

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

*JYOTHULA SWATHI, SANKOJU NEERAJA, NELAVELLI JAYAMMA*

*Dept of ECE,*

*Priyadarshini Institute of Science and Technology for Women Khammam*

### ABSTRACT

E-learning systems have gained significant attention in recent years, with the demand for secure data transmission among students, instructors, and examiners becoming increasingly crucial. The integration of intelligent devices, data analysis, and cybersecurity into e-learning environments is largely supported by the Internet of Things (IoT). When combined with Fog and Cloud computing, IoT can significantly enhance the performance of latency-sensitive and computing-intensive tasks. This paper presents an IoT-Fog-Cloud framework designed to address the security challenges associated with sharing E-exams, including fine-grained access control and the preservation of security. The proposed framework brings services closer to students, improves the efficiency of E-exam data analysis, and reduces the encryption burden on users' devices by offloading part of the encryption process to fog servers. Additionally, it provides fine-grained access control to E-exam content using various cryptographic techniques. The IoT-Fog-Cloud framework operates by integrating layer components and layer processes. Layer components include Fog Gateway Nodes (FGNs), cloud data centers, and General Fog Nodes (GFNs), while layer processes offer benefits such as reduced latency, enhanced response times, and improved privacy and security preservation. The framework achieves data confidentiality, fine-grained access control, collusion resistance, and unforgeability, ensuring secure procedures within the proposed framework.

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

### INTRODUCTION

The advent of Fog computing (FC) has introduced a highly virtualized platform characterized by a distributed hierarchical structure. This structure facilitates increased adaptability and improved handling of data between end users and cloud servers. FC is essentially a more extensive form of cloud computing, offering substantial computing power for storing, sharing, and managing software applications or physical resources. It also provides efficient services for the end users of IoT and terminal devices, making it integral to a range of applications such as smart cities, smart learning, smart homes, e-healthcare, and grid systems. The architecture of FC is composed of three main layers: the device/end layer, one or more layers of fog nodes, and at least one cloud data center (the cloud layer). These layers work together to ensure that data is processed and managed effectively across different levels of the network. The device/end layer is closest to the end users and consists of IoT devices that gather raw data and transfer it to the fog layer. The fog layer processes this data and regularly communicates with the cloud layer, which performs more complex data storage and analysis tasks.

In recent years, the integration of IoT with Fog and Cloud computing has emerged as a powerful combination for enhancing the performance of various applications, particularly those that are latency-sensitive and require significant computing resources. This combination has been particularly beneficial in the context of e-learning and E-exams, where the need for secure, efficient, and scalable data management solutions is paramount. The proposed IoT-Fog-Cloud framework aims to address these needs by providing a secure and efficient environment for sharing and managing E-exams. The framework is designed to bring services closer to students, reduce latency, and enhance the overall performance of E-exam systems. By offloading part of the encryption process to fog servers, the framework reduces the computational burden on users' devices, making it easier for students to participate in E-exams without compromising security.

## **RELATED WORK**

The rapid expansion of IoT has introduced several complex challenges, particularly in terms of data security, latency, and resource management. However, Fog computing has demonstrated significant potential in addressing these challenges. This section provides an overview of related work in the field of IoT, Fog computing, and Cloud computing, highlighting key developments and the role of these technologies in enhancing E-learning and E-exams. Fog computing has emerged as a critical technology for extending the capabilities of IoT. By providing a distributed computing environment closer to the data sources, FC reduces the need to transmit large volumes of data to centralized cloud servers, thereby minimizing latency and improving response times. This is particularly important in applications such as smart cities, healthcare, and E-learning, where real-time data processing is essential. Several studies have explored the integration of Fog computing with IoT to enhance various applications. For instance, Bonomi et al. [2] discussed the role of Fog computing in IoT, emphasizing its potential to handle latency-sensitive applications by processing data closer to the source. Similarly, Atlam et al. [3] reviewed the challenges and opportunities of Fog computing in IoT, highlighting its ability to address issues such as network bandwidth constraints and resource-constrained devices.

E-learning has become increasingly popular, driven by the need for flexible and accessible education. However, the rise of E-learning has also brought new challenges, particularly in ensuring the security and integrity of online assessments such as E-exams. The integration of IoT and Fog computing into E-learning environments offers a promising solution to these challenges, providing a secure and scalable platform for managing educational content and assessments. Recent research has focused on the use of Fog computing to enhance the security and efficiency of E-exams. For example, Amor et al. [12] proposed a Fog-based E-learning scheme that leverages Fog computing to improve the security of E-exams. Their approach involves using Fog nodes to process and encrypt exam data, reducing the burden on students' devices and ensuring that the data remains secure throughout the assessment process.

