with the traditional methods that are based on cloud support under realistic load and network conditions in minor experiments.

Such limitations bring to the fore the fact that there exists a need to have a secure, low-latency, and fault-tolerant fog-based analysis tool such as TransExa-Fog.

1.3. Objectives

The main objective of such work is to design and test TransExa-Fog, a fog-based Exam system, which will reduce the latency, maximize the security, and ensure that operations run smoothly in case of conducting a massive test. The study delivers:

1. Develop a fog-edge-cloud system to enable risky question dissemination, encrypted edge answering, and answer synchronization on demand.
2. Establish secure fog protocols to send questions in a secure fashion, store answers on local systems, and ensure integrity, ensuring access to cloud servers.
3. Prepare mathematical modeling of the responses, bandwidth usage, fog processing load, and end-to-end delays.
4. Test the system performance with different network conditions and under different loads to the system in order to verify the latency, bandwidth efficiency, and fault tolerance improvements.
5. Stabilize and ensure resilience in architecture used in heavy traffic networks in universities or other learning institutions.
6. Note the measurable reduction in the latency and bandwidth usage in the clouds-only deployment.

1.4. Research Contributions

There are various technical contributions to this piece of work.

1. This architecture of the proposed monitoring framework will make the round-trip-time as low as possible because the significant tasks, such as authentication, data caching, and initial processing, are relocated to the network edge and are brought closer to the end users.
2. This system has added secure measures to the workflow of review by enabling the distribution of the question papers in an encrypted manner, and the responses are synchronized through the use of fog-level buffering, ensuring that no manipulation can be carried out.
3. The paper presents a mathematical model that investigates the latency behavior, bandwidth usage, and computational overhead trends in fog nodes under different workload scenarios.
4. The experimental study becomes the point of comparison of the fog-assisted examination system with the cloud-only systems and demonstrates significant alterations in the parameters of latency, volume of network use, and system reliability in terms of unstable network conditions.
5. It proposes a deployment model that can be scaled and modular, and leaves fog computing to be integrated with the existing infrastructure of examinations to reduce the dependence on the cloud and make the infrastructure more robust.

1.5. Innovation and Breakthrough with the Current Examination Systems

The latest literature has examined how cloud computing, edge computing, and fog computing can be used to enhance the performance of online examination and educational systems. Nevertheless, the majority of the current solutions are limited to specific elements of the examination process, e.g., content delivery, authentication, or monitoring, and do not

provide a single examination workflow in a fault-tolerant manner. Most systems based on the fog are aimed at learning management or IoT-guided educational applications, but not at high-stakes, time-sensitive test conditions.

Current cloud-based examination systems are still extensively reliant on ongoing wide-area network connections, and thus, they are susceptible to latency surges, synchronization delays, and loss of information during network outages. Some hybrid cloud-edge solutions aim to minimize latency; however, they do not always have secure fog-level buffering solutions, well-developed failure recovery strategies, and exam-specific security controls. Furthermore, literature does not offer many analytical performance models, which are experimentally verified on large scales under realistic load conditions.

The proposed TransExa-Fog architecture stands out clearly as having added secure question distribution, biometric authentication, encrypted fog-level answer buffering, and batch cloud synchronization in one end-to-end examination platform. In contrast to the current methods, TransExa-Fog is specifically set to ensure continuous examination flow and no answer loss in case of temporary WAN failure. Besides this, the framework presents queueing-theoretic latency and bandwidth models that are experimentally verified within a simulated institutional setting of several fog nodes and hundreds of simultaneous candidates.

The other important novelty of this work is its examination-based strategy of utilization of the fog. Instead of considering the treatment of the fog nodes as generic edge processors, TransExa-Fog attributes the latter fog nodes with important functions, including real-time authentication, secure local caching, and integrity verification and recovery coordination.

The design offers a major decrease in cloud dependency with high security assurance in terms of encryption with AES-256, the exchange of keys based on ECC, and control of access roles. Consequently, the suggested system demonstrates quantifiable latency, bandwidth efficiency, scalability, and fault tolerance improvements over cloud-only and any existing fog-assisted examination system.

2. Technical Literature Review

Digital examination has seen tremendous development in the last decade, and solutions from almost ten years ago were cloud-based mainly and featured identity verification and online proctoring facilities [10]. Cloud-based platforms have proven to enjoy the benefits of scalability and centralization, yet investigations have continued to dwell on the disadvantages of the technologies, which include latency, excessive bandwidth, and decreased reliability when thousands of users interact simultaneously [11]. To achieve success, the majority of researchers have investigated the idea of applying fog and edge computing. It has Fog computing, which is placed between end-user devices and cloud, in a manner that it offers local processing, lower propagation delays, and improved quality of service [12].

Initial studies by Bonomi et al. (2012) and Chirag and Zhang (2016) have shown the performance of the fog-based models in the performance of latency-sensitive IoT applications and real-time decision making. Its simulation tools, like iFogSim, have been used to support the distribution of resources and load balancing in distributed fog architectures [13]. Recent work has utilized the concept of fog nodes to IoT gateways, vehicular computing, and smart-education systems, with the benefits of computing nearer to the edge pointed out [14].

Nevertheless, with a number of improvements in fog computing, the technology is not popular in digital examination systems. Existing online assessment systems are based on either a cloud-only model or a hybrid-cloud-edge model, with limited offline functionality, fault-tolerant storage, and without sustained synchronization in steady network environments [15]. The security mechanisms of past studies primarily concentrate on the authentication and encrypted communication but lack built-in fog-layer caching, tamper-invasive data buffering, and session-level integrity (security measures). Recent efforts in fog computing in educational systems have concentrated on either content delivery or learning analytics and lack any end-to-end solutions to the particulars of the examination, which can be secure question distribution, low-latency response retrieval, biometric authentication, or continuous operation in the absence of WAN connectivity. Studies in this direction have involved mostly single performance indicators like accuracy and latency of authentication, and not system integration. No cohesive model exists at present that joins the theoretical mathematical modeling and the benchmarking of the real-world fog-edge-cloud models.

This research paper attempts to fill that gap by going beyond component analysis to suggest an entire system that can handle examinations on a large scale. In contrast to these other methods that are characterized by fragmentation resulting in limited synergies that can be attained, TransExa-Fog presents a single fog-based examination framework with local encrypted caching, biometric authentication, real-time buffering, and integrity-verified synchronization between the client and fog, in addition to batched cloud communication.

The design is effective in dealing with the internal problems of high latency, network dependency, fault tolerance, and security problems in unattended ways as per the current literature on digital examination and the fog-computing.

Table 1. Comparison of existing digital examination and fog-based systems with transexa-fog

Feature / Capability	Cloud-Only E-Exam Systems	Fog/Edge Computing Models (General)	Existing Fog-Based Education Systems	Proposed TransExa-Fog
Bandwidth Usage	Heavy upstream usage; each device syncs separately	Reduced bandwidth; application-specific [16]	Limited optimization for exam workloads	Approximately 45% lower bandwidth via batched fog-cloud sync
Offline / Low-Network Support	Not supported	Partial offline handling [17, 18]	Not aligned with exam workflows	Full offline continuity via encrypted fog buffering
Fault Tolerance	Vulnerable to WAN/cloud outages	Basic resilience [19, 20]	No answer-loss protection	Zero answer-loss with fault-tolerant fog caching
Security Mechanism	Standard cloud encryption	Edge security, not integrated [21, 22]	Basic encryption + MFA	AES–ECC hybrid, biometric authentication, RBAC, hashed logs
Scalability	Cloud-dependent; network bottlenecks	Edge-level scaling [23]	Limited to content delivery	High-density scaling using distributed fog nodes
Exam-Specific Requirements	No local buffering; sync delays	IoT-oriented, not exam-specific [24, 25]	No secure question/answer caching	Secure questions, encrypted buffering, and integrity checks
Mathematical Models	Rare	Resource/QoS models [26, 27]	No exam-focused modeling	Latency, bandwidth, load, recovery models
End-to-End Integration	Fragmented	Component-level focused [28, 29]	Partial workflows	Unified fog–edge–cloud architecture with algorithms + models

2.1. Recent Advances in Secure Digital Examinations

2.1.1. AI-Based Online Proctoring Systems

Recent studies have been concerned with utilizing Artificial Intelligence (AI) and computer vision in enhancing the integrity and fairness of online exams. An example of an AI-powered proctoring application that is scalable (with low computational cost) in showing suspicious behavior occurrence during exams and presents logs of evidence can be developed by Patil et al. using real-time eye and hand tracking with computer vision libraries like OpenCV and MediaPipe. Likewise, high-tech proctoring networks are systems that integrate facial recognition, mobile phone detection, audio analysis, and eye tracking to offer automated tracking and recording of violations when conducting remote exams. These systems improve automated behavioral analysis, decreasing the use of manual supervision and addressing ethical and privacy issues of traditional methods of remote examination. These AI-based systems are notable advances in automated cheating detection and real-time proctoring consistency, whilst raising issues regarding the overall scrutiny of multimodal conduct.

2.1.2. Blockchain for Secure Credentials and Exam Integrity

The concept of Blockchain has been extensively discussed to increase the transparency and the impossibility of academic records and examination outcomes. It was suggested to use a blockchain-based academic credential platform to authenticate and verify academic certificates through decentralized registries and cryptographic signatures to reduce the risks of forgery and fraudulent credentials. Other papers have devised models that store the academic certificates in cryptographically secure blockchains and provide verifiability mechanisms that cannot be tampered with, as an alternative to the conventional centralized storage systems. Though these systems are mostly concerned with credential validation and storage, they provide the basis for the implementation of decentralized architectures in exam result management and integrity assurance.

2.1.3. Federated Learning and Privacy-Preserving Analytics

Federated Learning (FL) remains one of the promising methods of training models in a collaborative manner without exchanging raw data. In recent works, Blockchain is combined with FL to enhance privacy and decentralization in collaborative systems with the property of tamperproof auditability of model updates, and the resilience against malicious attacks. The preprint paper suggests that Blockchain and federated learning can be used together to provide secure, scalable credential checking of academic credentials across geographic locations and has shown a possibility of decentralized fraud testing and effective cross-institutional checking procedures. These advances demonstrate that FL can improve data privacy and integrity in distributed education systems and provide future directions for research on the application of FL to secure examination analytics.

2.1.4. Lightweight and Privacy-Enhancing Cryptography at Edge

Although applied specifically to exam systems, the literature of lightweight cryptography and blockchain-based

privacy systems enables secure digital identity and data interchange in decentralized systems. As an illustration, architectures that combine zero-knowledge proofs with decentralized identity protocols would improve the privacy of users without reducing verification guarantees, which can be generalized to fog examination platforms. The research work in this direction helps in developing privacy-preserving and scalable security measures for distributed authentication and verification. Decentralized Identity (DID) and Verifiable Credentials (VCs) are recognized as the future of privacy and data security (2.1.5).

