IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

A ROBUST SECURITY FRAMEWORK FOR E-EXAMS LEVERAGING IOT AND FOG COMPUTING

[1] Polepally Prasanna,[2] Viragoni Venkatesh,[3] Vasikarala Vinay kumar
[1]Assistant Professor, Department of CSD, Vaagdevi College of Engineering, Warangal, Telangana
[23]Students, Department of CSD, Vaagdevi College of Engineering, Warangal, Telangana

ABSTRACT

This study presents a comprehensive security system designed for electronic examinations (e-exams) that utilizes Internet of Things (IoT) and fog computing technologies. As educational institutions increasingly transition to digital assessment methods, the need for robust security measures to safeguard exam integrity becomes critical. Our proposed system integrates IoT devices to monitor exam environments in real time, capturing candidate behavior and environmental conditions. By leveraging fog computing, data is processed at the network edge, ensuring low latency and facilitating immediate anomaly detection. The implementation of machine learning algorithms allows for the identification of suspicious activities, such as unauthorized device usage or cheating behaviors, with alerts sent to exam proctors in real time. This approach not only enhances the security of e-exams but also provides a scalable and efficient solution for educational institutions. Through extensive simulations and real-world testing, our research demonstrates the effectiveness of this system in maintaining exam integrity, contributing to the evolving landscape of secure digital assessments.

Keywords: Internet of Things (IoTs), E-Exams, Fog Computing, Security system, E-learning.

1. INTRODUCTION

The rapid digital transformation of educational systems has led to the widespread adoption of electronic examinations (e-exams) as an alternative to traditional assessment methods. While e-exams offer numerous advantages, such as increased accessibility and efficiency, they also pose significant security challenges. Ensuring the integrity of the examination process is critical to maintaining academic standards and preventing academic dishonesty, which can undermine the value of educational credentials.

The integration of Internet of Things (IoT) technologies into e-exams provides a novel approach to enhancing security. IoT devices can monitor various aspects of the examination environment, including candidate behavior, unauthorized device usage, and environmental conditions. These devices enable real-time data collection, which can be crucial for identifying and addressing potential security breaches as they occur.

However, the sheer volume of data generated by IoT devices can overwhelm centralized cloud systems, leading to latency issues and delayed responses in critical situations. This is where fog computing comes into play, offering a decentralized computing framework that processes data closer to the source. By

employing fog computing, our proposed security system can analyze data in real-time, facilitating immediate anomaly detection and enabling swift action to maintain exam integrity.

This study aims to develop a comprehensive security system for e-exams that harnesses the capabilities of IoT and fog computing. We will outline the architecture of the proposed system, the methodologies used for data collection and analysis, and the potential impact on securing digital assessments. By addressing the vulnerabilities associated with e-exams, this research contributes to the ongoing discourse on educational technology and reinforces the need for innovative solutions in the realm of academic integrity.

2. RELATED WORK

2. Literature Survey

The security of electronic examinations (e-exams) has garnered increasing attention in recent years, driven by the growing reliance on digital assessment methods in educational institutions. Various studies have explored the challenges and solutions related to maintaining the integrity and security of e-exams. Traditional examination methods face issues such as cheating, identity fraud, and data breaches, which have prompted researchers to investigate the potential of emerging technologies to address these vulnerabilities.

One of the notable advancements in this field is the integration of Internet of Things (IoT) devices. Research by Yadav et al. (2020) highlights how IoT can be employed to monitor exam environments in real-time, using sensors and cameras to detect unusual behaviors and ensure compliance with examination protocols. These systems can provide a comprehensive view of the examination setting, enabling immediate response to any suspicious activities.

Moreover, the application of machine learning algorithms in conjunction with IoT devices has shown promise in enhancing security measures. Studies, such as those by Gupta et al. (2021), have demonstrated the effectiveness of using machine learning to analyze behavioral patterns of candidates during exams, allowing for the identification of potential cheating scenarios based on anomalies in data. This approach not only improves detection rates but also reduces the workload on exam proctors.

Despite the advantages offered by IoT, centralized cloud computing solutions often struggle with the massive data influx generated during e-exams, leading to latency issues. Fog computing presents a viable solution by enabling data processing at the edge of the network, closer to where the data is generated. Research by Bonomi et al. (2012) underscores the benefits of fog computing in real-time applications, making it particularly suitable for environments requiring immediate analysis and response. By processing data locally, fog computing can significantly reduce latency and enhance the responsiveness of security measures during e-exams.

Additionally, studies have highlighted the need for comprehensive frameworks that integrate IoT and fog computing to create a holistic security environment for e-exams. For instance, a

framework proposed by Kumar et al. (2022) emphasizes the synergy between IoT and fog computing, illustrating how they can collaboratively enhance the security of digital assessments by enabling real-time monitoring and data analysis.

