Journal of Theoretical and Applied Information Technology
31st January 2022. Vol.100. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURITY SYSTEM FOR E-EXAMS USING AN IoT AND FOG COMPUTING ENVIRONMENT

DALIA KHAIRY, MOHAMED A. AMASHA,[a] , RANIA A. ABOUGALALA,[a] SALEM ALKHALAF,[b] MARWA F. AREED [c]

[a] Faculty of Specific Education, Department of Computer Teacher Preparation, Damietta University, Damietta, Egypt.

[b] Department of Computer Science, College of Science and Arts in Alrass, Qassim University, Alrass, Saudi Arabia.

[c] Faculty of Engineering, Department of Electrical Engineering, Damietta University, Damietta, Egypt.

[a]shamaamora2014@gmail.com// [a]mw_amasha@yahoo.com, [a]Ronyabogalala@hotmail.com, [b]s.alkhalaf@qu.edu.sa//[c]Marwa_Areed@du.edu.eg/

ABSTRACT

A recently significant confirmation has adopted to e-learning systems are in great demand. Students, instructors, and examiners share large amounts of data, which should be transmitted securely. One of the most support infrastructures to merging intelligent devices, data analysis, and cybersecurity is the Internet of Things(IoT). Specifically, when combined with Fog and cloud potentials to strengthen the performance of various latency-sensitive and computing-intensive. This paper presents the IoT-Fog-Cloud framework to provide security factors in sharing E-exam which poses several security challenges, such as fine-grained access control and security preservation of E-exam. Further, the proposed framework supports bringing closer the services to the students. Besides, this paper improves the efficiency of E-exam data analysis, reduces the encryption burden in terms of computation cost on user's devices by offloading part of encryption cost to fog servers, and provides fine-grained access control to E-exam content by encrypting with different cryptographic techniques. IoT–fog–cloud framework works in consideration of two main elements: the layer components and the layer processes. Layer components to be integrated include the FGNs, cloud data centers, and GFNs. In layer processes, a series of benefits can be realized, since distribution processes help students to reduce latency and enhance response times and the preservation of privacy and security . Finally, this paper shows that the proposed IoT-Fog-Cloud framework can achieve data confidentiality, fine-grained access control, collusion resistance, and unforgeability to ensure secure procedures to apply the proposed framework.

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

1. INTRODUCTION

Fog computing (FC) is an extremely virtualized platform with a distributed hierarchical structure, which allows increased adaptability and handling data between end users and cloud servers [1]. In other words, it is a widespread form of cloud computing that has great computing potential for storage the sharing of software applications or physical resources, and efficient services for the end users of the IoT and terminal devices. It supports a range of different applications, such as smart cities, smart learning, smart homes, e-healthcare, and grid systems [2]. The architecture of FC depends on three main layers, as depicted in Figure1 a device/end layer, one or more layers of fog nodes, and at least one cloud data center (cloud layer).

Figure 1: Architecture of Fog Computing (Atlam et al. 2018)

Device/End layer: This is the nearest layer to end users. It consists of two types of IoT devices: first, mobile IoT devices that have restricted bandwidth, computing, and storage and are portable (e.g., cameras and mobile phones); second, fixed IoT devices like Radio-Frequency Identification(RFID). These IoT devices are capable of gathering raw data and transferring it to the fog layer [3].

***Fog layer*:** This is efficient for processing data, storing performed inquiries, and regularly transferring data reports to the cloud. The middle layer comprises fog nodes and devices, such as access points with expanded computational capacity, bridges, routers, laptops, specific fog servers, and similar. These devices are attached to the cloud server and can transfer inquiries to cloud centers. They can be used everywhere with communication links: via a cellphone, in a vehicle, or at the roadside [4].

***Cloud layer*:** This is composed of numerous data servers and centers capable of delivering complicated summaries and saving large amounts of data. The cloud has significant space for data storage and is accessible to people anytime and anyplace. It employs virtualization technology to ensure the privacy of IoT discrete data and applications, such that these applications can autonomously handle the requirements of many people. The cloud supports reports from multiple fog nodes and performs a universal investigation of the data offered by FC nodes to enhance IoT applications such as smart energy distribution, health state monitoring, and network optimization [5].