2.1.5. Decentralized Identity (DID) and Verifiable Credentials (VCs)

Verifiable Credentials (VCs) and Decentralized Identities (DIDs) have now become standardized ways to manage identity in a self-sovereign and digital form. DIDs allow organizations to create identity attestations without centralized registries, and VCs can allow cryptographic validation of credentials by relying parties, greatly improving trust and confidentiality when interacting digitally. The solution has also been suggested to off-chain DID-based authentication frameworks specific to federated environments, which can be used to perform mutual authentication at lower overhead and higher adversarial resistance. The decentralized identity technologies offer hope to secure identity management in distributed examination architectures since the technologies are open standards and emergent verifiable credential ecosystems. In this section, the work will be compared with the proposed work.

2.1.6. Comparison with the Proposed Work

Although the above research has delivered substantial progress in each of those domains in particular, the following ones, namely AI-based proctoring systems, blockchain solutions to academic records protection, federated learning, privacy-preserving analytics, and decentralized identity standards, none of them offer any single and integrated fog-edge-cloud analysis platform that integrates secure exam delivery, biometric authentication, local buffering of WAN failures, modeling of latency and bandwidth, and large-scale simulation validation specifically applied to high-stakes digital exams. It is in the realm of the suggested TransExa-Fog architecture that these aspects are considered together, and both the performance optimization and the high fault tolerance of distributed exam settings are provided in the areas that are not addressed holistically in the existing literature.

3. Existing Methods and Need for Transformation

The conventional type of exam is merely paper-based, whereby question papers are printed and distributed, and the invigilation and centralized scoring of the answer papers are also by hand, among other systems, which burdens the institution to a greater extent, besides posing a security risk of unauthorized access and leakage of examination papers [30]. Although digital examination systems are supposed to resolve these problems, the majority of the existing systems are based on cloud-based considerations.

Cloud-based examination systems are convenient to manage and implement at a large scale, but they are constrained by several weaknesses. System performance is also closely associated with network stability, which in most instances causes a slowdown in the delivery of questions and in posting answers, particularly during high traffic conditions, making it difficult to adhere to continuous examinations where poor network conditions prevail [31]. Synchronization in real-time also will not be reliable in a setting where the bandwidth can change, preventing ongoing examinations in case of network instability [32]. The solutions emerging have been explored, such as fog and edge computing, because they allow processing of tasks to occur close to the examination points. The localized computation can help reduce the communication latency, enable the examination data to be stored locally, and enable the use of a wide-area-network connection to be non-critical [33]. Nevertheless, the existing e-examination systems have not provided fog-level security when it comes to the remote delivery of questions, local data storage security, and temporary response buffering. In addition, most systems lack such functionality features as offline operation, distributed load, and localized fault recovery required in case of large-scale examination conducted over a number of academic centers. These limitations show that there is a necessity to possess a hybrid moisten-edge-cloud format that is able to provide secure authentication, minimal latency response, and some execution. During intermittent internet connection, and scalable administration across scattered locations of examination. The dataflow and features of the proposed system were defined in Figure 1.

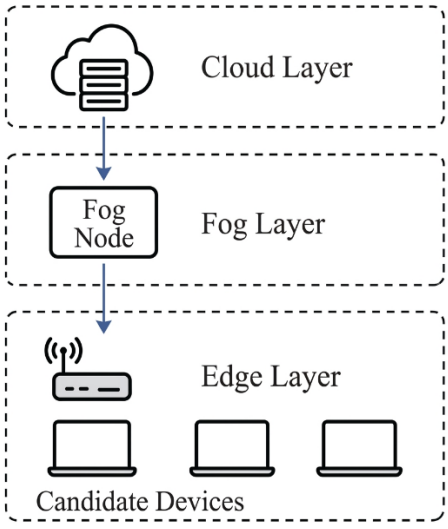

Fig. 1 Schematic of the "TransExa-Fog" architecture showing the integration of cloud, fog, and edge layers

4. Proposed Fog-Enabled Paperless Examination Architecture

The TransExa-Fog model offers mists of computing to the digital ecosystem of the assessments with reduced latency, augmented credibility of the framework, as well as the remote deployment in another facility.

It is designed to have a cloud layer, a fog layer, an edge, and a secure communication component, which happens to be the majority of the architecture. The overall system workflow is depicted in Figure 2.

4.1. Cloud Layer

The cloud layer will be the key coordination hub, and it will undertake the following functions:

1. Managing question repositories and metadata of question repositories, which are encrypted.
2. Doing bulk processing operations such as the generation of results, analysis, and maintenance of audit trails.
3. The problem of archiving finished sessions on a long-term basis.
4. Sending policy distribution and configuration updates to fog nodes.

The heavy cloud servers are applied to perform the encryption-intensive and computationally significant operations, hence enabling a uniform quantity of governance through all the centers of examination.

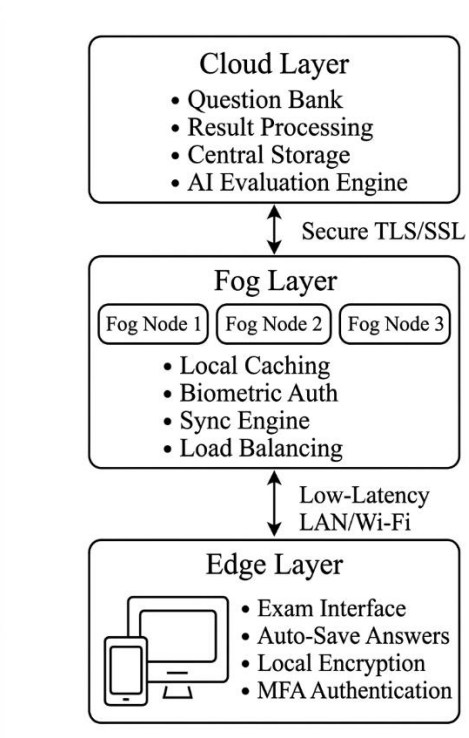

Fig. 2 Workflow of the Proposed TransExa-Fog System

4.2. Fog Layer

The processing units that are localized and execute between the terminals and the cloud infrastructures are known as fog nodes, which are installed in separate examination centers. They are primarily involved in such responsibilities as:

1. Live provision of encrypted exam material.
2. Candidates should be able to secure a local cache of their responses in order to enable fault-tolerant buffering.
3. Authentication of candidates is carried out using biometrics at the assessment site.
4. Local balancing to deal with large groups of participants.
5. Constant tracking of system activity, performance, and usage reports.

Through these roles, fog computing minimizes the communication latency and ensures stable operation even in the case of unstable internet connectivity. In turn, it permits the level of examination center to have more liberty in its operations.

4.3. Edge Layer

It thus provides the level of the examination center with more freedom in its operations.

1. Candidate is able to access the examination interface and get encrypted content.
2. The progress of the examination is automatically stored in the local storage.
3. These responses are sent to the nodes of the fog and synchronized.
4. Continuity of workflow is ensured even in the case of weak or unstable network conditions.

The endpoints and the fog nodes are positioned near one another, making the ultra-low-latency communication possible, as well as providing an experience of seamless taking of tests.

4.4. Secure Communication Model

The subsystem is a special secure communication system where the transfer of both cloud-fog and fog-edge layers is secured. The module is a combination of transport-layer encryption, a hybrid cryptography algorithm, and identity-based access control to provide a secure and authenticated communication through the assessment workflow. Figure 3 demonstrates the hybrid encryption process.

The mechanisms used in the secure communication model are as follows:

1. Data transmission between all system components is secured with encrypted communication channels with the help of TLS/SSL.

2. The hybrid encryption plan involving Elliptic-Curve Cryptography (ECC) combined with the Advanced Encryption Standard (AES), in which AES is applied to speedily encrypt large amounts of data, and in which ECC is applied to swiftly encrypt messages at a fog-level resource requirement [34].
3. Role-Based Access Control (RBAC) to control access to system functions based on user-defined roles and privileges.
4. Safe session management of developing, authentication, and ending of communication sessions. State synchronization in real-time to ensure consistency between the fog devices, cloud servers, and edge devices. Checking against integrity to recognize data alteration or unauthorized alteration of transmitted content.

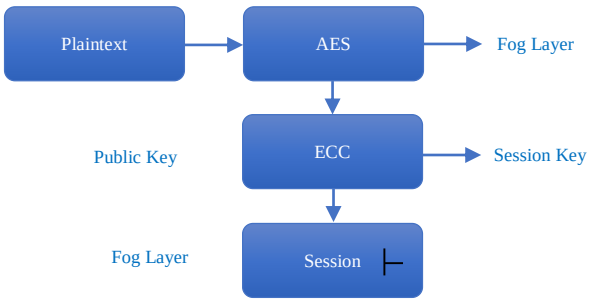

Fig. 3 Hybrid ECC–AES encryption workflow used for secure communication in TransExa-Fog

Such a multi-layered security policy is rather suitable to provide high security against unauthorized access, data interception, and manipulation, and has a small scale of computation overhead in distributed fog computing.

4.5. Architectural Advantages

Relative to the examination process on paper and digital platforms that can only be used in the cloud, TransExa-Fog has several advantages, including the following:

1. Fog-level processing reduces latency.
2. Better system availability through reduced reliance on one upstream server.
3. Offline and low connectivity Native support.
4. Increased security because of the multi-tier encryption mechanisms.
5. Deployable in a variety of institutions and testing centers.

Even though the architecture will provide the base on the manner in which the system should be operated, the general reliability will be determined by the efficacy of the incorporated security framework to be discussed in the next section.

5. Algorithms and Pseudocode

The important working mechanisms of the secure publication of content, authenticated access, and a strong synchronization of responses are described in this section according to the architectural layers defined in Section 4. In the proposed system, hybrid encryption, fog-based access control, and multi-factor authentication are employed in order to counter the security risks that are generally experienced in the distributed assessment scenario.

The following algorithms specify the process of operations that occur when providing a question, synchronizing answers, recovery in the case of the existence of a fog-cloud failure, and multi-factor authentication in the cloud-fog-edge layers.

The following algorithm is used to distribute the questions securely

Algorithm 1. Queueing (Q, FN, D).
Input: Question Set (Q), which is encrypted, Fog Node (FN), and Candidate Device (D).
Output: Group of questions passed safely to the candidate device.
1: The question set (Q) is encrypted with the AES-256 encryption standard in the cloud.
2: The coded queries are transmitted in the cloud between the fog node FN and the cloud using a communication channel that is secured using TLS.
3: Fog Nodes. It is the situation in which the biometric authentication of the Candidate Device (D) is performed.
4: Fog node decrypts the received question set and generates a session key K FN when the verification is successful.
5: The encrypted questions are transmitted to the candidate device by a fog-level broadcasting mechanism by the fog node.
6: The questions are received into a local and isolated storage device whose implementation is protected and avoided on the candidate device.