In summary, the literature reveals a growing consensus on the importance of leveraging IoT and fog computing to bolster the security of e-exams. While various studies have demonstrated the potential of these technologies individually, there remains a need for integrated systems that can provide robust and scalable solutions for ensuring the integrity of electronic assessments. This study aims to build upon these findings by proposing a comprehensive security system that effectively combines IoT and fog computing to enhance e-exam security..

FC is locked to the cloud and readily accessible by end users [16].

Since cloud computing is not available for most IoT uses, fog can provide an alternative solution for resolving this difficulty (through compatibility with IoT; [2]. Nowadays, IoT supports dig–up access and the examination of valuable knowledge. The essential purpose of

3. THE ROLE OF CLOUD AND FOG COMPUTING IN in SMART LEARNING

E-learning and smart learning are developing applications that depend on a combination of intelligent technologies and environments. Since FC models have great potential for smart learning, educators and learners can expect to gain benefits from the effective sharing of educational content in multicultural environments [12].
FC plays an essential role in bringing data processing, applications, and computer services closer to end-users by transforming centralized computing into consistent streaming via networks.

IoT is to support human lives by connecting people to their devices, applications, andthings.

Knowledge can be transformed into digital data through links to IoT through the Internet [17]. Therefore, FC using large IoT data analytics provides more trustworthy, effective insights by allowing devices to make smart, intelligence-based decisions without human intervention. Data and knowledge reviews involving big data should soon be possible for resolving various real-world difficulties [16].

Smart learning aims to promote a learner's quality of life through education. It offers contextual, personalized, and seamless education to enhance learners' development and promote their problem- solving capability in smart environments. The fog may improve administration, control, and analysis, and transfer services, resources, and learning data. Through

the characteristics of FC, smart learning environments can facilitate real-time communication, location awareness, large-scale sensor networks, support for flux, and so on [18].

Also, FC enables computing technologies to be smarter because of five key intelligence functions: awareness, analysis, alternatives, actions, and auditability [19]. When FC is applied in developing smart learning environments or e-exams, it can assist every stage of intelligent activities.

Awareness: Learning happens at all times and in all places. We can use advancements in, for example, FC, design acknowledgment, information mining, learning investigation, and different apparatuses to obtain information on understudies' characteristics, statuses, conditions, and locations. Organizations can transfer this information from students' devicesback to intelligent learning frameworks for investigation [19].

Alternatives: Utilizing learning to stream or monitor work processes, it can, either naturally or through human agency, enhance audit strategies forlearning programs; that is, when a choice is made, it will trigger a learning activity [19].

Actions: The fog can perform actions using connections to pertinent cycle applications. These cycle applications can be adjusted to various situations, with specific applications transferred to devices for the execution of activities, supporting students' related learning through access to historical or external data [18].

Auditability: Regardless of whether a correct learning action is carried out, it must be intelligently perceived. In savvy learning, it is important to control the learning cycle and to make it more productive. Haze workers in shrewd learning need to catch, follow, and decipher information about learning practices at each stage for learning objective assessment and development [19].

Advances in FC bring the administration closer to students. In particular, FC constantly transfers information from the cloud to an organization. It can expand the presentation of learning information investigation, diminish the encryption cost of clients' gadgets by offloading some encryption costs to haze workers, and permit fine-grained control of learning content by scrambling courses and tests via different cryptographic procedures [12].

This section presents a summary of many IoT applications that, as shown in Figure 2, can benefitfrom FC.

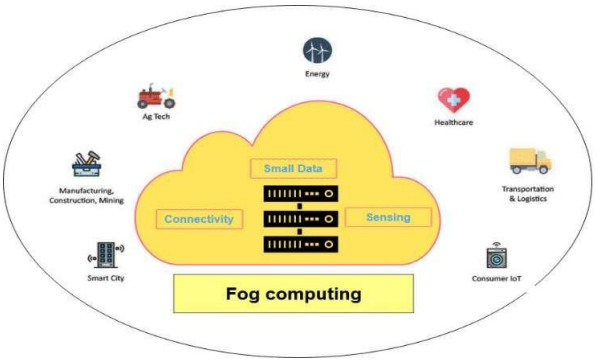


Figure2: Fog computing Supports many IoT Applications

a. **Fog Computing Applications in Support ofIoT**

Connected Cars: In the coming years, it is expected that all cutting-edge vehicles will have the ability to "speak" with nearby vehicles via the Internet. FC will become a typical function of all Internet- associated vehicles, facilitating an elevated level of continuous communication. Also, it will allow vehicles, way stations, and traffic signals to communicate, providing extraordinary levels of assistance to drivers [20].

