An Internet-of-Things and fog computing-based exam security system

Dr. AVULA MAHESWARA[1] RAO, B MADHAVA[2]

Assistant professor1,2
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
P.B.R.VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE
S.P.S.R NELLORE DIST, A.P , INDIA , KAVALI-524201

ABSTRACT

There has been recent indication that e-learning systems are in high demand. There is a lot of information being sent back and forth between students, teachers, and examiners, and it has to be delivered safely. The Internet of Things provides a crucial platform for integrating smart devices, data analysis, and cybersecurity (IoT). Specifically, the integration of Fog with cloud computing has the potential to improve the efficiency of many different kinds of latency-sensitive and computationally heavy applications. This article introduces the IoT-Fog-Cloud architecture for addressing the security concerns raised by the widespread distribution of electronic examinations, including the need for fine-grained access control and the maintenance of examination integrity. In addition, the suggested structure helps provide services to the kids who need them. In addition to enhancing the effectiveness of E-exam data analysis, this study enables fine-grained access control to E-exam material through encryption, offloads some of the encryption cost from users' devices to fog servers, and minimises the computational cost of encryption. The components and activities of each layer are taken into account in the course of the framework's operation, making IoT-fog-cloud a viable option. The FGNs, cloud data centres, and GFNs are all part of the layer that has to be merged. Distribution procedures aid students in decreasing latency, improving reaction times, and preserving privacy and security, all of which are advantageous in layer processes. This study demonstrates that the proposed IoT-Fog-Cloud system may provide safe processes for their implementation, including data confidentiality, fine-grained access control, collusion resistance, and unforgeability.

Keywords:

E-learning, Fog Computing, Security Systems, Internet of Things (IoTs), and Exams.

INTRODUCTION

Fog computing (FC) is a highly virtualized, hierarchically distributed platform that improves scalability and data management for both end users and cloud servers [1]. What this means is that it is a popular kind of cloud computing that can store and share large amounts of data, run complex programmes, and provide effective services to the people who use the Internet of Things and endpoint devices. It's useful for a wide variety of things, including "smart cities," "smart learning," "smart homes," "e-health," and "grid systems" [2]. As shown in Figure1, the architecture of FC is composed of three distinct levels: the device/end layer, one or more layers of fog nodes, and a cloud data centre (cloud layer)

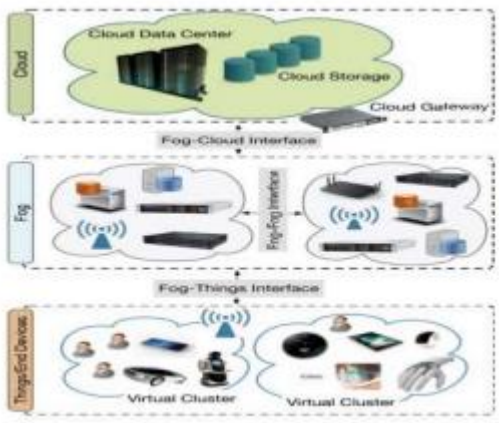

Figure 1: Architecture of Fog Computing (Atlam et al. 2018)

Terminal/Device Layer:

This layer is the one that's most directly accessible to the people who will be using the system. It is made up of two distinct categories of Internet-of-Thing's gadgets: first, mobile IoT gadgets like cameras and smartphones, which have limited bandwidth, computational power, and storage space; and second, stationary IoT gadgets like RFID readers (RFID). These Internet-of-Thing's gadgets may collect data in its raw form and send it to the fog layer [3].

Layer of fog:

The processing of data, archiving of queries, and frequent uploading of data reports to the cloud are all facilitated by this method. Devices and nodes in the intermediate layer of a fog computing system include things like bridges, routers, laptops, and dedicated fog servers, as well as access points with increased processing power. Any of these devices connected to a cloud server will be able to forward queries to data centres in the cloud. They may be used everywhere there is an internet connection, even in a car or on the side of the road [4].

Puffs of cloud:

It consists of several data servers and storage facilities, each of which can provide complex summaries and store vast quantities of information. Large amounts of data may be stored on the cloud, which users can access from any device, at any time. It uses virtualization technology to protect the confidentiality of IoT data and apps, allowing them to independently serve the needs of a large number of users. Enhancing IoT applications like smart energy distribution, health condition monitoring, and network optimization necessitates the cloud to accept reports from many fog nodes and conduct a universal examination of the data given by FC nodes [5].