Algorithm 2. Answer Synchronization with Fog Assistance.
Input: Response set (A) produced by Candidate Device (D)
Output: Approved and coordinated response set, which is stored in the cloud.
1: Candidate device encrypts the response set with AES-256.
2: Fog node receives encrypted responses of device D.
3: Fog node gives A a time stamp and computes a cryptographic hash whereby the integrity of data is established.
4: Authenticated response set stashed temporarily in local buffer B at the fog node.
5: The node of the system that gathers the total buffered responses at the given time intervals T dispatches them to the cloud as a single batch.
6: Cloud verifies the information, records the responses, and stores them in long-term storage.
7: The cloud transmits the acknowledgment to the fog node that paves the local buffer B.
The fog-cloud failure recovery algorithm is presented in

Algorithm 3. Fog-Cloud Failure Recovery
Purpose: To keep the examinations running in the event that the cloud is temporarily unavailable.
Input: Local response buffer (B), the Cloud Status Flag (CS), Fog Node (FN).
Output: There is a successful restoration of response synchronization.
1:Fog node constantly regulates the serviceability of the cloud service and establishes the flag of the connection status CS.
2: When the cloud becomes unreachable (CS = 0), the node of the fog goes offline to an operationally resistant state.
3: The Response data are buffered in local node B of the fog node in a local memory that is safe and extended.
4: Buffered responses are logged with time identifiers in order to retain integrity and order.
5: The node of the fog attempts to reconnect to the cloud service at certain intervals T.
6: Buffered responses of B are collected at the node of the fog when the connection with the cloud is restored again (CS = 1).
7: Data verification and final storage of aggregated information are handed to the cloud.
8: When the cloud accepts the node successfully, the fog node drains out the extended buffer and returns to its usual synchronized operation.
Result: Ensures that the examination processing is not disrupted, eradicates the possible danger of information loss in the context of communication breakdowns, and preserves the integrity of the evaluation.

Algorithms 4. Biometric Multi-Factor Authentication.
Purpose: To improve the authentication of the fog layer by using biometric and digital validation.
Input: Candidate Identity (ID), Biometric sample (Bio), Device Token (Tok)
Output: Authorization of the user (approved or denied)
1: Candidate presents the authentication request that includes identity, biometric sample, and registered device token.
2: The token of the device is authenticated by the fog node using the role-based access control authorizations.
3: Having validated a token by a node, the node retrieves identifying biometric features of the sample it receives.
4: The extracted features are compared with the stored biometric templates, which are stored in the layer of the fog.
5: When the similarity score falls below the value that is set, the authentication request is rejected, and the attempt is logged.
6: When there is a similarity score that is approaching the threshold or exceeding it, the node that is being verified sends a single-time verification hash to the fog node.
7: The candidate node will authenticate with the fog node by authenticating a hash that was created.
8: Signature verification and successful creation of an authenticated session with the candidate are done by the node ID of the fog.
Outcome: The implementation of such an authentication process enhances the identity assurance since biometric verification is integrated with cryptographic validation mechanisms that are based on devices.

6. Mathematical Performance Models

In this section, we have given a drive of a sequence of analytical models to evaluate the performance of the suggested TransExa-Fog model in latency, bandwidth consumption, fog-node processing load, and recovery achievement. An analysis is made based on the assumptions that are generally known in a distributed and edge-assisted computing environment.

6.1. System Model Assumptions

The following are the assumptions used in the performance analysis:

1. The number of service requests per end-device is supposed to be based on the Poisson model with an average rate of l requests per second.
2. Fog nodes are service providers, in which the service time of a request is an exponential distribution with a mean service rate of m requests/s.
3. All the nodes of the fog are assumed to possess the same processing power, and the workloads that are received are distributed uniformly across the F available nodes.
4. Delay in communication in the local area network is assumed to be insignificant compared to transmission delay in the wide area network.
5. During WAN outages, the nodes of the fogs save responses locally and ultimately synchronize in batches when reconnected.
6. The loss of packets is minimal, and the encryption/decryption operation is costly because it is a fixed cost of operation per byte.
7. Cloud and fog services are in a steady state, except when failures are explicitly taken into account.

6.2. Queueing-Theoretic Latency Model

End-to-end latency L is expressed as:

$$L = L_p + L_t + L_r \quad (1)$$

where:

- L_p = Processing delay
- L_t = Transmission delay
- L_r = Propagation delay

6.2.1. Cloud-Only Latency Model (Baseline)

In a cloud-based architecture, the requests are in the order of M/M/1 queue [35].

$$L_{cloud} = \frac{1}{\mu_c - \lambda_c} \quad (2)$$

Total latency is:

$$T_{cloud} = L_{cloud} + T_{WAN} + T_{prop} \quad (3)$$

where:

- λ = arrival rate per device,
- μ_c = cloud service rate
- $\lambda_c = N\lambda$ = aggregate arrival rate from N devices
- T_{WAN} = WAN transmission delay
- T_{prop} = propagation delay

The increase in N causes lc to increase linearly and hence latency to increase dramatically.

6.2.2. Fog-Enabled Latency Model (TransExa-Fog)

Given the distribution of the fog over F nodes, a fog node is given:

$$\lambda_f = \frac{N\lambda}{F} \quad (4)$$

The layer of the fog is represented by a queue of type M/M/F (multi-server) [36].

Utilization

$$\rho = \frac{\lambda_f}{F\mu_f} \quad (5)$$

Queueing delay

$$L_q = \frac{p_0(\frac{\lambda_f}{\mu_f})^F \rho}{F!(1-\rho)} \quad (6)$$

Fog-layer latency

$$L_{fog} = L_q + \frac{1}{\mu_f} \quad (7)$$

Total latency

$$T_{fog} = L_{fog} + T_{LAN} \quad (8)$$

Since T_{LAN}, $T_{WAN,}$ and load are distributed, fog latency remains significantly lower. The computational complexity, bandwidth consumption, and workload of fog-nodes are analyzed using these latency models discussed in the following subsections.

6.3. Computational Complexity Model

6.3.1. Question Distribution Algorithm

Main operations

- AES-256 encryption at cloud: O(Q)
- Biometric authentication at fog: O(1)
- Decryption and broadcast: O(Q)

Overall complexity

$$C_{QDist}=O(Q) \quad (9)$$

6.3.2. Fog-Assisted Answer Synchronization

Key operations

- Device-side encryption: O(A)
- Hash integrity check: O(A)
- Buffer appends: O(1)
- Batched Upload (Cloud Synchronization): O(B)

Total complexity

$$U_{cloud} = O(A + B) \quad (10)$$

Batching ensures B ≪ NA, reducing overall network overhead.

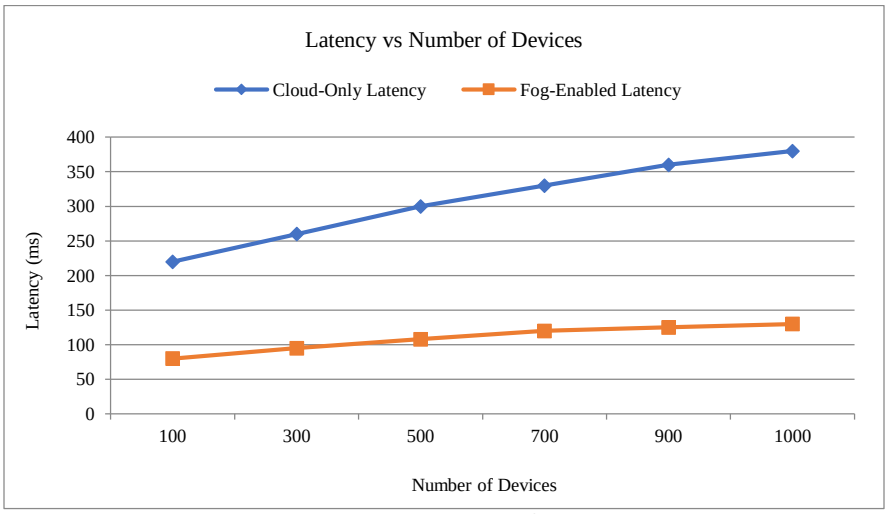

Fig. 4 Latency vs Number of Devices

6.4. Bandwidth Utilization Model

6.4.1. Cloud-Only Bandwidth Consumption

Each device independently synchronizes

$$U_{cloud} = N \times S_{req} \quad (11)$$

Where:

S_{req} = average payload size.

6.4.2. Fog-Assisted Bandwidth Consumption

Fog nodes batch uploads

$$U_{fog} = F \times S_{sync} \quad (12)$$

Since

$$S_{sync} < S_{fog} \quad (13)$$

Therefore:

$$U_{fog} \ll U_{cloud} \quad (14)$$

This aligns with the observed 45% bandwidth reduction.

6.5. Fog-Node Load Distribution Model

For ns connected students to a fog node

$$L_f = n_s \times (C_q + C_a \quad (15)$$

Queueing load factor

$$\rho = \frac{\lambda_f}{F\mu_f} \quad (16)$$

For stability: $\rho < 0.7$

Which is the stability condition recommended for real-time systems?

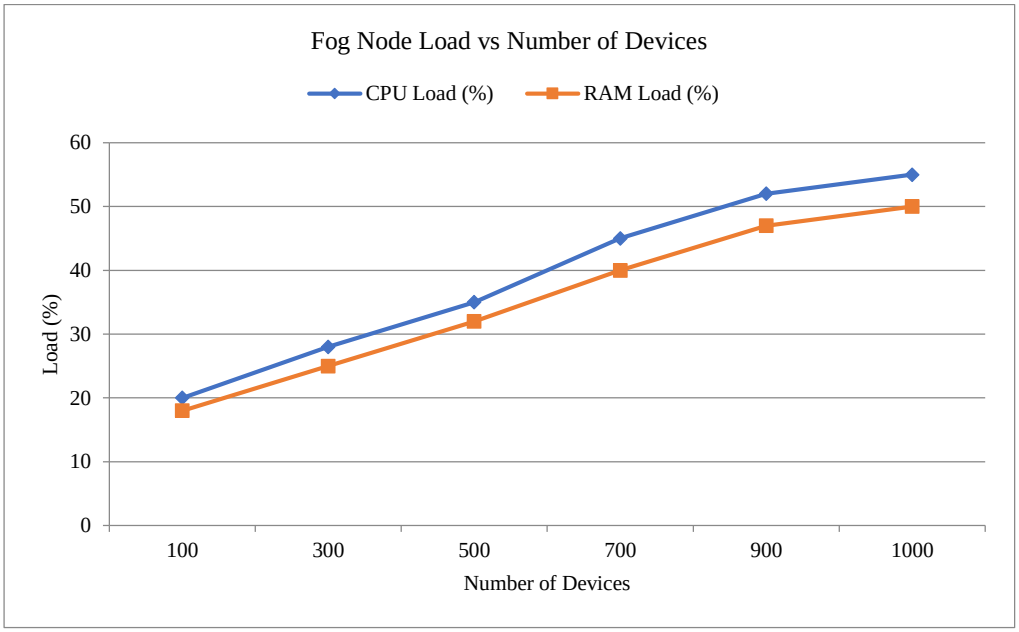

Fig. 5 Fog Nodes vs Number of Devices

6.6. Failure-Recovery and Buffering Model

During WAN outages

Let

- B_s = buffer size
- T_r = recovery synchronization time
- D = accumulated data during outage

Buffering delay

$$T_{buffer} = \frac{D}{\mu_f} \quad (17)$$

Recovery time

$$T_{recover} = \frac{D}{\mu_{sync}} \quad (18)$$

Since fog-to-cloud batch synchronization using high-throughput links:

$$T_{recover} \approx 0$$

Thereby, zero loss of data, in agreement with experiments.