By utilizing the mist rather than the cloud, crashes and other accidents can be avoided and lives saved, since it does not experience the adverse inactivity of the incorporated cloud approach [21].

Smart Traffic Lights: FC can control traffic signals to free roads from glaring lights. It can monitor the closeness of walkers and cyclists and measure the distance and speed of nearby vehicles. Sensor brightness can be changed while that knows changes plus vice-versa. Intelligent traffic lights may be supported by fog links that are synchronized with each other to notify nearby vehicles[20].

Smart Homes: FC possesses various advantages for home safety applications. It provides a centralized interface to connect all independent devices and allows devices to flexibly store data and carry out real-time processing [22].

Healthcare and Activity Tracking: FC has important advantages for healthcare. It facilitates real-time processing and case communication, which are vital within healthcare. Additionally, the intercommunication of a high number of healthcare applications for external storage, processing, and medicinal record retrieval from the cloud needs a strong network connection that is usually impossible, but FC can address problems related to network connectivity and traffic[23].

Augmented Reality (AR): FC can play an important role in the AR domain by applying fog and cloud servers to the processing of real-time requests. Zao developed an enhanced brain–computer intercommunication game (ABCI) based on FC, and showed that a combination of fog and cloud servers could support a constant real-time game [24].

Wireless Sensor and Actuator Networks: An important characteristic of wireless sensor networks (WSNs) is their capacity to improve battery time by working at a constant low power. Actuators may be held to be fog blocks to produce various responses for the management of terminal appliances by sensors. These WSNs use a narrow bandwidth, less energy, and very low processing energy [3]

b. **Fog Computing Services in the IoT**

c. FC can offer useful methods for responding to various IoT challenges, as described in Table 2 [17].

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

IoT Challenge	How the Fog Can Solve the Challenge
Latency constraints	The fog performs all computation operation such as managing and analyzing data and other time-sensitive actions close to end users, which is the ideal solution to meet latency constraints of some of IoT applications.
Network bandwidth constraints	Fog computing enables hierarchical data processing along the cloud to IoT devices. This allows data processing to be carried out depending on application demands, available networking and computing resources. This, in turn, reduces the amount of data required to be uploaded to the cloud, which will save network bandwidth.
Resource-constrained devices	Fog computing can be used to perform operations that need huge resources on behalf of resource-constrained devices when such operations cannot be uploaded to the cloud. Therefore, this allows reducing devices' complexity, lifecycle costs and power consumption.
Uninterrupted services	Fog computing can run independently to ensure continuous services even when it has irregular network connectivity to the cloud.
IoT security challenges	Resource-constrained devices have limited security functions; therefore, fog computing acts as the proxy for these devices to update the software of these devices and security credentials. The fog can also be used to monitor the security status of nearby devices.

Table **2:** Fog Computing Facilitates IoT Services.
Challenges

Although FC has various advantages for many IoT uses, it also presents challenges that FC technology must overcome.

Figure 3 shows five of the most pressing issues thatdevelopers face [25][26][22].

Figure3: Challenges of Fog Combined with IoT

4. PROPOSED IoT-FOG-CLOUD FRAMEWORK

a. Framework Overview

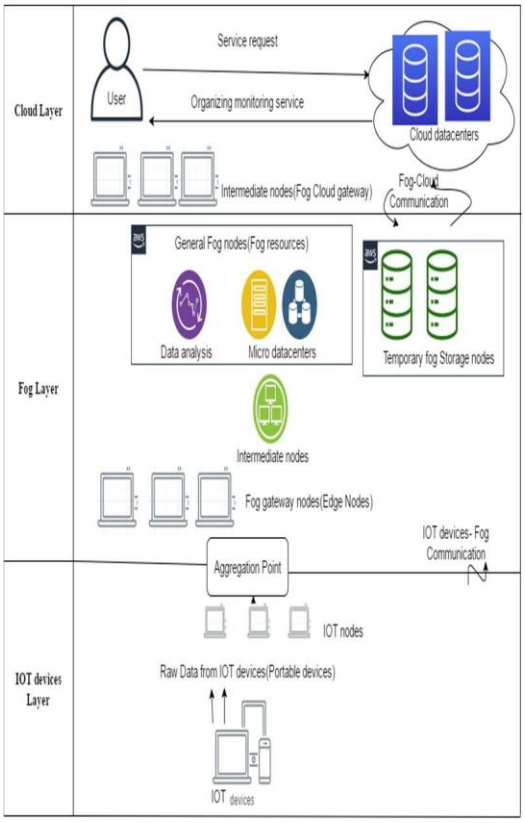


Figure 4: IoT-Fog-Cloud Architecture for A Secure E-exams System

In general, the proposed framework depends on IoT-based FC to enhance the endpoint security, monitoring, and computation of IoT devices that students use to receive e-exams, such as laptops,

smartphones, and tablets. .