Fog computing can handle IOT limitation such as latency constraints, network bandwidth constraints, and resource constrained devices. Through IoT–fog–cloud framework, we can determine some limitation. First, fog nodes enable to aggregate transmitting E-exams data to reduce communication overhead on behalf of intermediates without learning any information for large-scale IoT applications. However, both the cloud and fog nodes cannot be fully trusted, whether the returned result is correct or not becomes a huge concern for the user, as the user cannot compute the result by himself because of the low computational capability of his devices. Second, the computing resources, fog nodes can assist the IoT devices to perform complex computational operations that they cannot executed by themselves. However, this method inevitably exposes all sensitive information to fog nodes, which may have been compromised by attackers. Third, secure E-exams analysis using data mining and machine learning algorithms pose a great challenge on individual privacy in big data era. Although de-identification is widely used to prevent attackers from linking the processing data with individual's identity, the anonymous data is still easily hacked in terms of privacy.

This paper is organized as follows: Section 2 discusses FC–related work. The proposed IoT–fog–cloud framework and supporting protocols are briefly described in Sections 3 and 4, respectively. The security and performance of the proposed framework are analyzed and discussed in Sections 5 and 6. Finally, Section 7 summarizes the research paper.

2. RELATED WORK

The emerging IoT has presented several complex challenges, but the new FC technology can overcome many of these challenges, as seen in Table 1 (APPENDIX I) which outlines some related work. Through the previous highlight literature, the current IoT-Fog-Cloud framework provides security factors in sharing E-exam which poses several safety challenges, such as fine-grained access control and security preservation of E-exam. Further, the proposed framework supports bringing closer the services to the students. Besides, this paper improves the efficiency of E-exam data analysis, reduces the encryption burden in terms of computation cost on user's devices by offloading part of encryption cost to fog servers, and provides fine-grained access control to E-exam content by encrypting with different cryptographic techniques. Moreover, the proposed IoT-Fog-Cloud framework can achieve data confidentiality, fine-grained access control, collusion resistance, and unforgeability to ensure secure procedures to apply the proposed framework.

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.

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

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' devices back 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 for learning 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 benefit from FC.

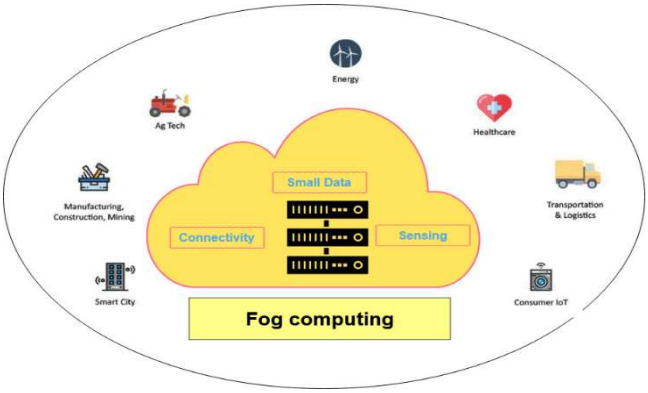

Figure2: Fog computing Supports many IoT Applications

a. *Fog Computing Applications in Support of IoT*

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].

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

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.

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].

d. *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 that developers face [25][26][22].

Journal of Theoretical and Applied Information Technology
31st January 2022. Vol.100. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure3: Challenges of Fog Combined with IoT

4. PROPOSED IoT-FOG-CLOUD FRAMEWORK

a. Framework Overview

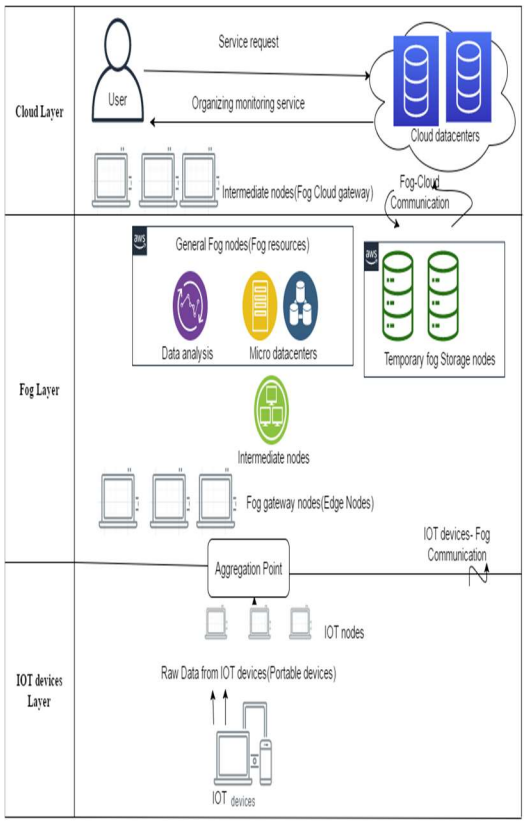

Figure 4: IoT-Fog-Cloud Architecture for A Secure E-exams System

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 least one 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 cloud layer.