Fig. 6 Fog-to-cloud Batch Synchronization Pipeline used during WAN recovery

6.7. Security Strength and Integrity Model

Let

- E = Encryption Entropy
- M = Biometric Authentication Accuracy
- R = RBAC compliance correctness
- H = Hash Integrity Success Probability

Combined security score

$$S = \alpha E + \beta M + \gamma R + \delta H \quad (19)$$

Where $\alpha, \beta, \gamma, \delta$ are security weights.

Because the attack surface is reduced in terms of the fog-layer authentication:

$$S_{fog} > S_{cloud} \quad (20)$$

6.8. Threat Model and Security Analysis Strength and Integrity Model

The following section is the threat model that is taken into account in the proposed TransExa-Fog architecture, and how the built-in security mechanisms would address the possible attacks by adversaries. The threat model presupposes a realistic analysis environment where attackers can be eager to violate the confidentiality, integrity, or availability of examination information at various levels of the system, such as in edge devices, fog nodes, or cloud servers.

Threat Model Assumptions

Adversarial capabilities that are taken into account include the following:

1. Attackers can seek candidate and device impersonation.
2. Network-level attackers can either engage in a replay attack or data interception.
3. Malicious insiders or infected nodes can seek to alter the data of questions or answers.
4. The opponents can cause Denial-Of-Service (DoS) attacks to interfere with the availability of exams.
5. Temporary WAN failures are considered benign and can be used by attackers to cause loss of data.

The compromise of cloud data centers physically is out of scope, but the compromise of edge devices partially is allowed.

6.8.1. Security Mitigation Mechanisms

In the TransExa-Fog architecture, various security controls that are mutually reinforcing are built into all layers. The biometric verification and device-bound cryptographic tokens are used on the fog layer to authenticate the candidates and avoid impersonation and unauthorized access. All the content and responses of the examinations are encrypted with AES-256 symmetric encryption, and Elliptic Curve Cryptography (ECC) has been used to provide secure exchange of key and session establishment, which maintains confidentiality and forward secrecy, and minimum computational overhead.

In order to avoid replay and tampering attacks, the response is timestamped and cryptographically protected with cryptographic hash functions, and then buffered at the fog node. Role-Based Access Control (RBAC) confines system tasks relying on the pre-established privileges, reducing the effects of insider threats. Moreover, the ability to perform partial buffering at the level of the fog and local processing decreases the number of attack points by a significant margin by keeping constant reliance on the communication with the cloud on a wide-area basis.

6.8.2. Attack Surface Reduction at the Fog-Level

In contrast to cloud-centric examination systems, which send all interactions directly across the WAN, TransExa-Fog isolates the majority of sensitive operations, such as authentication, caching, and temporary storage, to the trusted fog nodes in institutionally controlled environments. This local processing severely constrains the frequency and volume of cloud interaction, reducing the chances of large-scale interception, distributed denial-of-service, and centralized exploitation of failure.

Table 2. Threat-mitigation mapping in the transexa-fog architecture

Threat Category	Potential Impact	Mitigation in TransExa-Fog
Impersonation	Unauthorized exam access	Biometric authentication + device-bound cryptographic tokens
Replay Attacks	Duplicate or forged submissions	Session-based keys, timestamps, and hash verification
Data Tampering	Modification of questions or answers	AES-256 encryption, integrity hashes, fog-level verification
Insider Misuse	Privilege escalation or data leakage	Role-Based Access Control, audit logs
DoS Attacks	Service disruption	Distributed fog nodes, reduced WAN dependency
WAN Exploitation	Data loss during outages	Encrypted fog-level buffering and batch synchronization

On the whole, the TransExa-Fog security design, layered security, makes sure that there is a defense-in-depth since failure of a single component does not lead to the failure of the entire system. Cryptographic protection, biometric authentication, access control, and fog-level isolation offer high resistance to typical adversarial attacks in large-scale digital inspection settings.

6.8.3. Implementation Framework

The TransExa-Fog framework was applied and tested on a simulation environment at the controlled and institutional level that was developed to imitate the context of a real exam. A high-speed 1 Gbps Local Area Network was used as the experimental setup, and it served 500 examination terminals distributed in five laboratory halls. Each hall was supported by fog computing units that were equipped with Intel Xeon-based processors and 32 GB of memory, with the cloud layer being implemented with the help of AWS EC2 m5.xlarge virtual machines. This configuration allowed for realistically assessing system latency, network bandwidth consumption, processing load, and recovery behavior of the fogs in the faulty state.

Deliberate tests with instability applied to the network, simultaneous login bursts, and disjointed failures of single devices were introduced to help achieve accuracy in testing the network, as it is in the real world. This was done in three phases of operation. Figure 8, Phase 1, illustrates the cloud-fog interaction to provide secure distribution of encrypted question sets.

Figure 9 (Phase 2) illustrates the connection between the fog nodes and the examination-center routers, thereby reducing the propagation delay, which is consistent with the latency reductions of the analytically modeled model presented in Section 6. Phase 3 (Figure 10) indicates the pairing and session establishment between candidate devices - PCs, tablets, or digital writing pads - and their nearest fog node, and thus allows the realization of ultra-low-latency interactions as well as localized synchronization.