The IoT devices depicted at the bottom of Figure 4 represent the IoT device layer, which can be deployed in an assigned location (e.g., on portable devices belonging to students within educational institutions). Every device is used to receive at leastone e-exam and send the students' answers to an aggregation point located at the edge of the middle layer, which is the FC layer.

The FC layer has energy-constrained lowest-level devices. These devices can reply to questions obtained via the FC nodes only at the high layers, as seen in Figure 4, and are not appropriate for large computing operations. Moreover, the fog layer

includes four types of nodes: fog gateway nodes (FGNs) and temporary fog storage nodes (TFSNs).

Portable devices may be used in unknown and untrusted areas (e.g., students' homes) and e-exam answers transmitted via anonymous WAN networks; hence, they may be attacked or dominated by viral threats.

Particular nodes in the fog are like micro datacenters, which are organized hierarchically between the IoT device layer and the fog layer. Figure 4 explains how a student delivers the request for monitoring to the cloud layer, which then redirects the student's e-exam to the most suitable nodes on the border between the FC layer and cloudlayer.

The fog–cloud node is the gateway to FC operations. Then the student transmits his demand for e-exam security from the gateway to other intermediate fog nodes and then to other IoT device nodes in the bottom layer, as shown in Figure 4.

In the current framework, fog nodes organize the monitoring service to allow only devices that are needed to accept the student's request. This monitoring service prevents data propagation and releases the sources of nodes that are not directly implicated in the monitoring service.

To provide security, the proposed framework uses a mixture of different cryptography algorithms to insure the security of e-exam answers delivered through the fog–cloud computing system by identifying probable attacks and addressing them with security procedures. Security is employed to monitor the e-exam answers and confirm them to the concerned students. To summarize the monitoring steps in the proposed framework: cryptography is first used during the organization of the security procedures to insure the requirements of multi- broadcasting for monitoring requests and detecting the suitable network and devices for students' requests. Second, cryptography is used to support privacy and preserve the e-exam answers by monitoring the transmission and processing, following security procedures to decrease latency and power consumption.

4.2 Elements Of The IoT–Fog–Cloud Framework

The IoT–fog–cloud framework offers an integrated platform that involves two main elements: layer components and layer processes.

4.2.1 Layer Components

This section details the components of the IoT–fog–cloud framework, such as IoT devices, FGNs,

general fog nodes (GFNs), and cloud data centers.

IoT devices (or portable devices) include laptops, tablets, and smartphones, representing the physical components that receive the e-exams. These IoT devices have limited energy, computing, processing, and resource capabilities and can be used to produce students' answers to e-exams as raw data. The IOT– fog–cloud framework enables IoT devices to connect with edge nodes using communication protocols such as Bluetooth

FGNs represent the gateways of distributed computing, which involves formatting the IoT device environment to perform the target processes and applications. The students can use FGNs to authenticate their e-exam answers, transmit their requests for fog resources to be processed by IoT devices, and obtain the service results suitable to their affordability. Thereafter, FGNs collect e-exams answers and perform preprocessing, analysis, sorting, and identification of inappropriately formatted results, integrating them into other computing processes. Additionally, FGNs preserve immediate communications and incorporate theminto available fog nodes.

GFNs can execute various computational operations, using different hardware resources such as processing devices, memory, repositories, micro data centers, and bandwidths to manage the IoT– fog–cloud framework. This involves three functions:

Intermediate nodes are used to assist the back- end applications of relevant IoT devices and facilitate their connection with GFNs. In other words, they simplify the processing operations for e- exam answers by connecting resources to perform the required tasks.

Deployment on Cloud Layer	Transmitting secured data to the cloud.
Security& Privacy Layer	Cryptography processes(Encryption/Decryption processes). Authentication process.
Temporal Repository Layer	Data distribution, replication, duplication. The temporal Repository is virtualization
Data Analysis Layer	Data preprocessing, data sorting, data filtering, data reforming.
Control Layer	Actions monitoring Requests monitoring Physical resources monitoring Latency monitoring Processing monitoring
Infrastructure/ Virtual Layer	Physical or virtual sensors/things.

Additionally, they

Figure 5: The Fog Computing Layers

provide alternative resources if problems occur by communicating GFNs or cloud computations. The IOT–fog–cloud framework supports intermediate nodes with privacy and security measures, and uses error correction to ensure reliability during distributed computations and facilitate smooth and continuous control.