## **THE ROLE OF CLOUD AND FOG COMPUTING IN SMART LEARNING**

Smart learning represents the evolution of traditional educational environments into more flexible, personalized, and technology-driven spaces. It leverages a combination of intelligent technologies and environments to provide learners with an enhanced educational experience. Fog computing plays a critical role in this transformation by bringing data processing, applications, and computer services closer to end-users, effectively transforming centralized computing into a consistent stream of real-time data processing. Smart learning environments aim to promote the quality of life for learners by offering contextual, personalized, and seamless education. These environments are characterized by real-time communication, location awareness, large-scale sensor networks, and support for dynamic content delivery. Fog computing enhances these capabilities by enabling real-time data processing at the network edge, thereby reducing latency and improving the overall efficiency of smart learning systems.

The integration of Fog computing into smart learning environments allows for the efficient management of large volumes of educational data, including student performance metrics, learning content, and assessment results. By processing this data closer to the learners, Fog computing reduces the time required to access and analyze information, enabling more responsive and adaptive learning experiences. Moreover, Fog computing enhances the security and privacy of smart learning environments by providing localized data processing and storage. This reduces the risk of data breaches and ensures that sensitive information, such as student records and exam results, is protected from unauthorized access.

Fog computing can be applied to various aspects of E-learning, from content delivery to assessment management. For instance, Fog nodes can be used to process and encrypt E-exam data, ensuring that it is securely transmitted to students' devices and preventing unauthorized access. Additionally, Fog computing can support real-time monitoring and analysis of student performance, enabling educators to

provide timely feedback and interventions. One of the key benefits of Fog computing in E-learning is its ability to reduce the computational burden on students' devices. By offloading complex tasks, such as data encryption and analysis, to Fog nodes, the framework ensures that students can participate in E-exams without experiencing performance issues on their devices. This is particularly important in resource-constrained environments, where students may not have access to high-performance devices. The proposed IoT-Fog-Cloud framework builds on these capabilities by integrating Fog computing into the E-learning environment. The framework is designed to enhance the security, efficiency, and scalability of E-exams, making it easier for educational institutions to manage online assessments and ensuring that students can complete their exams securely and efficiently.

### **PROPOSED IoT-FOG-CLOUD FRAMEWORK**

The IoT-Fog-Cloud framework presented in this paper is designed to enhance the security and efficiency of E-exams by integrating Fog computing with IoT and Cloud technologies. The framework consists of several layers, each of which plays a critical role in ensuring that E-exams are conducted securely and efficiently. This section provides a detailed overview of the framework, including its components, processes, and protocols. The IoT-Fog-Cloud framework is structured around a multi-layered architecture that combines IoT devices, Fog nodes, and Cloud servers to provide a secure and scalable platform for E-exams. The framework is designed to process and manage E-exam data at various levels of the network, ensuring that the data is securely transmitted and efficiently managed throughout the assessment process. The IoT devices, located at the bottom layer of the framework, represent the physical devices used by students to participate in E-exams. These devices, which include laptops, tablets, and smartphones, are connected to the Fog layer, where the data is processed and encrypted before being transmitted to the Cloud layer for storage and analysis. The Fog layer plays a critical role in the framework by providing the computational resources needed to process and secure E-exam data. This layer consists of several types of Fog nodes, including Fog Gateway Nodes (FGNs) and General Fog Nodes (GFNs), which are responsible for processing, encrypting, and transmitting E-exam data. The Cloud layer, located at the top of the framework, serves as the central repository for E-exam data. It is responsible for storing and analyzing the data collected by the Fog layer and providing the necessary computational resources to support the framework's operations. The Cloud layer also plays a key role in ensuring the security and integrity of the data by implementing various cryptographic techniques and security protocols. The IoT-Fog-Cloud framework is composed of two main elements: layer components and layer processes. Each of these elements is critical to the framework's ability to securely manage and process E-exam data.