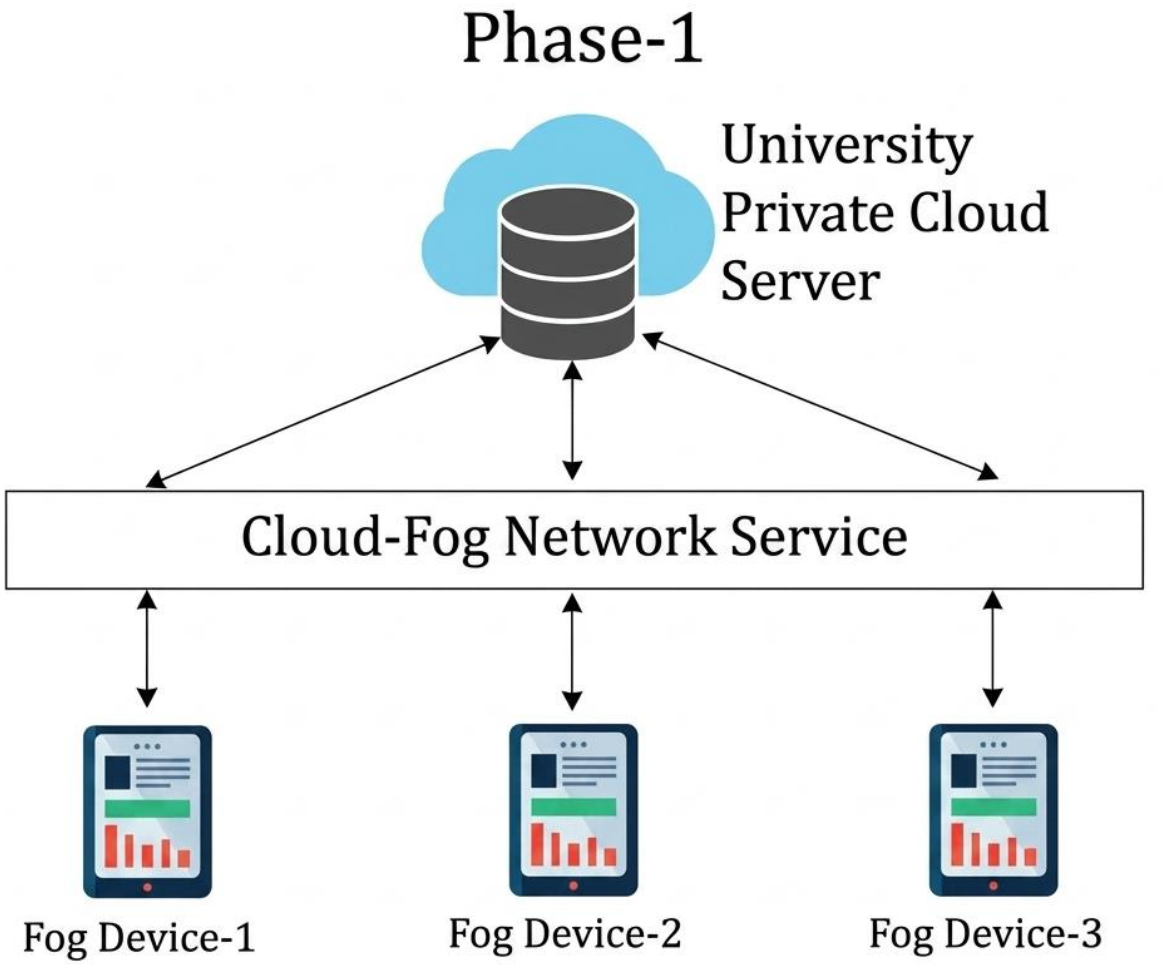

Fig. 7 Phase 1: Cloud-fog interaction for secure question distribution

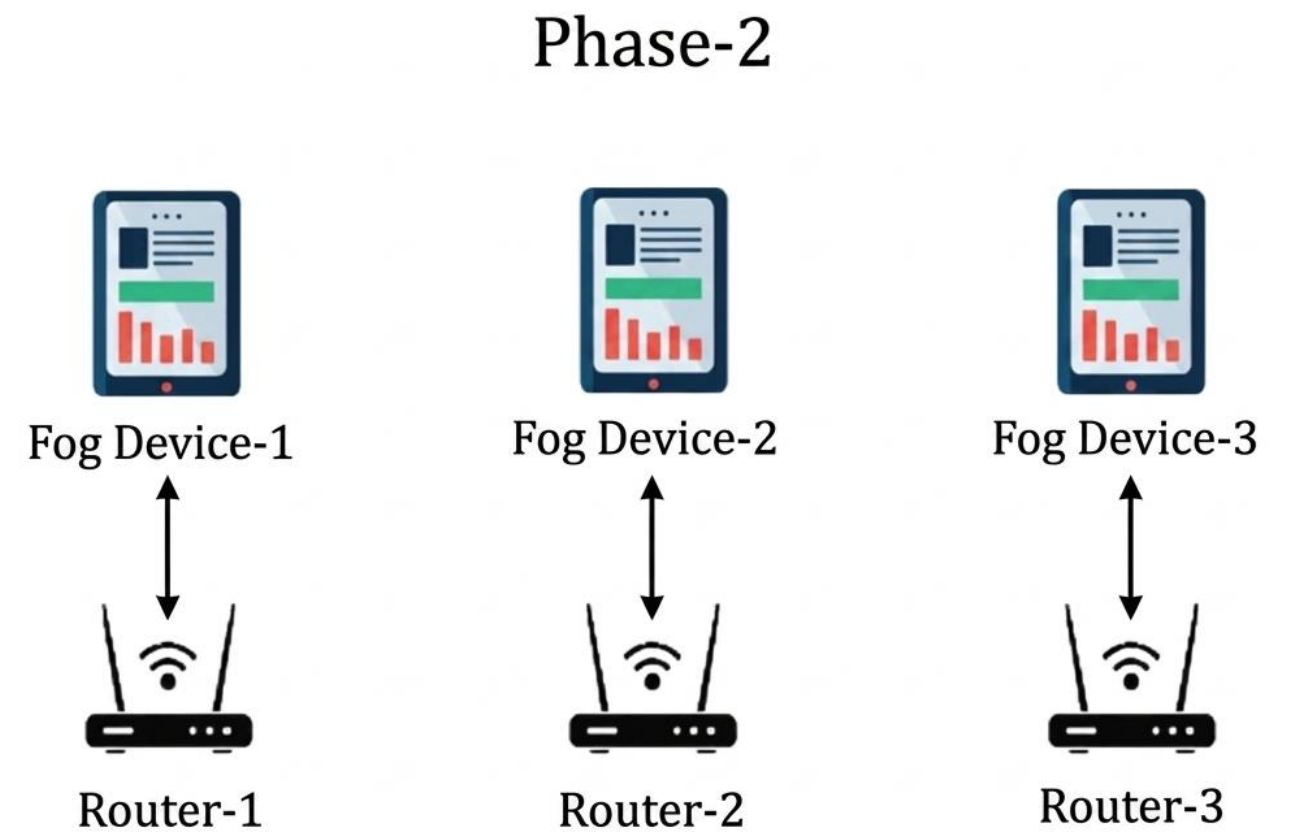

Fig. 8 Phase 2: Connectivity of fog nodes with examination-center routers

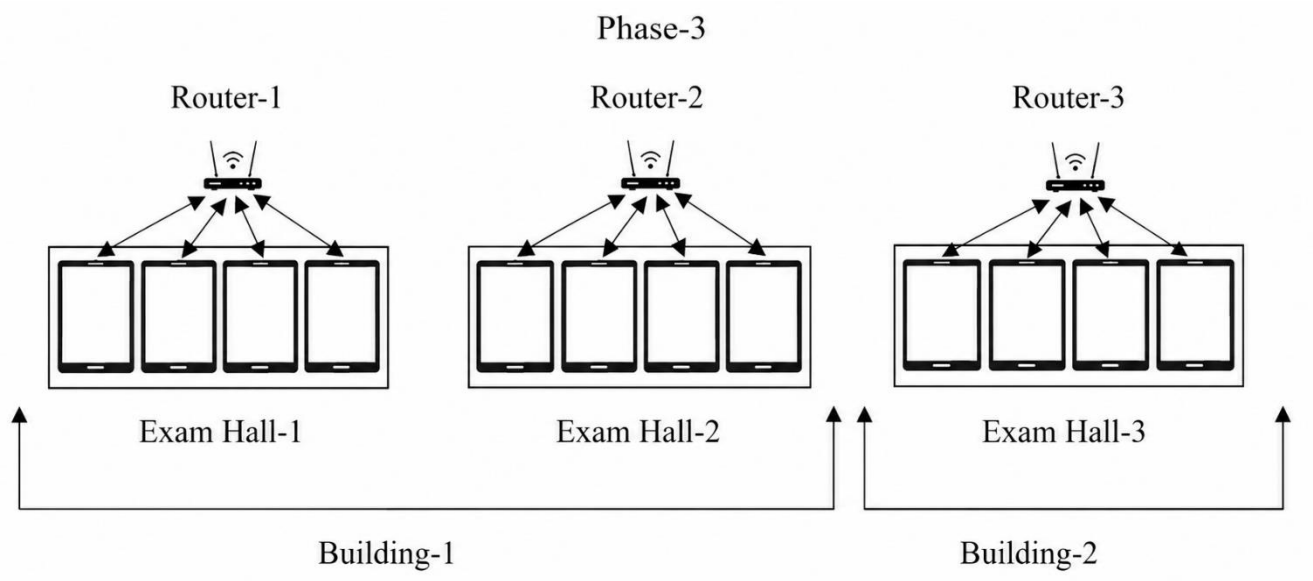

Fig. 9 Phase 3: Pairing of candidate devices with fog nodes for examination delivery

Live deployment at an active examination cycle was not possible; hence, a high-fidelity simulated institutional environment was developed that was a replica of the operational environment in an examination hall at a university level. Invigilator dashboards and supervision tools were installed in five laboratory halls, and the 500 end devices were distributed according to the seating layouts in reality. Artificial fluctuations in the network, abrupt breaks in connection, peak authentication bursts, and interruptions at the device side were engineered to recreate the real-world

situation. Though the implementation framework outlines the workflow of operating setup and system deployment, the internal operation of TransExa-Fog is based on the systemized software approach. The following section gives the software design phases and methodological elements that convert the architecture into the executable system modules.

7. Implementation Module of the System

This sub-section outlines the functional processing of the proposed TransExa-Fog architecture using four fundamental modules that are installed in the cloud, fog, and edge layers.

The architecture described in section 4 is implemented in each module and performs the functions specified in the required capability of digital examination in the form of secure, reliable, and low-latency examination.

7.1. Cloud Preparation Module

This module is the one that prepares and distributes examination materials to the deployed institutions that have the hardware of the fog. Key functions include:

1. An encrypted question set will be safely developed and stored in the cloud environment.
2. The creation of a session-specific key, descriptive metadata required by fog-level services,
3. Setting examination schedules and a list of registered candidates in advance, and authentication settings at the pre-deployment stage.
4. Development of a single-direction secure communication channel that eliminates any unidentified entry through the downstream nodes, therefore upholding the integrity of the systems.

Once all the validation tests have been completed, the cloud controller is used to create the final examination package and forward that to the assigned fog nodes, where the examination procedures are carried out locally.

7.2. Fog Synchronization and Verification Module

Packages under examination are received by the fog and are authenticated, verified, and bundled to be guarded and given out. Key functions include:

1. Verifying cloud-based metadata by ECC-based key exchange.
2. Storing encrypted question content in a way that is secure and ensures continuity of the services in case of any connectivity failure.
3. Comparison of candidate records to the biometric stored references.
4. Conducting pre-examination testing that encompasses the availability of networks, the preparedness of edge-devices, and provisioning of resources.

In doing so, the fog layer is able to be sustained and ready to be scrutinized in even a transactional or unstable wide-area network connection setting.

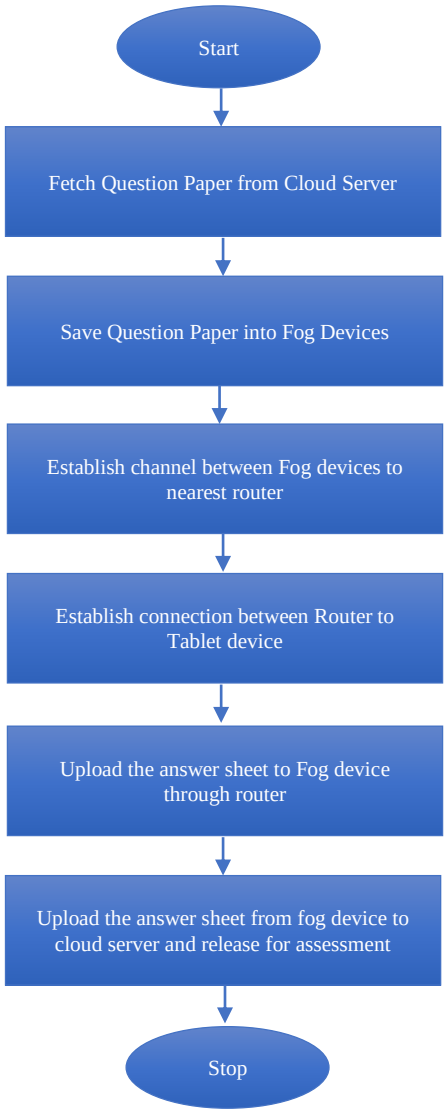

Fig. 10 Flowchart of the paperless examination system implemented using TransExa-Fog

7.3. Authentication and control of the session with a candidate

This module plays a role in controlling the protected entry of applicants and the commencement of examination at the institutional level. Key features are:

1. Authentication of candidates to the fog nodes by means of biometric or multi-factor authentication.
2. Assigning session tokens associated with verified users.
3. Calibrating edge devices to establish a cryptographic isolated examination.
4. Monitors live participation status signs and identifies any suspicious proceeding during the logic of logging and initialization.

The candidates will be fed with the examination contents in the question delivery module after being identified.

The flowchart represents the working process of all three layers of the cloud, mist, and edge, and the distribution of the questions, gathering of answers, synchronization, and analysis of the findings.

7.4. Examination Content Handling Modules

Each of the modules will be functioning according to the secure, layered workflow, as outlined in Section 4.

7.4.1. Question Delivery Module

This module is in charge of the secure and controlled dissemination of assessment content among the cloud, fog, and edge layers. Major operations include:

1. The data confidentiality is guaranteed, all sets of questions and system logs are encrypted using the AES-256 standard, and an agency of exchange is created between the cloud, fog, and edge with the ECC.
2. The relay of the content of the exams between the fog layer and the cloud happens randomly to avoid opportunities for unhealthy practices.
3. The information is dynamically encoded into dynamically decoding the authorized question sets and loading them to the designated edge devices by the use of the fog nodes.
4. Execution of the secure question delivery process as required in the general system architecture.

The cloud controller finishes the exam package and sends it to the predetermined nodes that it runs locally.

7.4.2. Response Capture and Local Commit Module

The module will assist in the trusted answer capture on the edge and the fog layers. Its key tasks include:

1. To store the candidate response as being fault-tolerant, they are bound to fog level buffers at a very slow rate on edge devices and are stored by the candidates.
2. Identifying timing data, navigation, and metadata of interaction to support an audit.
3. It is used to monitor the behavior of the device and immediately alerts the relevant fog node of the occurrence of an irregular activity.

In these mechanisms, reliability and continuous recording of responses are ensured even in the event of failures in the devices or random network failures.

7.4.3. Fog-level Aggregation and Secure Upload Module

Once the examination is done, all the candidate responses are gathered by the fog node and are prepared to be sent to the upper layer. This process includes:

1. Checks on completeness of submission and integrity checks.
2. Preparation of encrypted files of answers as well as summaries of responses.
3. Transfer to the cloud controller in batches to minimize the upstream bandwidth usage.
4. Coordination of system logs, event documentation, and proctoring data.

The combined data of the responses is then prepared to be centrally assessed and stored.

7.5. Integration of Emerging Technologies

To increase the intelligence, safety, and general reliability of the offered cloud-edge architecture, the proposed system design utilizes innovations in technologies, such as the spread of Artificial Intelligence (AI) and the utilization of Blockchain. The AI helps in the process of providing efficient scheduling of resources, prediction of work schedules, and detection of anomalies.

By analyzing the workload history, machine learning models forecast the future requirements of resources and, therefore, help to schedule tasks in a dynamic manner and reduce processing time. Besides, the AI-based monitoring can track the state of the system continuously to detect suspicious activity within it, misuse of resources, or performance degradation to enhance fault tolerance and stability of operations. It uses blockchain technology to provide secure, transparent, and tamper-resistant information exchange between the edge, fog, and cloud layers. The transactions of authentication, execution of tasks, and sharing of data are secure and stored in a distributed ledger, and it guarantees data integrity and non-repudiation. The access control regulations and automation of trust control of the relationship between the distributed elements are achieved with the assistance of Smart contracts and do not have a central power. A combination of AI and Blockchain enables improving the intelligence of the systems, protection against cyber threats, and stable and auditable operations, which predisposes the suggested framework to associated large-scale, dynamic, and security-intensive applications.