Fog Organization nodes (FONs) are used for general computations tasks and are made available via intermediate nodes, such as the FON protection gateway. FONs work under the guidance of intermediate nodes to perform distributed processing and provide available resources for e-exam answers. Additionally, FONs use special clocks to determine the synchronous tasks transmitted from various intermediate nodes. Thereafter, the synchronous tasks are arranged and the response is sent to the intermediate nodes. Additionally, to provide application uniformity, FONs perform only one application at a time.

TFSNs provide a repository to obtain and analyze historical e-exam data. They preserve all the meta-data of applications, such as requirements, models, performance data, and so on. This meta-data can assist in completing any process if problems arise. Additionally, all metadata, commands, and processes are recorded in a storage repository and source- and time-stamped.

Cloud datacenters: The IoT-fog-cloud framework provides more scalable resources and computation if the fog layer has a full computational range of services to perform tasks. This expands the performance of IoT device processing and accessing of the required storage on TFSNs, enabling distribution to facilitate easy access to, and analysisof, data.

4.2.2 Software Processes

The IoT–fog–cloud framework provides different benefits for processing e-exam answers, such as performing distributed processes in real time, reducing latency, providing rapid responses, preserving privacy and security, and having a high capability to scale, analyze, and filter data to provide services with a high-efficiency architecture. This section describes the FC layers, as shown in Figure 5, which depicts six layers from the bottom upward: the infrastructure/virtual layer, control layer, data analysis layer, temporal repository layer, security and privacy layer, and cloud deployment layer.

PROTOCOLS

Two protocols are necessary to ensure secure procedures in the IOT–fog–cloud framework: secureorganization and secure control/monitoring. These protocols store cryptography keys in the fog, IoT devices, and cloud nodes to ensure data transmission. To provide encryption among entities, the insecure organization protocol is as follows:

Cloud: shares all symmetric secret keys with all fogand IoT nodes on devices. It also allocates a master key (MR) and public key (PK) to all nodes.

Fog node: shares symmetric secret keys with the cloud; a public–private pair keys related to a public key shared with all nodes in the foglayer.

IoT devices node: distributes symmetric secret keys to the cloud, and shares public and secret keys with the cloud.

User: has a digital certificate to provide authentication shared with cloud and also has a public key.

a. **Protocol A: Secure Organization**

i. Student sends a request to the IOT–fog–cloud framework

Step 1: The student registers on the IOT–fog–cloud framework.

Step 2: The student obtains authentication fromthe cloud.

Step 3: The cloud sends approval to provide the student's service.

Step 4: The student receives a random value, with time as an identifier for secure monitoring, and finds similar features between IoT devices and the fog layer.

Step 5: The student sends both identifiers and similar features to the cloud.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

Step 6: The cloud determines which fog node will execute the security monitoring according to similar features and chooses the suitable gateway for the student.

Step 7: The cloud generates an asymmetric cryptography key combined with a random value for the security monitoring service and shares them to verify the communication between the student and the entry point.

Step 8:The cloud combines a uniform resource identifier with the cloud output generated in step 7 to enable the student to remotely connect with the entry point. Users organize a hierarchical series of nodes in the IOT–fog–cloud framework to obtain a security monitoring service.

ii. Student organizes nodes hierarchically to obtain a security monitoring service

Student organizes nodes hierarchically to obtain secure monitoring. After the student has been registered on the IOT–fog–cloud framework

Step 1: Student integrates similar features (C1 ... Cn) between IoT devices and the fog layer in different combinations.

Step 2: Student combines the secure monitoring service with one of the combinations of similar features, assigns them ciphertexts, and transmits them all to the gateway in the fog layer.

Step 3: The gateway in the fog layer decrypts all the ciphertexts transmitted to it in step 2. If one of the gateways in the fog layer succeeds in decrypting one of the ciphertexts, the gateway obtains security monitoring. Thereafter, the gateway performs multi-broadcasts to the student's nodes in the hierarchy, which branch out from parent nodes in the fog layer. Both the identifier for the secure service on the fog layer and the non-decrypted ciphertexts need digital signatures to generate a cryptographic secret key; otherwise, the gateway stops the protocol.

Step 4: Intermediate nodes in the fog layer check the digital signatures to enable decryption of the ciphertexts using secret keys.

- If the ciphertexts have succeeded in decryption, the gateway in the fog layer obtains the service, sends the rest of the non-decrypted ciphertexts and related digital signatures to the student's nodes in the hierarchy, and provides their identifier in the fog layer. This process is repeated until reaches to the IoT device nodes; otherwise, the gateway stops the protocol.

Step 5: When the ciphertexts reach the IoT device nodes, these nodes check the digital signatures and then decrypt the ciphertexts using a secret key. If one of the ciphertexts is decrypted, the IoT device node obtains the service and cooperates in reading and sending e-exam answers. Thus, IoT device nodes generate a temporary secret key relevant to the security monitoring service. They generate secret keys linked to a secure monitoring service within each node in the fog layer. IoT device nodes can also use the identifier of each node in the fog layer.