FURTHER READING

Table 1 (APPENDIX I) provides an overview of some related studies that shows how the new FC technology may solve many of the challenging issues posed by the burgeoning IoT. Several safety concerns, including fine-grained access control and security preservation of E-exam, are highlighted in the prior highlight literature, and these difficulties are addressed by the present IoT-Fog-Cloud system. In addition, the suggested structure helps provide services to the kids who need them. In addition to enhancing the effectiveness of E-exam data analysis, this study enables fine-grained access control to E-exam material through encryption, offloads some of the encryption cost from users' devices to fog servers, and minimises the computational cost of encryption. Additionally, the proposed IoT-Fog-Cloud framework is capable of achieving data security, fine-grained access control, collusion resistance, and unforgeability to guarantee safe practises while implementing the framework.

What Cloud and Fog Computing Mean for Personalized Learning?

Applications for e-learning and smart learning are currently being developed, and they rely on many forms of intelligence both inside and outside of the classroom. Educators and students alike stand to profit from the efficient dissemination of instructional materials in multi-ethnic settings when FC models are used [12]. By changing centralised computing into consistent streaming via networks, FC plays a pivotal role in bringing data processing, applications, and computer services closer to end-users. FC is a cloud-only service that customers may access without much difficulty [16]. As cloud computing is not yet widely accessible for most IoT applications, fog computing offers an alternate solution to this problem (via its interoperability with IoT; [2]. In today's day, the Internet of Things facilitates the uncovering and analysis of previously inaccessible information. The Internet of Things (IoT) is designed to improve human life by bridging the gap between people and their electronic gadgets, software, and physical surroundings.

Challenges

While FC offers significant benefits for certain IoT applications, it also introduces difficulties that FC technology must address. In Figure 3, we see five of the most critical problems that programmers confront today [25,26,22].

Figure 2: Challenges of Fog Combined with IoT

PROPOSED IoT-FOG-CLOUD FRAMEWORK

Framework Overview

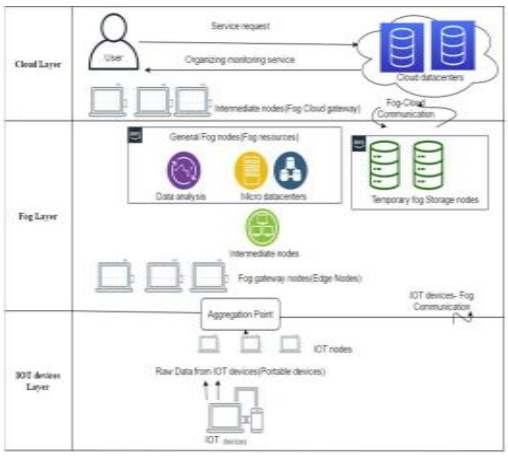

Figure 3 : IoT-Fog-Cloud Architecture for A Secure E-exams System

As a whole, the suggested framework is reliant on IoT-based FC to improve the endpoint security, monitoring, and computation of IoT devices used by students to take e-exams. Figure 4's lower half

depicts the IoT device layer, which consists of deployable devices (e.g., on portable devices belonging to students within educational institutions). Devices are employed to receive at least one electronic test and forward student responses to a central location at the FC layer's periphery. The FC layer has power-limited components. Since can be seen in Figure 4, these devices are not suited for significant computational processes as they can only respond to inquiries collected at the higher levels through the FC nodes. In addition, there are four distinct kinds of nodes in the fog layer, including gateway nodes, storage nodes, and temporary storage nodes (TFSNs). E-exam responses may be transferred through anonymous WAN networks, and portable devices may be utilised in unfamiliar and untrusted environments (such as students' homes), making them vulnerable to attack or control by malicious software.

Analysis of security measures

Here, we take a look at how four different approaches affect the proposed system's security and privacy. Numerous claims [27][28] back up each thesis. a. First Hypothesis: Sensor Ports Can Be Trusted for Reliable Communication This novel technique shields transmitted sensor passages from internal or external criminals who may launch dynamic assaults, ensuring their privacy, authenticity, and truthfulness. If malicious actors inside a system are in charge of a fog or sensor block, their assaults will only disrupt the nodes that have been altered, dripping the information that identifies them. The proposed approach would effectively reveal the issue if internal attackers attempt integrity attacks or disturb the data in transfer. Figure 6 presents the five assertions that underpin this hypothesis.