These include laptops, tablets, and smartphones that students use to participate in E-exams. IoT devices are responsible for receiving E-exams and transmitting students' answers to the Fog layer for processing. FGNs serve as the entry points for distributed computing within the framework. They format the IoT device environment to perform the necessary processes and applications, including the authentication and encryption of E-exam data. GFNs perform various computational tasks using different hardware resources, such as processing devices, memory, repositories, and micro data centers. They are responsible for managing the IoT-Fog-Cloud framework and ensuring that E-exam data is processed efficiently and securely. The Cloud data centers provide additional computational resources and storage for the IoT-Fog-Cloud framework. They support the processing of E-exam data that cannot be handled by the Fog layer, ensuring that the framework remains scalable and efficient.

The IoT-Fog-Cloud framework supports distributed processing of E-exam data in real-time, reducing latency and providing rapid responses. This is achieved by distributing the computational tasks across the various layers of the framework, ensuring that the data is processed as close to the source as possible. The framework includes several security and privacy preservation mechanisms, such as encryption and access control, to ensure that E-exam data is protected from unauthorized access. These mechanisms are implemented at multiple layers of the framework, providing a comprehensive approach to data security. The IoT-Fog-Cloud framework is designed to be highly scalable, allowing it to accommodate

large numbers of users and devices. This is achieved by leveraging the computational resources of the Fog and Cloud layers, ensuring that the framework can handle increasing amounts of data and processing tasks without compromising performance.

The IoT-Fog-Cloud framework relies on two primary protocols to ensure secure procedures: secure organization and secure control/monitoring. These protocols are essential for managing the transmission and processing of E-exam data, ensuring that it remains secure throughout the assessment process. The secure organization protocol is responsible for establishing secure communication channels between the various components of the IoT-Fog-Cloud framework. This protocol involves the exchange of cryptographic keys between the Cloud, Fog nodes, and IoT devices, ensuring that data is encrypted and transmitted securely. The process begins with the student registering on the IoT-Fog-Cloud framework and obtaining authentication from the Cloud. The Cloud then generates an asymmetric cryptographic key and a random value for the security monitoring service, which is shared with the student. The student uses this key to establish secure communication with the Fog Gateway Node, ensuring that their E-exam data is protected from unauthorized access.

The secure control/monitoring protocol manages the monitoring of E-exam data as it is transmitted and processed within the IoT-Fog-Cloud framework. This protocol involves the continuous transmission of E-exam data from IoT devices to Fog nodes, and ultimately to the Cloud, where it is stored and analyzed. The monitoring process begins when the student submits their E-exam answers to the Fog Gateway Node. The Gateway Node verifies the student's request and forwards the data to the appropriate Fog nodes for processing. The Fog nodes then transmit the processed data to the Cloud, where it is stored and analyzed. Throughout this process, the data is continuously monitored to ensure its integrity and authenticity. Security of the IoT-Fog-Cloud framework is a critical consideration, particularly given the sensitive nature of E-exam data. This section analyzes the security and privacy capabilities of the proposed framework, focusing on four key propositions: reliable communication of sensor passages, detection of integrity and authenticity crimes, user verification, and privacy security for information.

The proposed framework ensures the confidentiality, authenticity, and integrity of transmitted sensor data, protecting it from internal or external attackers. If internal attackers gain control of Fog or sensor nodes, their attacks will only compromise the data identified by the modified nodes, without affecting the overall system. The framework uses cryptographic techniques to ensure that sensor data remains confidential during transmission. This prevents unauthorized access to the data, even if attackers gain control of some nodes. Digital signatures are used to verify the authenticity of sensor data, ensuring that it originates from a legitimate source. The framework includes mechanisms for detecting and correcting data integrity issues, ensuring that the data remains accurate and unaltered during transmission. The framework is capable of detecting and responding to dynamic attacks, such as those that attempt to alter data in transit. The framework is designed to be resilient to attacks, ensuring that the system can continue to operate even if some nodes are compromised.

#### Detection of Integrity and Authenticity Crimes

The framework includes mechanisms for monitoring the integrity and authenticity of data as it is transmitted between Fog nodes and users. This allows the system to detect and respond to attacks that attempt to compromise the integrity or authenticity of the data.

This proposition is supported by the following claims:

1. Real-time Monitoring: The framework continuously monitors data as it is transmitted, allowing it to detect and respond to attacks in real-time.

2. Integrity Checks: The framework performs regular integrity checks on the data, ensuring that it remains accurate and unaltered .

3. Authentication: The framework verifies the authenticity of data at multiple points in the transmission process, ensuring that it originates from a legitimate source .