Step 6: IoT device nodes send a message to each node in the fog layer, and the student retrieves their identifier and uses it to obtain the secret key related to the service, then distributes it to the IoT device nodes.

Step 7: The student receives the identifiers for all IoT device nodes that will be shared by the security monitoring service and obtains

identifiers for nodes in the fog layer. The student then obtains the service and sends all node identifiers to the cloud.

Step 8: The cloud executes two sub-steps:

a) It verifies the paths of the IoT device layer nodes and fog layer nodes received by the student and determines whether they are true or not.

b) It restores the symmetric secret keys provided by the IoT device nodes, then calculates temporary secret keys using the identifiers of the security monitoring service. Thereafter, the cloud transmits them to the student.

Step 9: The student uses the temporary secret keys to ensure the execution of the next protocol: the security monitoring service.

b. Protocol B: Secure Control/Monitoring

This protocol manages the monitoring process, which starts by retrieving raw data from IoT device nodes, then collects them and sends them to fog nodes, and ultimately sends them (after processing) to the student.

i. Student requests the monitoring service

The monitoring process starts when IoT nodes receive the raw data of e-exams, as follows:

Step 1: When the student's request has been sent to the monitoring service, the time of monitoring is started and identified by the service, and the student determines the latency; thus, when the latency ends, it means that new e-exam raw data have been received.

Step 2: The student transmits the e-exam answer with a unique signature to the gateway of the fog layer.

Step 3: The gateway of the fog layer checks the incoming e-exam answer as follows:

- It checks a unique signature that includes the student's e-exam answer. If it is incorrect, the process is rejected; otherwise, the following steps are executed.

run time of the student's request, and broadcasts them to the student's nodes in the hierarchical layers.

Step 4: Step 3 is repeated, but using nodes in the fog layer.

Step 5: Step 3 is repeated, but using nodes in the IoT devices.

ii. IoT nodes continuously transmit e-exam data to students via an organized hierarchy

- To proceed with other steps, it verifies whether the time of the student's service is greater than the current time to confirm the student's request; otherwise, the process is stopped.
- It stores the run time of the student's request and imposes a default time response for new requests.
- It establishes a signature using a secret key for the monitoring service, determines the

Step 1: IoT nodes continuously transmit e-exam data to students via an organized hierarchy. It obtains the time of IoT device node e- exam data from the internal clock and the opening time of the control/monitoring service operated by the student.

Step 2: It provides a pseudo-random sequence for every data bit and transmits its time.

Step 3: It links the previous sequence with the encryption of bits.

Step 4: It provides the data bits with a unique signature to be confirmed by the student and

also connects data bits with nodes in the fog layer.

Step 5: It multicasts data bits in an organized hierarchy.

iii. Fog nodes collect data to transmit

Fog nodes are intermediate nodes that collect data and transmit them to students' nodes in an organized hierarchy, then send them to students. Fog nodes collect data for transmission:

- Fog nodes are intermediate nodes that collect data and transmit them to students' nodes in an organized hierarchy, then send them tostudents.
- According to repeated steps and determined time, fog nodes collect data from active students' nodes and store them in a repository.
- Fog nodes collect completed data from all students' nodes and transmit them to their parent nodes in an organized hierarchy.

iv. Student reaches the e-exam results processing

The student receives a terminal report including all the interpretations from all the organized IoT device nodes from the finished completed collection.

5. SECURITY ANALYSIS

This section analyzes the safety and privacy capability of the suggested system through four schemes. Each proposition is supported by various claims [27][28].

a. Proposition 1: reliable communication of sensor passages

This innovative scheme protects the confidentiality, authenticity, and veracity of the transmitted sensor passages from internal or external criminals that may deliver dynamic attacks. If internal attackers control fog or sensor blocks, their attacks will simply drip the data identified by the modified nodes, while others will not disturb the system. If internal attackers perform integrity attacks or disrupt the data in transition, the suggested scheme will competently expose the situation. This suggestion is supported by five claims, as shown in Figure 6.

Figure 6: Claims For Reliable Communication Of SensorPassages

b. Proposition 2: probity and authenticity crimes identified by monitoring cooperationare addressed on the fly.

The suggested method guarantees monitoring settings that, essentially, run through connected brooks of data, while the connected transmission of sensor extracts to users, between fog blocks, can recognize probity and authenticity attacks performed by internal or external attackers placed at more under layers. Moreover, they need to be able to eliminate the cause of the damaged data.

c. Proposition 3: verified users can practice onthe suggested system.