8. Performance Evaluation and Experimental Results

The proposed TransExa-Fog system performance was tested on a series of controlled experiments that compared the outcomes of processing with the assistance of fog and the conventional cloud-only systems. The analysis has taken into account four primary metrics, which are: the response time, bandwidth usage, the load control in fog-nodes, and the system recovery under the condition of the network segmentation. The experiments were conducted under a simulated institutional environment where the candidate

devices were 500, which were distributed in five nodes of the fog environment as described in Section 7.

8.1. Latency Reduction

The measurement of the end-to-end latency was done at the stage of question retrieval and submission of the answer.

- Cloud-only system: 220-260 ms
- TransExa-Fog system clouded with fog: 80-110 ms.

This will give a round-trip delay savings of approximately 40-60%, and much of it is owed to the local processing in the fog layer, decreased propagation overhead, and utilization of pre-buffered encrypted sets of questions. In turn, the interaction approach was nearly real-time even in the conditions of the high-density deployment as depicted in Figure 11. The encryption of communications to AES-256, which guaranteed the secrecy of the content, was provided during the experiments, and the key exchange between the cloud, fog, and edge layers was implemented on the basis of the key exchange mechanisms powered by ECC. All these results lead to the latency benefits of the fog-level processing in the TransExa-Fog architecture.

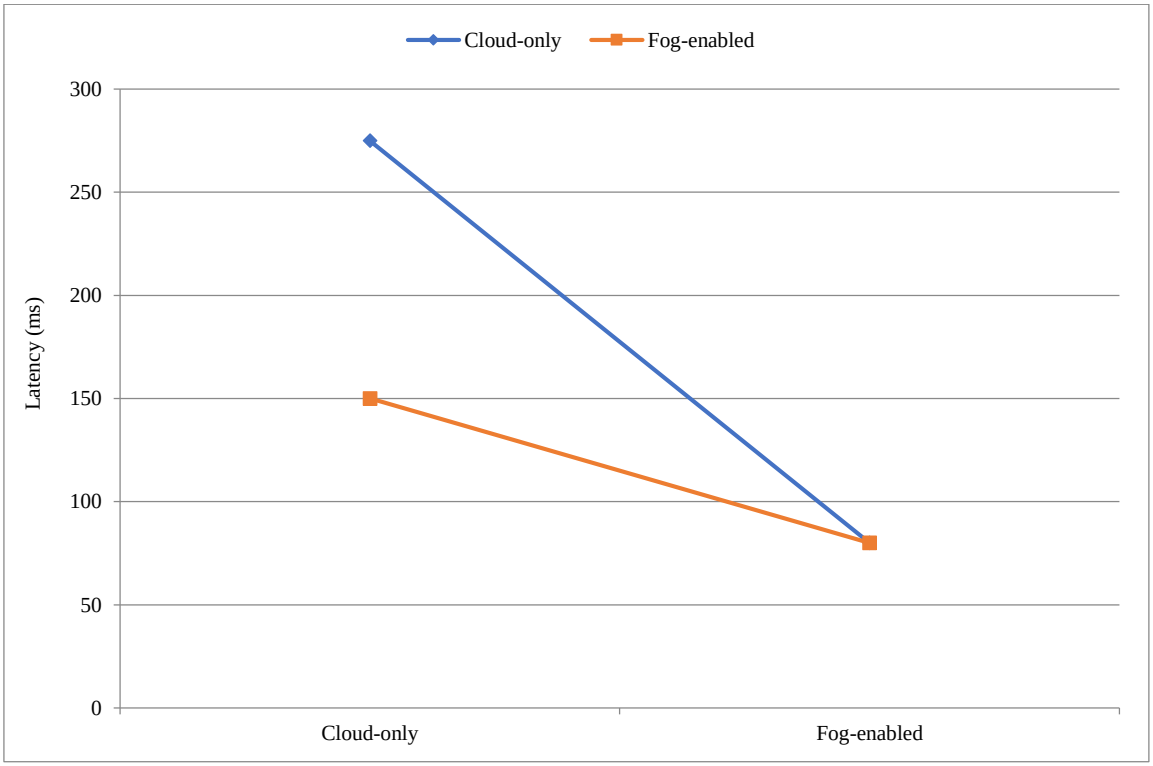

Fig. 11 Latency comparison between cloud-only and fog-enabled TransExa-Fog systems

8.2. Bandwidth Consumption

Bandwidth consumption was measured on 1,000 active devices at a constant test load of examinations:

- Cloud-only system: Intensive upstream traffic, caused by high frequency, device-level synchronization.
- Fog-based system: Bandwidth in upstream bandwidth reduction of close to 45 percent by batched local AES-256-caching of fog nodes and synchronization.

The minimalized amount of communication routes to the cloud also increases the resilience of the entire network structure of the one in question and decreases the problem of load during the peak, which is a feature of the high-density deployment. The results indicate that the bandwidth efficiency of the fog-cloud hybrid solution is particularly applicable to the delivery of massive parallel exams.

8.3. Fog Node Load Handling

Fog nodes were tested regarding the capability to support simultaneous connections of numerous devices:

1. Connection processing: Approximately 800-1,000 devices/fog node spent time in a stable state.
2. Resource usage: There was no usage of the fog nodes that went beyond the set limits (CPU 70% and RAM 65%).
3. Load distribution: the distribution of workloads evenly between the nodes of the system was done to maintain the responsiveness and low latency of the system.

These notes reveal that the TransExa-Fog framework can be scaled and can even accommodate large examination centers whose performance loss is not apparent. The results also confirm the scalability and consistency of the fog layer in terms of resources in heavily crowded examination rooms.

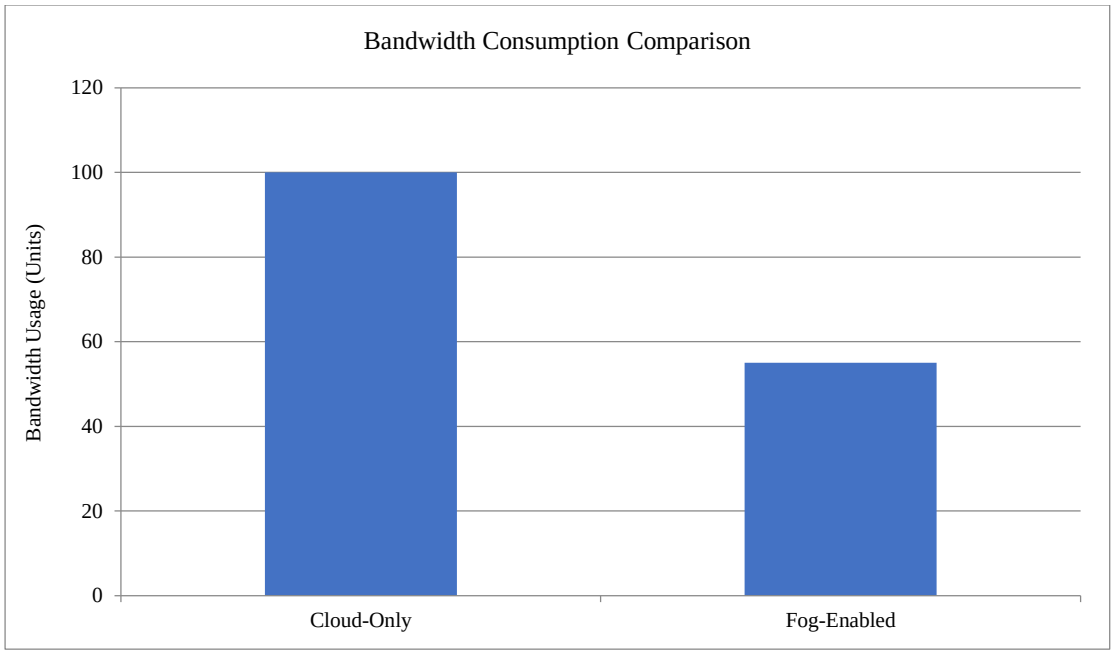

Fig. 12 Bandwidth usage for cloud-only vs fog-enabled systems

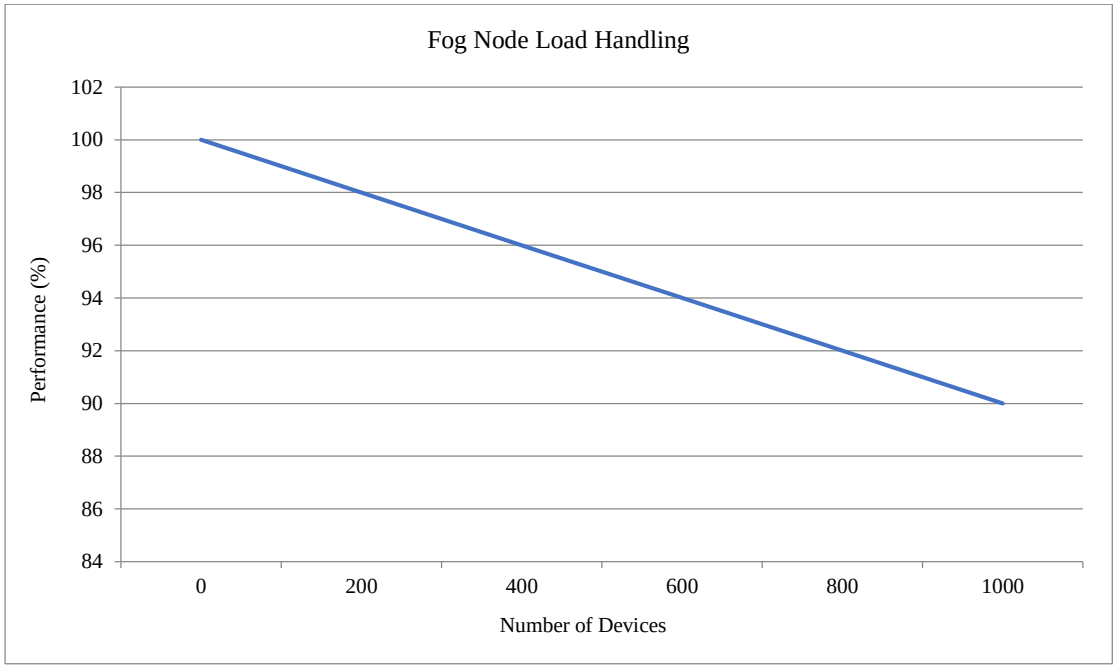

Fig. 13 CPU and RAM utilization of fog nodes under varying device loads

8.4. Recovery Stability During Network Interruptions

The fault tolerance was also tested, which served as a temporary scenario of WAN disconnection:

1. Cloud-only system: There was an increase in risk of answers being lost during network interruptions.
2. TransExa-Fog system: There were no losses of data, which was guaranteed by AES-256-encrypted local buffering, logging integrity checked, and automatic synchronization of batches on re-establishing connectivity.

The results of such are an indication of the ability of the system to provide secure, lossless, and continuous examination operations even when the network is unstable or unsynchronized.