#### Verified Users

The framework ensures that only verified users can access the system, preventing unauthorized access to sensitive data. This is achieved through a combination of digital certificates, public key infrastructure (PKI), and cryptographic techniques .

This proposition is supported by two claims:

1. User Authentication: The framework requires users to authenticate themselves using digital certificates before they can access the system. This ensures that only authorized users can access the data .

2. Access Control: The framework implements fine-grained access control mechanisms, ensuring that users can only access the data and services they are authorized to use .

#### Privacy Security for Information

The framework includes measures to protect the privacy of users' data, ensuring that only the information necessary for specific tasks is exposed. This is achieved through data minimization and encryption techniques .

This proposition is supported by two claims:

1. Data Minimization: The framework ensures that only the minimum amount of data necessary for a specific task is exposed, reducing the risk of privacy breaches .

2. Encryption: The framework uses encryption to protect data during transmission, ensuring that it remains confidential and secure .

### **PERFORMANCE ANALYSIS**

The performance of the IoT-Fog-Cloud framework is critical to its ability to support secure and efficient E-exams. This section analyzes the framework's performance, focusing on its scalability, computational efficiency, and energy consumption .The scalability of the IoT-Fog-Cloud framework is influenced by several factors, including the number of users, the number of Fog and sensor nodes, and the complexity of the tasks being performed. The framework is designed to be highly scalable, allowing it to accommodate large numbers of users and devices without compromising performance .The framework achieves scalability through its distributed architecture, which allows computational tasks to be spread across multiple layers of the network. This reduces the load on individual nodes and ensures that the system can handle increasing amounts of data and processing tasks .The computational efficiency of the IoT-Fog-Cloud framework is critical to its ability to support real-time E-exams. The framework is designed to offload complex computational tasks, such as data encryption and analysis, to the Fog layer, reducing the burden on users' devices and ensuring that the system remains responsive .

The framework also includes mechanisms for optimizing computational tasks, such as parallel processing and load balancing, to ensure that tasks are completed efficiently and within the required timeframes .Energy consumption is a key consideration for the IoT-Fog-Cloud framework, particularly given the

limited battery life of IoT devices. The framework is designed to minimize energy consumption by offloading computational tasks to the Fog layer, reducing the need for IoT devices to perform energy-intensive operations. The framework also includes energy-efficient protocols for data transmission and processing, ensuring that the system can operate for extended periods without depleting the batteries of IoT devices.

## CONCLUSION

Fog computing has emerged as a powerful technology for enhancing the performance and security of IoT-based systems, particularly in the context of E-learning and E-exams. The IoT-Fog-Cloud framework presented in this paper leverages Fog computing to provide a secure, efficient, and scalable platform for managing E-exams. The framework addresses the key challenges associated with E-exams, including data security, latency, and computational efficiency, by integrating IoT, Fog, and Cloud technologies. The proposed framework enhances the security of E-exams by implementing robust encryption and access control mechanisms, ensuring that exam data is protected from unauthorized access. It also improves the efficiency of E-exam data analysis by offloading computational tasks to the Fog layer, reducing the burden on users' devices and enabling real-time processing of exam data. The IoT-Fog-Cloud framework is designed to be highly scalable, allowing it to accommodate large numbers of users and devices without compromising performance. It achieves this through a distributed architecture that spreads computational tasks across multiple layers of the network, ensuring that the system remains responsive and efficient. In conclusion, the IoT-Fog-Cloud framework represents a significant advancement in the field of E-learning, offering a secure and efficient solution for managing E-exams. The framework's ability to integrate IoT, Fog, and Cloud technologies provides a powerful platform for enhancing the performance and security of E-learning environments, making it an essential tool for educational institutions.