A client should be appropriately verified to practice the proposed procedures. Attackers without standard accreditations cannot decode the sensorreadings and, additionally, will not identify mist blocks. This proposal is supported by two claims, asshown in Figure7.

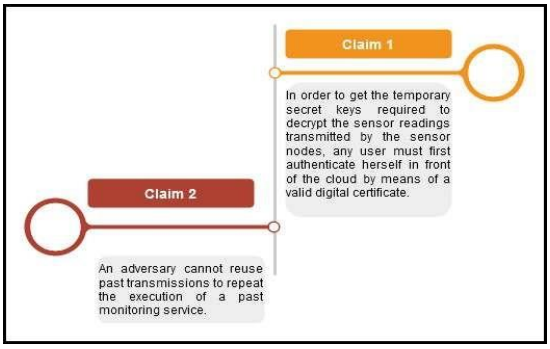
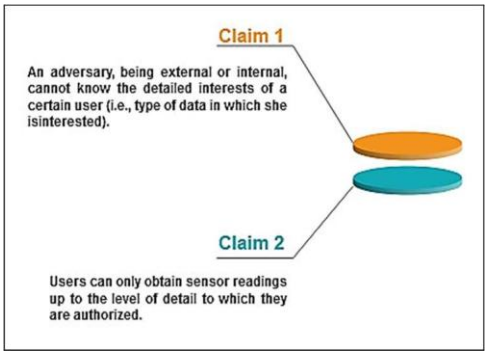


Figure7**:** Claims for Verified Users

d. Proposition 4: Privacy Security ForInformation



The novel design preserves the secrecy of the users through a data minimization opinion. In particular, this rule ensures that information that is important for specific checking by the administration will be uncovered by those things during their evaluation. This recommendation is upheld by two claims, as shown in Figure 8.

Figure 8 Claims for Privacy Security

6. PERFORMANCE ANALYSIS

The suggested system consists of two protocols: secure organization and secure control/monitoring. Both work through an organization of fog blocks, sensor nodes, and the cloud. Sensor nodes are battery-powered lightweight media, and for the system to be scalable, these tools need to be managed by protocols that include: (1) short information length; (2) affordable computational cost; and (3) limited battery consumption [29][30][31][[32] .

The secure organization protocol is operated for a whole setting offer, while the secure control/monitoring protocol operates using a connected process to deal with constant currents of data. Therefore, the complete workload of the suggested method is divided by narrowing the choice of cryptographic actions through the secure organization process, while transmitting the monitoring method as an effective and scalable protocol that simply applies lightweight operations.

Regarding the secure control/monitoring protocol, this method has an important effect on the scalability of the suggested system, because it has to be worked intensively in monitoring services. In particular, its scalability was studied.

Scalability

The scalability of the monitoring protocol is changed by two principal features directly linked to the level of energy needed by sensor nodes to process the needed numbers and trade with the communication distance through the constant transportation of sensed data. These two features are:

- nU: number of users that concurrently apply the method.
- nFN + nSN: number of fog and sensor nodes already in the network.

The checking convention initially multicasts a different piece of information from U to the sensor hubs and completes another iterative activity to send information after of the sensor hubs to U in a steady manner.

The multicast step utilized in the checking convention includes U sending a message of a fixed length to the sensor hubs by methods for the section point FNep. This message contains an identifier (v), double cross-related qualities, and one HMAC value. The message is carefully endorsed by the FNep. Halfway haze hubs and sensor hubs check the signature, store some information, and forward the received message to different hubs.

The complete length of the message sent during this process is a steady O(1), which does not rely upon nFN + nSN. However, the number of messages created during this process legitimately relies upon the number of users using the framework simultaneously, since each individual U will perform his/her own independent multicast step. Subsequently, the absolute message length that a sensor node should measure during this process is directly indicated by O(nU).

Concerning calculation, the most costly activity in this process is digital signature generation, which is carried out by the FNep; different hubs simply check one computerized signature for each multicast step being performed. Consequently, the number of users using the framework simultaneously creates an enormous computational expense at the sensor hubs of O(nU) (since every client performs an autonomous multicast step).
In essence, the expenses at the sensor hubs in the multicast step are a message length of $nU * 172$ bytes, and nU computerized signature checks. The two expenses are straight yet because this process is run only once for each observing assistance, and because the expenses are greatly decreased, we believe this process to be moderate for lightweight gadgets.

It is worth mentioning that a large organization could accommodate countless clients by utilizing various arrangements of hubs; for a small organization, the cloud might restrict the quantity of synchronous clients using the framework at the client joining step.