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 them into 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. Additionally, they

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.

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 analysis of, 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: secure organization 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 fog and 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 fog layer.

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.

b. 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 from the 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.
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.

c. 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.
- 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

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

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 to students.
- 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.

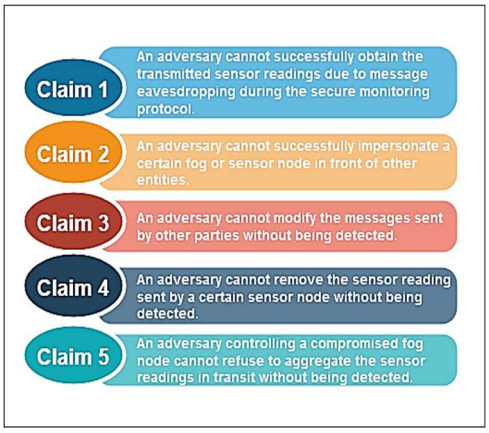

Figure 6: Claims For Reliable Communication Of Sensor Passages

b. Proposition 2: probity and authenticity crimes identified by monitoring cooperation are 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 on the suggested system.

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

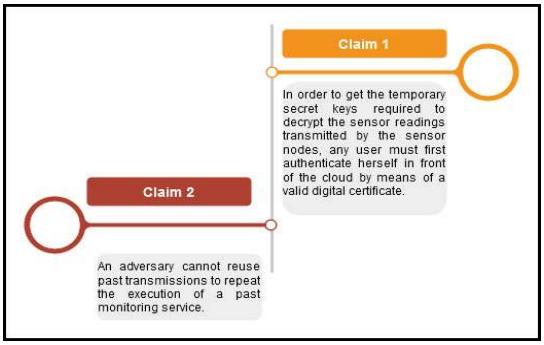

Figure7: Claims for Verified Users

d. Proposition 4: Privacy Security For Information

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.

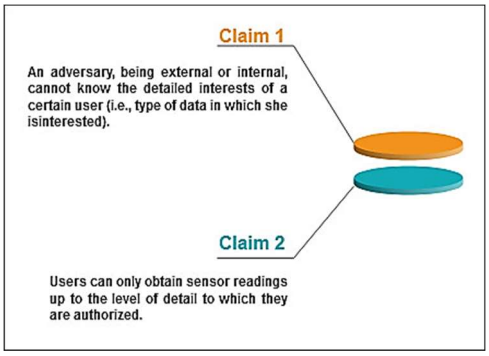

Figure 8 Claims for Privacy Security

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, it is evident that fog computing (FC) not only allows for further adaptability, but also insures easy handling of both cloud servers and end users. As a widespread facility that allows for high computing potential and the sharing of physical resources, FC has the capability to solve the complex emerging IoT challenges. As mentioned previously, FC can be applied in different sectors, including manufacturing and healthcare, and for decentralized privacy and e-learning, to mention only a few applications. In the manufacturing sector, FC insures an efficient examination system that allows for smart manufacturing through the integration of an FC-HDLF using a CNN.

It also facilitates the combination of deep learning and health-condition analysis. As far as e-learning is concerned, fog computing insures the optimization of access control during learning through encryption of learning content and exams. Subsequently, FC insures that data processing, computer services, and applications are brought closer to the end-user transfer of data. Notably, when FC is integrated into the development of smart learning, it enhances a range of factors, including awareness, alternatives, action performance, and auditability. Moreover, fog applications support IoT use for connected cars, smart homes, and smart traffic lights, and allow for AR, which can be applied to user real-time requests with the help of cloud servers.