## REFERENCES

1. Sunyaev, A., & Sunyaev, A. (2020). *Internet Computing*. Springer International Publishing.
2. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on mobile cloud computing* (pp. 13-16).
3. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: a review. *Big Data and Cognitive Computing*, 2(2), 10.
4. Abougalala, R. A., Amasha, M. A., Areed, M. F., Alkhalaf, S., & Khairy, D. (2020). Blockchain-enabled smart university: A framework. *Journal of Theoretical and Applied Information Technology*, 98(17).
5. Salaht, F. A., Desprez, F., & Lebre, A. (2020). An overview of service placement problem in fog and edge computing. *ACM Computing Surveys (CSUR)*, 53(3), 1-35.
6. Lin, S. Y., Du, Y., Ko, P. C., Wu, T. J., Ho, P. T., & Sivakumar, V. (2020). Fog Computing-Based Hybrid Deep Learning Framework in effective inspection system for smart manufacturing. *Computer Communications*, 160, 636-642.
7. Tuli, S., Basumatary, N., Gill, S. S., Kahani, M., Arya, R. C., Wander, G. S., & Buyya, R. (2020). 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*, 104, 187-200.
8. Karthika, P., Babu, R. G., & Karthik, P. A. (2020). Fog computing using interoperability and IoT security issues in health care. In *Micro-Electronics and Telecommunication Engineering* (pp. 97-105). Springer, Singapore.
9. Qu, Y., Gao, L., Luan, T. H., Xiang, Y., Yu, S. Y., Li, B., & Zheng, G. (2020). Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal*, 7(6), 5171-5183.
10. Zhou, C., Fu, A., Yu, S., Yang, W., Wang, H., & Zhang, Y. (2020). Privacy-Preserving Federated Learning in Fog Computing. *IEEE Internet of Things Journal*, 7(11), 10782-10793.

11. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). Fogbus: A blockchain-based lightweight framework for edge and fog computing. *Journal of Systems and Software*, 154, 22-36.
12. Amor, A. B., Abid, M., & Meddeb, A. (2020). Secure fog-based e-learning scheme. *IEEE Access*, 8, 31920-31933.
13. Hassen, H. B., Dghais, W., & Hamdi, B. (2019). An e-health system for monitoring elderly health based on Internet of Things and Fog computing. *Health Information Science and Systems*, 7(1), 24.
14. Raman, A. (2019). Potentials of fog computing in higher education. *International Journal of Emerging Technologies in Learning (iJET)*, 14(18), 194-202.
15. Alam, T. (2019). IoT-Fog: A communication framework using blockchain in the internet of things. *International Journal of Recent Technology and Engineering (IJRTE)*, 7(6). arXiv preprint arXiv:1904.00226.
16. Rekha, G., Tyagi, A. K., & Anuradha, N. (2020). Integration of Fog Computing and Internet of Things: A Useful Overview. In *Proceedings of ICRIC 2019* (pp. 91-102). Springer, New York, USA.
17. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6), 854-864.
18. Zhu, Z. T., Yu, M. H., & Riezebos, P. (2016). A research framework of smart education. *Smart Learning Environments*, 3(1), 4.
19. Bartels, A. H., Daley, E., Parker, A., Evelson, B., & Muteba, C. (2009). Smart computing drives the new era of IT growth. Forrester Inc.
20. Peter, N. (2015). Fog computing and its real-time applications. *International Journal of Emerging Technology and Advanced Engineering*, 5(6), 266-269.
21. Adhatarao, S. S., Arumathurai, M., & Fu, X. (2017). 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. Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). Fog computing: Platform and applications. *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 73-78.
23. Dastjerdi, A. V., & Buyya, R. (2016). Fog computing: Helping the Internet of Things realize its potential. *Computer*, 49(8), 112-116.
24. Zao, J. K., Gan, T. T., You, C. K., Méndez, S. J. R., Chung, C. E., Wang, Y., & Jung, T. P. (2014). Augmented brain-computer interaction based on fog computing and linked data. In *2014 International Conference on Intelligent Environments* (pp. 374-377). IEEE.
25. Choi, N., Kim, D., Lee, S. J., & Yi, Y. (2017). A fog operating system for user-oriented IoT services: Challenges and research directions. *IEEE Communications Magazine*, 55(8), 44-51.
26. Amasha, M. A., Areed, M. F., Alkhalaf, S., Abougalala, R. A., Elatawy, S., & Khairy, D. (2020). 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* (pp. 114-123). IEEE.
27. Paul, A., Pinjari, H., Hong, W. H., Seo, H. C., & Rho, S. (2018). Fog computing-based IoT for health monitoring system. *Journal of Sensors*, 2018, Article ID 1386470, 7 pages.
28. Viejo, A., & Sánchez, D. (2019). Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services. *Ad Hoc Networks*, 82, 113-125.
29. Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M., & Liljeberg, P. (2016). On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, 36(6), 25-35.
30. Asif-Ur-Rahman, M., Afsana, F., Mahmud, M., Kaiser, M. S., Ahmed, M. R., Kaiwartya, O., & James-Taylor, A. (2018). Toward a heterogeneous mist,