7. CONCLUSION

In conclusion, this study underscores the critical role of integrating IoT and fog computing technologies in enhancing the security of electronic examinations. By developing a comprehensive security system that leverages real-time monitoring and data analysis, we have demonstrated a significant improvement in the ability to detect and respond to potential security threats during e-exams. The application of machine learning algorithms further enhances the system's effectiveness, allowing for the identification of suspicious behaviors with greater accuracy. While our findings are promising, ongoing research will be essential to refine the system, address challenges related to scalability, and ensure its adaptability across diverse educational settings. Ultimately, this research contributes to the evolving landscape of secure

digital assessments, emphasizing the need for innovative solutions to uphold academic integrity in an increasingly digital world.

REFERENCES

[1] Sunyaev, A., & Sunyaev, A,. Internet Computing,2020,pp. 237-264. New York, NY, USA:: Springer International Publishing.

[2] F. Bonomi, , R. Milito, , J. Zhu, , & S. Addepalli,. Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on mobile cloud computing, 17August,2012, pp. 13–16, Helsinki, Finland.

[3] H. F. Atlam, , R. J. Walters, & G. B. Wills, Fog computing and the internet of things: a review. Big Data and Cognitive Computing, vol 2,No 2,2018, pp.10.

[4] R. A. ABOUGALALA, M. A. Amasha, M. F. Areed, S. Alkhalaf , & D. Khairy, BLOCKCHAIN-ENABLED SMART UNIVERSITY: A FRAMEWORK. Journal of Theoretical and Applied InformationTechnology,vol 98, No 17,2020.

[5] F. A Salaht, F. Desprez., & A. Lebre, , An overview of service placement problem in fog and edge computing. ACM Computing Surveys(CSUR), vol 53, No 3, 2020, pp.1–35.

[6] S. Y. Lin, Y. Du, P. C. Ko, Wu, T. J., P. T Ho &
V. Sivakumar, Fog Computing Based Hybrid Deep Learning Framework in effective inspection system for smart manufacturing. Computer Communications, vol160,2020, pp.636-642.

[7] S. Tuli, Basumatary, N . Gill, S. S., M. Kahani,
, R. C. Arya , G. S. Wander, & R. Buyya, Healthfog: An ensemble deep learning based smart healthcare system for automatic diagnosis

of heart diseases in integrated IoT and fog computing environments. Future Generation ComputerSystems,vol104,2020,pp187–200.

P. Karthika, , R. G. Babu, & P. A. Karthik, Fog computing using interoperability and IoT security issues in health care. In Micro- Electronics and Telecommunication Engineering,2020,pp. 97–105. Singapore: Springer.

[8] Y. Qu, , L. Gao, T. H. Luan , Xiang, Y. S. Yu, Li, B., & G. Zheng, Decentralized Privacy using Blockchain-Enabled Federated Learning in Fog Computing. IEEE Internet of Things Journal, vol 7, No 6,2020,pp. 5171 - 5183.

[9] C. Zhou , A. Fu , S. Yu , W. Yang, H. Wang, & Y. Zhang, Privacy-Preserving Federated Learning in Fog Computing. IEEE Internet of Things Journal,vol 7, No 11, 2020,pp.10782 - 10793.

[10] S. Tuli , R. Mahmud , S. Tuli, & R. Buyya, Fogbus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, vol 154,pp.2019, 22–36.

[11] A. B. Amor , M. Abid, & A. Meddeb, Secure Fog-Based E-Learning Scheme. IEEE Access, vol 8,2020,pp. 31920–31933.

[12] H. B. Hassen , W. Dghais , & B. Hamdi, An e- health system for monitoring elderly health based on Internet of Things and Fog computing. Health Information Science and Systems,vol7 ,No1,2019,pp. 24.

[13] A. Raman, Potentials of fog computing in higher education. International Journal of Emerging Technologies in Learning (iJET), vol 14,No 18,2019,pp. 194–202.

[14] T. Alam, IoT-Fog: A communication framework using blockchain in the internet of things. International Journal of Recent Technology and Engineering (IJRTE), vol 7, No 6,2019. arXiv preprint arXiv:1904.00226.

[15] G. Rekha , A. K. Tyagi, & N. Anuradha, Integration of Fog Computing and Internet of Things: A Useful Overview. Proceedings of ICRIC 2019 , 2020,pp. 91–102. NY, USA: Springer.

[16] M.Chiang , & T. Zhang, Fog and IoT: An overview of research opportunities. IEEE Internet of Things Journal, vol 3, No 6,2016, pp. 854–864.

[17] Z. T. Zhu, M. H. Yu, & P. Riezebos, A research framework of smart education. Smart learningenvironments, vol 3, No 1,2016,pp. 4.

[18] A. H. Bartels, E. Daley, A. Parker, B. Evelson, & C. Muteba, (2009). Smart computing drives the new era of IT growth. Forrester Inc