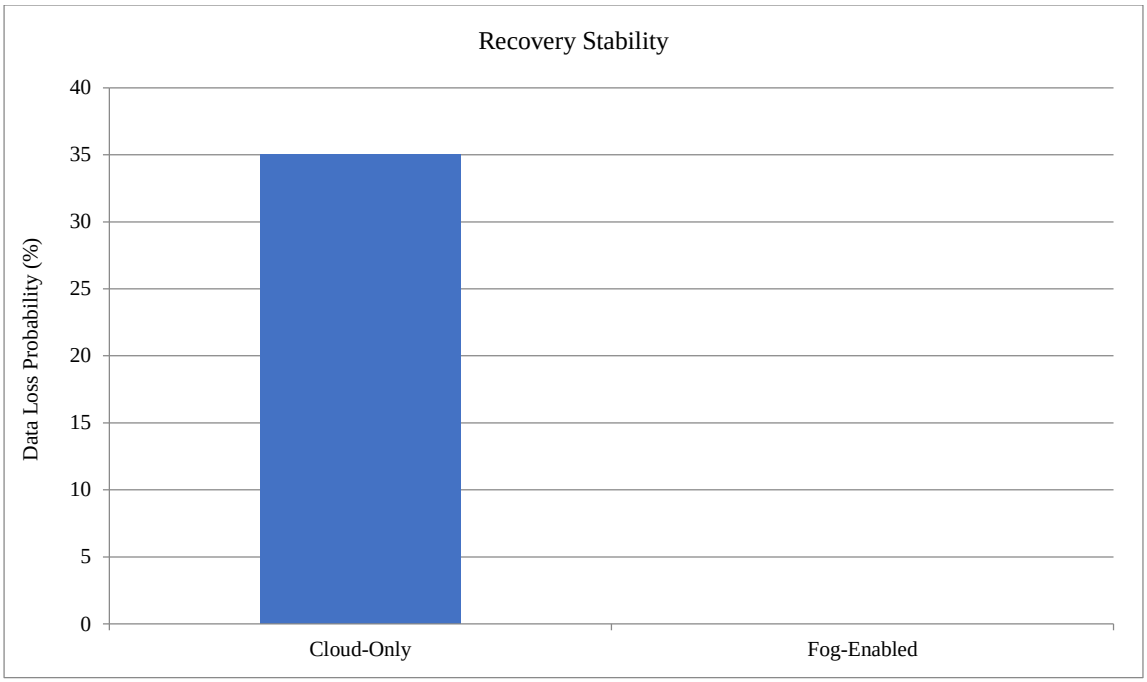

Fig. 14 Response recovery behavior under temporary network outages

8.5. Summary of Experimental Results

The testing experiment demonstrates that TransExa-Fog offers:

1. Reduction of latency in a significant way, relative to more traditional cloud-only architectures.
2. Reduced bandwidth usage by encrypted fog-level caching and batch-based synchronization.
3. Good load control, with the ability to support a high-density deployment of candidates.
4. Unable to disrupt or lose data. Fault-tolerant operation during network interruptions.
5. Extensive security through AES-256 encryption and key exchange based on ECC on all levels.

These findings confirm the usefulness and resilience of the proposed architecture in regard to massively secure and reliable digital examinations as well as its practicality in regard to its implementation in real academic settings.

8.6. Statistical Validation of Experimental Results

In order to make sure that the experimental observations could be reliable and consistent, all the performance evaluations of the proposed TransExa-Fog systems were performed with repeated simulation runs under the same configurations. Each experiment was repeatedly run 30 times independently, and the values mentioned in the results are the averaged values calculated over these repetitions. By doing so, we reduce the effects of transient variations due to network variability and the effects of system scheduling. Under latency assessment, the fog-enabled structure showed a mean end-to-end latency of 94.6 ms with a standard deviation of 8.3 ms , and the cloud-only baseline had a mean latency of 238.1 ms and a standard deviation of 15.7 ms with similar workload conditions. On the basis of these observations, the mean decrease in latency by TransExa-Fog is in the range of 40-60 percent and the ninety five percent confidence limit at 4.2 percent which implies that the results are statistically consistent in terms of the improvement in performance over repeated runs. Besides the average-case analysis, stress testing was conducted at the peak load scenario by adding more and more concurrent candidate devices than the nominal setting. The layer of fog did not have any performance loss and functioned steadily until some predetermined use of resources. These findings testify to the fact that the system does not experience a sudden performance outburst when it is in high-load conditions. The behavior of scalability was also studied by monitoring the performance of the system when the number of connected devices was increased in a proportional manner between the fog nodes. The experimental data show that there is almost a linear scale effect between the limits examined and prove that spreading workloads across a number of fog nodes is an effective approach to avoiding a bottleneck and maintaining low latency even in dense examination conditions. In general, all the features of repeated experiments, statistical measures of dispersion, and confidence limits prove that reported performance improvements of TransExa-Fog are systematic and reproducible, but not a result of single simulation runs.

8.7. Scalability and Stress Testing Analysis

In order to test the scalability limits and robustness of the proposed TransExa-Fog architecture, further stress and scalability tests were performed based on upper simulation

scenarios beyond the base case of 500 candidate devices. These tests were to study the behavior of the systems in extreme workload conditions, saturation limits of the fog-nodes, and long network failures.

8.7.1. Scalability Beyond Nominal Deployment

The number of candidate devices in concurrence was slowly raised to 500, then 1200, in the simulation Moreover, the number of fog nodes was also raised proportionately. The outcome suggests that the system is stable under the conditions where the device-to-fog ratio is not more than 180-220 devices per fog node. In this range, the end-to-end latency marginally grew and exhibited a nearly linear growth pattern, which validated that the workload has been well distributed between the fog nodes. Increases in latency past this point were nonlinear as resources began to compete with each other on a per-fog node basis, reaching a practical expression of the fog layer.

8.7.2. Fog-Node Saturation Threshold

The saturation of fog-nodes was observed based on the CPU usage, memory usage, and the latency of the responses to the gradually increasing loads. The results of the simulation indicate that the fog nodes can be successfully operated in reasonable usage rates (CPU utilization not exceeding 75% and memory not exceeding 70%) until reaching around 900-1000 simultaneous connections of the devices to the node. As soon as these thresholds are surpassed, the queuing delays begin to grow significantly, and this is the sign that degradation of performance begins. The findings can be used to give practical deployment recommendations on the number of fog nodes required in large-scale examination facilities.

8.7.3. Stress Testing Under Prolonged Network Outages

Simulated scenarios that tested system resilience and recovery behavior were those of extended WAN outage scenarios. All candidate responses were buffered at the fog layer during the outages up to 15 minutes without any loss of data using the encrypted local storage. When connectivity was restored again, batch-based synchronization took 12-18 seconds, depending on the amount of buffered data. Inconsistency of the response during the recovery process, as well as integrity violations, was never discovered, indicating that even long-term disconnections do not affect the continuity of the examinations.

8.7.4. Outlier and Extreme Case Observations

The outlier conditions were also tested, such as sudden bursts in simultaneous logins, like the bursts in simultaneously submitted answers around test deadlines. Although these extreme events triggered a spike in latency, the load-balancing and buffering systems implemented by the fog framework prevented system malfunction and guaranteed data capture consistency. These findings prove that TransExa-Fog maintains a graceful performance degradation as opposed to sudden service failure due to extreme operating conditions. In general, the scalability and stress testing outcomes indicate that the proposed architecture can be used to reliably execute high-density examination settings through the adequate scaling of fog-node deployments. The results also confirm that TransExa-Fog stands strong even when subjected to heavy workloads and when networks are taken offline, allowing it to be a viable solution to large-scale and high-stakes digital examination systems.

8.8. User Experience and Usability Observations

Even though the main objective of this research is to determine the performance and security aspects of a system, the user experience within the simulated examination scenarios was qualitatively measured to determine the practicality of the system. The architecture made possible through the use of the fog led to a major decrease in the number of perceivable delays during the loading of questions and submission of answers, leading to a more responsive and smooth examination interface presented to the candidates. The minimization of the latency contributed to the reduction of interruptions and removed redundant delays in synchronizing, which is not uncommon in cloud-only examination systems. On the side of the candidates, the presence of a buffer at the level of the fog allowed continuous study of the exam even in the case of momentary instability in the network, eliminating the stress and negative uncertainty of connection breakdowns. Local response saving in automatic mode also boosted user confidence, as there was no chance of data loss during submission. The proposed architecture was also beneficial to invigilators and examination administrators. Localized supervision Fog level monitoring provided local invigilators an opportunity to detect anomalies or technical problems in their activity in time, and did not use centralized cloud dashboards. This minimized operation overhead and enhanced situational awareness when examining high-density areas. The cited usability attributes, overall, suggest that TransExa-Fog facilitates a stable and low-disruption examination experience on both sides - the candidates and the administrators.

9. Comparative Analysis with State-of-the-Art

The proposed TransExa-Fog architecture and traditional cloud-only examination system are comparatively detailed in Table 3 and compared with the existing fog-based education platforms. The analysis demonstrates the tremendous improvements that are offered by TransExa-Fog in most of the performance factors, like latency, bandwidth efficiency, fault tolerance, security, and scalability. Unlike traditional cloud-based models, which are usually quite volatile and latent, TransExa-Fog will take advantage of the local processing in the fog to enhance the time to respond, in addition to reducing the dependence on the wide-area network links. The architecture also includes robust security measures like the AES-256 encryption, the key management based on ECC, as well as fog-level logging that ensures greater security against data manipulation and unauthorized users. Altogether, this results in the facts that TransExa-Fog performs better

regarding its performance, reliability, and scalability regarding the operations, which is why this is highly applicable to the digital examination of high-stakes and large-scale operations. It is an understatement that the design approach to TransExa-Fog has added a lot to the improved performance of the software, as it has ensured that the software is dedicated to localized processing and reduced the necessity to deploy wide-area networks. The critical operations, such as authentication, buffering, and synchronization, are brought closer to the user at the fog layer, and consequently, the communication delays are minimal, and the congestion of the network is reduced. Furthermore, AES encryption and key management based on ECC are merged in order to provide a good security level and maintain high computational efficiency. There are multiple overall impacts of all such design options that ensure that the latency is minimized, the overall fault tolerance is enhanced, and the overall scalability is better than the fossil-based cloud-only or partial mist fog-enabled solutions. User satisfaction levels across reliability, usability, scalability, and responsiveness are illustrated in Figure 15.