Nevertheless, FC is not 100% effective and presents some challenges. The most pressing issues faced by developers include scalability, complexity, security, and dynamicity, among others. However, this cannot stop developers from integrating FC into IoT; hence, the proposed IoT–fog–cloud computing framework. Generally, the proposed framework in Figure Computing with IoT strives to enhance the monitoring, endpoint security, and expansion of computational applications.

Consequently, the proposed framework provides security factor in sharing E-exam which poses several security challenges, such as fine-grained access control and security preservation of E-exam. It improves the efficiency of E-exam data analysis through using a mixture of different cryptography algorithms and highlights the security of e-exams, with a focus on the organization of security procedures. It also enhances the privacy and preservation of e-exam answers, not only through monitoring, but also through a decrease of power execution and latency.

Significantly, the IoT–fog–cloud framework cannot work without consideration of two main elements: the layer components and the layer processes. Layer components to be integrated include the FGNs, cloud data centers, and GFNs. In layer processes, a series of benefits can be realized, since distribution processes help people to reduce latency and enhance response times and the preservation of privacy and security. In particular, two protocols must be included to ensure secure organization and enhance the monitoring process.

To enhance cryptography, it is important to understand that the following have to be in place: the cloud, fog nodes, users, and IoT device nodes. Enabling students to send requests to the IoT–fog–

cloud framework and hierarchically obtain the monitoring service ensures smooth and efficient e-learning. Notably, both of these protocols work efficiently together, since they allow the creation of fog blocks, cloud computing, and the use of sensor nodes. Its scalability has to be taken into consideration regarding the management of protocol actions, with benefits including affordable computation costs, limited battery consumption, and short information lengths.

As part of the future work, we propose to improve IoT-Fog-Cloud framework architecture to allow cost-optimal execution and overcome IoT-Fog computing challenges. Furthermore, we will extend the execution to process the entire learning process in higher education.

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 Information Technology,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 Computer Systems*, *vol 104*,2020,pp 187–200.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

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

[20] N. Peter, Fog computing and its real time applications. *International Journal of Emerging Technology and Advanced Engineering*, *vol 5, No* 6,2015,pp. 266–269.

[21] Adhatarao, S. S., Arumaithurai, M., & Fu, X. , FOGG: A fog computing-based gateway to integrate sensor networks to Internet. *2017 29th International Teletraffic Congress (ITC 29)* ,Vol. 2, September 2017, pp. 42–47. IEEE.

[22] S. Yi, Z. Hao, Z. Qin, & Q. Li, November). Fog computing: Platform and applications. *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*,2015,pp. 73–78. IEEE

[23] A. V. Dastjerdi, & R. Buyya, Fog computing: Helping the Internet of Things realize its potential. *Computer*, vol *49*, No 8, 2016,pp.112–116.

[24] J. K . Zao, T. T. Gan, C. K.. You, S. J. R. Méndez, C. E. Chung, Y. Wang, & T. P. Jung, Augmented brain computer interaction based on fog computing and linked data. In *2014 International Conference on Intelligent Environments*, June 2014,pp. 374–377. IEEE.

[25] N. Choi, D. Kim, S. J. Lee, & Y. Yi, A fog operating system for user-oriented IoT services: Challenges and research directions. *IEEE Communications Magazine*,vol *55*,No 8,2017,pp. 44–51.

[26] M. A. Amasha, M. F. Areed, M. F.,Alkhalaf , R. A. Abougalala, S. Elatawy, & D. Khairy, . The future of using Internet of Things (IoTs) and Context-Aware Technology in E-learning. In Proceedings of the 2020 9th International Conference on Educational and Information Technology, February 2020,pp. 114-123.

[27] A. Paul, H. Pinjari, W. H. Hong, H. C. Seo, & S. Rho, Fog computing-based IoT for health monitoring system. *Journal of Sensors*, *2018* vol. 2018, Article ID 1386470, 7 pages.

[28] A. Viejo, & D. Sánchez, Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services. *Ad Hoc Networks*, vol *82*, 2019,pp. 113–125.

[29] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M. Rahmani, & P. Liljeberg, On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, vol *36*, No 6,2016,pp. 25–35.

[30] M. Asif-Ur-Rahman, F. Afsana, , M . Mahmud, M. S. Kaiser, M. R . Ahmed, O. Kaiwartya, & A. James-Taylor, Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. *IEEE Internet of Things Journal*, *vol 6, No* 3, 2018,pp.4049–4062.