Figure 4 : Claims for Reliable Communication of Sensor Passages

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.

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.

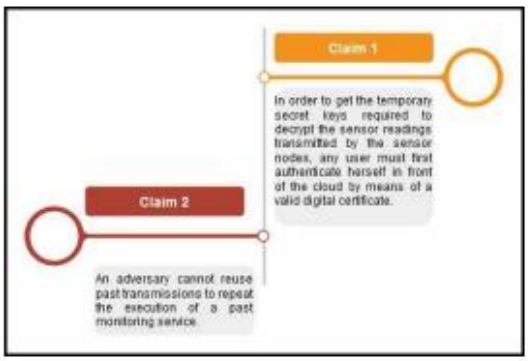

Figure 5 : Claims for Verified Users

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.

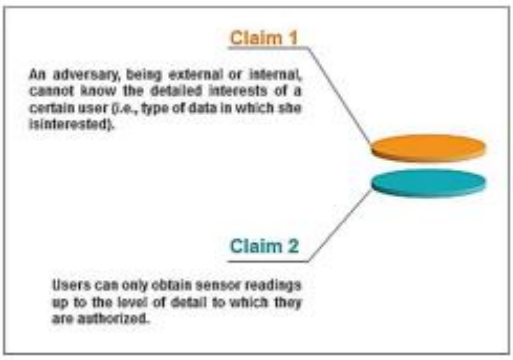

Figure 6 Claims for Privacy Security

Evaluation of Past Efficiency

The proposed system is comprised of two protocols: secure organisation and secure control/monitoring. Both are operational because of how the fog blocks, sensor nodes, and cloud are structured. For the system to scale, it requires protocols that account for sensor nodes' (battery-powered, lightweight media) three unique characteristics: (1) short information length; (2) inexpensive computational cost; and (3) restricted battery usage. [29][30][31][[32] . In contrast to the secure organisation protocol, which is managed on a per-offer basis, the secureA linked process is used by the control/monitoring protocol to handle the continual streams of data. Since the burden of the proposed technique is split, the selection of cryptographic activities is restricted by the secure organisation process, and the monitoring method is sent as an efficient and scalable protocol that just performs lightweight operations. Due to the extensive labour involved in monitoring services, the secure control/monitoring protocol has a significant impact on the scalability of the proposed system. Particular attention was paid to the question of how well it scales. Scalability The energy required by sensor nodes to process the necessary numbers and the communication distance traded off by the persistent conveyance of sensed data are two primary aspects that alter the scalability of the monitoring protocol. The two characteristics being referred to are:

• nU = the number of people using the technique at once.

A network's current fog and sensor node count is denoted by nFN + nSN. Initial information is disseminated from U to the sensor hubs using the checking convention, and subsequent information is sent back and forth between U and the hubs in a steady fashion using the same checking convention. U broadcasts a message to all of the sensor hubs using FNep-specific protocols, which is a multicast stage in the checking protocol. There is a unique identifier (v), two complementary characteristics, and a single HMAC value in this transmission. The FNep has cautiously approved the statement. Hubs in the middle of the haze and the sensors verify the signature, store some data, and forward the message to the appropriate hubs.

CONCLUSION

In conclusion, it is clear that FC not only enables more flexibility but also guarantees easier management of both cloud servers and end users. FC has the potential to answer the complicated growing IoT difficulties since it is a widely available facility that permits high processing potential and the sharing of physical resources. As was previously said, FC has a wide range of potential uses, including but not limited to manufacturing, healthcare, decentralised privacy, and e-learning. By incorporating an FC HDLF trained with a CNN, the industrial industry has access to an efficient inspection system that enables smart production. In addition, it makes it easier to integrate deep learning with health data analysis. Fog computing offers the best possible access control during e-learning by encrypting all course materials and assessments. Therefore, FC guarantees that data processing, computer services, and application transfer is facilitated at a location closer to the end-user. The incorporation of FC into the design of intelligent learning improves a number of aspects. Moreover, fog applications enable augmented reality, which may be applied to user real-time requests with the aid of cloud servers, and IoT usage for linked automobiles, smart homes, and smart traffic signals.

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 MicroElectronics 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 ehealth 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.