Table 3. Comparative analysis of cloud-based, existing fog-enabled, and proposed transexa-fog examination systems across key performance metrics

Feature	Cloud-Based	Existing Fog-based Education System	TransExa-Fog
Latency	220-260 ms	140-180 ms	80-110 ms
Bandwidth	High Upstream	Moderate	≈45% lower
Offline Support	None	Partial (limited caching)	Full fog caching
Security	Basic cloud encryption	Encryption + MFA	AES-256 + ECC + MFA + Fog level logs
Fault Tolerance	Low	Medium	Zero answer-loss (fog buffering)
Scalability	Good	Good	Very High (distributed fog layer)

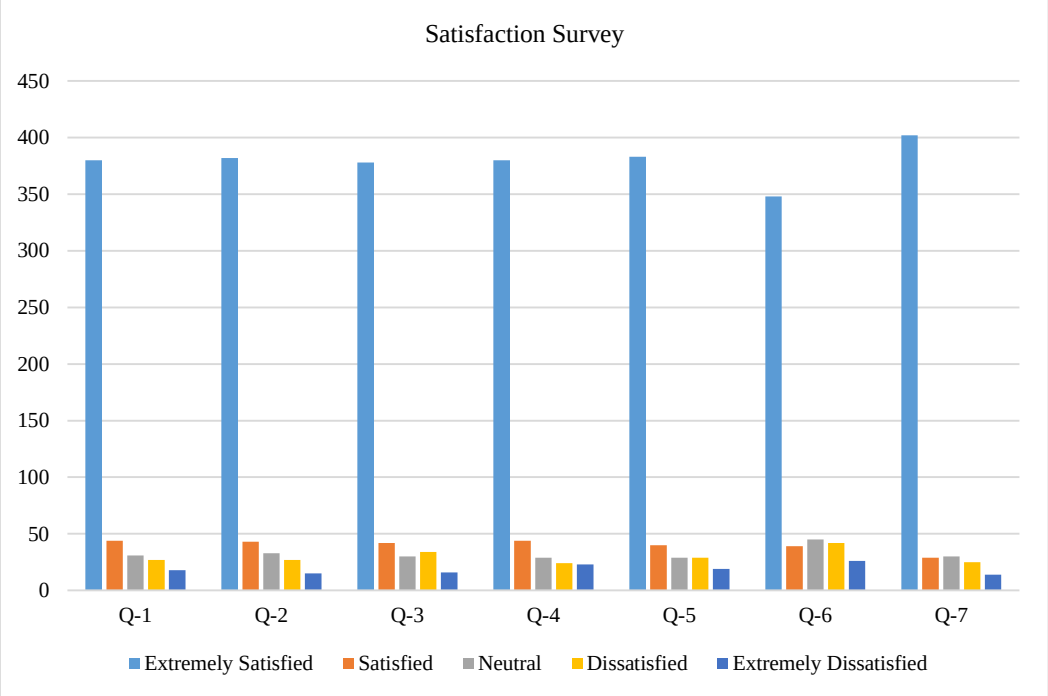

Fig. 15 User satisfaction level across multiple performance categories using the proposed transexa-fog system

10. Future Enhancements

To make the proposed system even better, certain improvements that are even more sophisticated can be explored in the context of further work. Intelligence, deployed with the help of AI, and security systems based on Blockchain can be applied to make the architecture more flexible, reliable, and resilient, which can potentially address the current challenges in the distributed computing environment. The potential future enhancements are the adoption of AI-based anomaly detection, which can identify any suspicious activity, unauthorized access, and deviant behavior in the process of conducting online tests. Lightweight cryptography protocols can be used to attain strong security and be optimized to use resource-constrained edge devices in order to reduce the level

of computation. In addition, blockchain-based audit trails will outperform the tamperproof examination event logging, enhance transparency, and maximize the data integrity of cloud-edge settings.

10.1. Ethical, Privacy, and Regulatory Considerations

The TransExa-Fog design integrates the ethical and privacy-by-design concepts to have responsible use of examination data.

Minimization of data is imposed through gathering of information that is necessary to deliver examinations, authentication, and evaluation to decrease avoidable revelation of personal or behavioral information. The candidate information and examination artifacts are meted out under the principles of data protection, which are commonly considered, such as the General Data Protection Regulation (GDPR), like purpose limitation, storage limitation, and access control.

Only the time necessary by the institutional policies is maintained in sensitive data, after which they are safely stored or destroyed. Biometric data utilized as authentication is afforded special safeguards. The templates of biometrics are encrypted and stored at the fog layer, and the templates are never sent in plaintext to the cloud's servers.

Role-based access control limits access to biometric records, and biometric verification is only done to verify identity in examination rooms. Regulatively, the proposed architecture will facilitate compliance by institutions through secure audit logs, controlled data access, and traceable system operations. These steps can help in maintaining transparency, accountability, and compliance with the requirements of academic governance, while also maintaining ethical considerations and user privacy in the examination lifecycle.

11. Conclusion

To address the gaps of the old cloud-based solution of digital evaluation systems, the paper introduces TransExa-Fog, which is a multi-layer fog-cloud architecture created to solve the weaknesses of the old digital evaluation systems. The framework facilitates safe and low-latency service of examination content through the application of fog-level caching, biometric authentication, ECC-based key exchange, and distributed answer synchronization (use of AES-256 encryption).

It is found through analytical models and controlled experimental analysis that the latency, bandwidth usage, scalability, and fault tolerance have improved significantly. Because the architecture is still capable of operational continuity even when there is a complete failure of the WAN, it is enabled to capture responses to candidates fully and without loss. In summary, TransExa-Fog is a highly scaled and strong platform of the next generation digital examinations that can support the entire institution-level applications and the addition of AI-based proctoring and blockchain-based audit systems in the future.

Conflicts of Interest

The author(s) state their lack of conflict of interest with the publication of this research. This is independent research, and there was no financing or professional or personal connection that influenced the research design, data analysis, findings interpretation, and the conclusion made in the current paper.

References

[1] Koustabh Dolui, and Soumya Kanti Datta, "Comparison of Edge Computing Implementations: Fog Computing, Cloudlet and Mobile Edge Computing," *2017 Global Internet of Things Summit (GIoTS)*, Geneva, Switzerland, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Karrar Hameed Abdulkareem et al., A Review of Fog Computing and Machine Learning: Concepts, Applications, Challenges, and Open Issues," *IEEE Access*, vol. 7, pp. 153123-153140, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] Donagani Ramakrishna, and Mohammed Ali Shaik, "A Comprehensive Analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges," *IEEE Access*, vol. 13, pp. 11576-11593, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xueshi Hou et al., "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3860-3873, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[5] Qiang Duan, "Cloud Service Performance Evaluation: Status, Challenges, and Opportunities-A Survey from the System Modeling Perspective," *Digital Communications and Networks*, vol. 3, no. 2, pp. 101-111, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[6] Weisong Shi et al., "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] Ahmad Alzu'bi et al., "A Review of Privacy and Security of Edge Computing in Smart Healthcare Systems: Issues, Challenges, and Research Directions," *Tsinghua Science and Technology*, vol. 29, no. 4, pp. 1152-1180, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Laha Ale et al., "Delay-Aware and Energy-Efficient Computation Offloading in Mobile-Edge Computing using Deep Reinforcement Learning," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 3, pp. 881-892, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mahadev Satyanarayanan, "The Emergence of Edge Computing," *Computer*, vol. 50, no. 1, pp. 30-39, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] Aditya Nigam et al., "A Systematic Review on AI-based Proctoring Systems: Past, Present and Future," *Education and Information Technologies*, vol. 26, no. 5, pp. 6421-6445, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Kilbert Amorim Maciel et al., "Ubunye: An MEC Orchestration Service based on QoE, QoS, and Service Classification using Machine Learning," *Future Internet*, vol. 17, no. 2, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Tom H. Luan et al., "Fog Computing: Focusing on Mobile Users at the Edge," *Arxiv Preprint*, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[13] Harshit Gupta et al., "IFogsim: A Toolkit for Modeling and Simulation of Resource Management Techniques in the Internet of Things, Edge and Fog Computing Environments," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275-1296, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[14] Tiago M. Fernández-Caramés, and Paula Fraga-Lamas, "Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, Iot, Fog and Edge Computing Enabled Smart Campuses and Universities," *Applied Sciences*, vol. 9, no. 21, pp. 1-24, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Fateneh Golpayegani et al., "Adaptation in Edge Computing: A Review on Design Principles and Research Challenges," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 19, no. 3, pp. 1-43, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Weisong Shi et al., "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[17] Subhadeep Sarkar, and Sudip Misra, "Theoretical Modelling of Fog Computing: A Green Computing Paradigm to Support IoT Applications. *Iet Networks*, vol. 5, no. 2, pp. 23-29, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] Pasika Ranaweera, Anca Delia Jurcut, and Madhusanka Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1078-1124, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mohammad Aazam, and Eui-Nam Huh, "Fog Computing Micro Datacenter-based Dynamic Resource Estimation and Pricing Model," *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, Gwangju, Korea (South), pp. 687-694, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jitendcr Grover, and Rama Murthy Garimella, "Reliable and Fault-Tolerant IoT-Edge Architecture," *2018 IEEE Sensors*, New Delhi, India, pp. 1-4, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[21] Shanhe Yi, Zhengrui Qin, and Qun Li, "Security and Privacy Issues of Fog Computing: A Survey," *Lecture Notes in Computer Science*, pp. 685-695, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[22] Sajid Hussain et al., "Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431-4438, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Ivan Stojmenovic, and Sheng Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," *2014 Federated Conference on Computer Science and Information Systems*, Warsaw, Poland, vol. 2, pp. 1-8, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[24] Soumya Kanti Datta, Christian Bonnet, and Jerome Haerri, "Fog Computing Architecture to Enable Consumer Centric Internet of Things Services," *2015 International Symposium on Consumer Electronics (ISCE)*, Madrid, Spain, pp. 1-2, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[25] Arij Ben Amor, Mohamed Abid, and Aref Meddeb, "Secure Fog-Based E-Learning Scheme," *IEEE Access*, vol. 8, pp. 31920-31933, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] Koustabh Dolui, and Soumya Kanti Datta, "Comparison of Edge Computing Implementations: Fog Computing, Cloudlet, and Mobile Edge Computing," *2017 Global Internet of Things Summit (GIoTS)*, Geneva, Switzerland, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[27] Subhadeep Sarkar, Subarna Chatterjee, and Sudip Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 46-59, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] Flavio Bonomi et al., "Fog Computing and its Role in the Internet of Things," *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13-16, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[29] Amir Vahid Dastjerdi, and Rajkumar Buyya, "Fog Computing: Helping the Internet of Things Realize its Potential," *Computer*, vol. 49, no. 8, pp. 112-116, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[30] Sahil Kadam, Mahesh Kothalkar, and Dayanand Ambawade, "Blockchain-Enabled Examination Platform: A Secure Approach for Academic Assessments," *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kamand, India, pp. 1-7, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Qiang Duan, "Cloud Service Performance Evaluation: Status, Challenges, and Opportunities-A Survey from the System Modeling Perspective," *Digital Communications and Networks*, vol. 3, no. 2, pp. 101-111, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[32] Yuyi Mao et al., "A Survey on Mobile Edge Computing: The Communication Perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322-2358, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[33] Nancy A Angel et al., "Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies," *Sensors*, vol. 22, no. 1, pp. 1-38, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Priyanka Rajan Kumar, and Sonia Goel, "A Secure and Efficient Encryption System based on Adaptive and Machine Learning for Securing Data in Fog Computing," *Scientific Reports*, vol. 15, no. 1, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[35] Jianhua Tang, Wee Peng Tay, and Yonggang Wen, "Dynamic Request Redirection and Elastic Service Scaling in Cloud-Centric Media Networks," *IEEE Transactions on Multimedia*, vol. 16, no. 5, pp. 1434-1445, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[36] Romano Fantacci, and Benedetta Picano, "Performance Analysis of a Delay-Constrained Data Offloading Scheme in an Integrated Cloud-Fog-Edge Computing System," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12004-12014, 2020. [CrossRef] [Google Scholar] [Publisher Link]