[31] N. Oualha, & K. T. Nguyen, Lightweight attribute-based encryption for the internet of things. *2016 25th International Conference on Computer Communication and Networks (ICCCN)* , August 2016,pp. 1–6. IEEE.

[32] A. Viejo, & D. Sánchez, Secure monitoring in IoT-based services via fog orchestration. Future Generation Computer Systems, vol 107,2020,pp. 443–457.

APPENDIX I

Table 1: Description Of Fog Computing-related Work in Different Fields

Authors	Field	Methods/ technologies	Related work description
Lin et al. [6]	Manufacturing	Fog computing and deep learning	Presented an efficient examination system with high accuracy for smart manufacturing using an FC-based hybrid deep-learning framework (FC-HDLF) and a convolutional neural network (CNN), which could detect possible defective products. The results showed that FC-HDLF handled massive amounts of data by removing computing from the servers to the FC nodes. It also significantly adapted its calculation execution and handled the structure and strength of problems concurrently.
Tuli et al. [7]	Healthcare	Fog computing, deep learning, and IOT devices	Proposed a framework called health fog to combine deep learning with end computing devices for heart disease analysis. Health fog used IoT to enhance healthcare services for heart patients/end users. Health fog could expand and examine the execution model in terms of energy exhaustion, network bandwidth, latency, precision, and performance duration. The results demonstrated that health fog had the most beneficial quality and forecast precision for healthcare service with respect to some fog computation summaries.
Karthika et al. [8]	Healthcare	Fog computing and IOT devices	Delivered health care services via FC to transmit knowledge easily from IoT devices. Also identified two particular related barriers (interoperability and security) and ways to deal with them. Additionally explained the fog networking essay, which centered on a response for home use, monitoring chronic disease cases.
Qu et al. [9]	Decentralized privacy	Fog computing, blockchain, and IOT devices	Highlighted problems that could be handled using FC and IoT devices, such as network bottlenecks, latency, and local independence. The work proposed a blockchain-enabled federated learning (FL-block) scheme to overcome these problems. It also facilitated independent device learning using the consensus mechanism of blockchain. The results showed the excellent performance of FL-

Authors	Field	Methods/ technologies	Related work description
			block for privacy security, execution, and resistance to attacks.
Zhou et al. [10]	Privacy-preservation	Fog computing and IoT devices	Proposed an FC privacy-preserving training design. Every fog node was permitted to accept IoT device data and perform the learning duty in the recommended manner. The results proved that the recommended design performed highly.
Tuli et al. [11]	Integrated fog platform	Fog computing, blockchain, and IoT devices	Proposed a FogBus framework to support a combination of IoT devices, FC facilities, and cloud scalability. It combined finger-pulse oximeters as IoT devices with a smartphone-based gateway and Raspberry Pi-based fog nodes for sleep apnea examination. The results showed that FogBus was lightweight and sensitive, and various FogBus environments could harmonize the FC environment through the position requirements.
Amor et al. [12]	E-learning	Fog computing	Provided an e-learning system based on FC that delivered learning from the cloud to students. The results were positive. The proposed system improved the production of the learning data summaries. Moreover, it decreased the encryption and computation costs of students' devices and optimized access control of learning content by encrypting the content and the exam.
Hassen et al. [13]	Healthcare	Fog computing and IoT devices	Proposed e-health for monitoring elderly people's health using IoT devices and FC, which enabled the regular monitoring of combined physiological and overall health indicators for the aged. Also, it assisted doctors by sending alerts. The results showed that most users considered the proposed system helpful, simple to use and learn, and capable of monitoring a variety of health care issues for the elderly.
Raman [14]	Education	Fog computing	Highlighted the potential of FC for education, demonstrating that FC technology supported educational operations and facilitated an agile platform. The results indicated the potential of FC for high growth in the future, due to it substantially supporting

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Authors	Field	Methods/ technologies	Related work description
			day-to-day procedures for various sectors, including education.
Alam [15]	Use of IoT to provide secure and authentic communication among the physical things.	Fog computing, blockchain, and IoT devices	Built a framework that combined IoT, FC, and blockchain. Blockchain technology was used to join, transmit, and exchange data among IoT nodes. IoT nodes were used to validate the actions in the network, then they were combined with preexisting blockchains and transferred to the network. The framework was tested, and the results were positive.