A Fog-assisted Secure Architecture for heterogeneous IoT-based Educational Scenario

Prabhdeep Singh
Department of Computer Engg.
Punjabi University, Patiala
Punjab, India
ssingh.prabhdeep@gmail.com

Rajbir Kaur
Department of ECE Punjabi
University, Patiala Punjab, India
Email: rajbir277@yahoo.co.in

Rajni Aron
Department of CSE Lovely
Professional University
Punjab, India
Email: rajni3387@gmail.com

***Abstract*—**IoT is inter-networking of physical devices, vehi- cles, smart-devices, buildings, and other items embedded with electronics, software, sensors, actuators, and network connec- tivity which enable these objects to collect and exchange data. Improving response time and security for highly latency-sensitive applications such as smart healthcare, smart education and smart agriculture has become increasingly difficult. Higher education is still in its early stage with regards to innovation appropriation and joint effort. This article aims to reduce the latency, energy consumption of cloud data centres and total delay of various IoT educational devices with the help of fog devices. To solve the problem mentioned above, we proposed A Secure IoT based Educational Cloud-Fog Architecture, a three-tier architecture for educational institutions. This architecture helps to provide the secure environment for transferring and storage of data. In order to achieve data security, the concept of Offset Code Book (OCB) is used and modified Dynamic Source Routing Protocol (DSR) is proposed for delivering fast and secure communication between layers in the architecture. The performance of the proposed framework has been evaluated through the iFogsim toolkit. Furthermore, the efficiency of the proposed Modified DSR algorithm has been compared with the existing DSR algorithms through NS-2. The experimental results show that the proposed framework outperforms the existing algorithms by minimizing latency, delay, and energy consumption.

Keywords*—*Fog Computing, Cloud Computing, Offset Code Book, Dynamic Source Routing, Internet of Things, Educational Framework.

I. INTRODUCTION

the Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of the concept is the perva- sive presence around us of a variety of things or objects such as Radiofrequency Identification (RFID) tags, sensors, actuators and mobile phones. the emergence of IoT has influenced various application domain such smart cities [9], e-learning [6], health-care applications [24], agriculture [4], and so on. In to- day era, the connected devices combined with cloud computing has become the pioneer to provide education accessible across the globe. Education plays an important role in the growth of a country [2]. The higher education is provided to students by opening new universities and colleges across the country to be transformed by IoT. By 2020, more than 5 billion devices will be connected worldwide. In the education system, IoT delivers basic connectivity among students, faculty members, and staff. It enables the integration of smart laboratories with new smart types of equipment and systems. The latest survey shows that nearly 2/3 of total workloads in traditional IT space will be shifted to the IoT enabled cloud [8]. In cloud-based systems, the increasing workload on cloud data-centres leads to introduce network congestion, high latency and more energy consumption of data-centres [8]. On the other hand, the storage of educational data needs a secure transmission protocol and security of data-centres.

Fog Computing, proposed by Cisco in 2014, plays a bridge between end-user and cloud that provide services with low latency and less traffic congestion [18]. The fog layer consists geo-distributed fog servers those process computations at the edge of systems. Each fog server has equivalent computing capabilities to process a huge amount of workload at the edge. Thus, a very less amount of workload is transferred to the cloud for storage, analytic or further processing purpose. Therefore, fog computing becomes a major driver of the IoT in education systems. With an ever-increasing number of connected devices generating an unprecedented amount of data, connecting everything to a central cloud is become possible with fog computing.

1) Motivation: Although significant efforts are required to utilize traditional Information and Communication Technology (ICT) infrastructures for implementing educational service- based solutions. Cloud computing becomes insufficient to process real-time data for quick decision making due to the limited set of constrained resources. Moreover, fog-based infrastructures are usually confined to process data with mini- mum time delay within a geographic region and thus result in the minimized cost of processing, latency, storage and energy requirements. Fog computing, in contrast, relieves users from the need to own their physical computing infrastructures and gives them the liberty to perform the intensive computations at the edge of the network. It allows for wide accessibility and provides access to huge amount of computational and storage resources as per the requirements of users limited by the available infrastructure at fog layer.

In this paper, A Secure IoT-based Educational Cloud- Fog Architecture is proposed. The focus of the the proposed framework is to reduce the workload, latency, and energy consumption of cloud data-centres. In addition, it provides a secure communication protocol as well as the overall data security of cloud data-centres. It uses a three-layer architecture. The first layer consists IoT sensors and actuators (mobile devices and tablets, IoT enabled board, attendance tracking systems, security cameras, doorbells & lock etc.) to collect the end-user data to be processed. The second layer has fog nodes which are used for pre-processing of the data received from IoT devices. It consists of network edge devices such as router and switch, etc. those are responsible for the local processing of data at the edge. The uppermost layer has cloud data- centres where final processing of data is completed. To secure the communication between fog servers and data-centres the DSR protocol is modified. The Offset Code Book(OCB) [15] concept is used for providing data security at cloud data- centers.

The remainder of this paper is organized as follows. Section II presents previous work related to performance challenges as well as security challenges of cloud and fog computing. In section III an secure IoT based Educational cloud-fog Archi- tecture is proposed. In section IV, the Performance Evaluation is presented by simulating the proposed architecture in ifogSim and NS2. Finally, section V concludes the paper.

II. RELATED WORK

It is observed that all the above ongoing educational issues were focused to resolve by using the integration of several technologies and communications solutions. Almost all of the research focused on storage, cost reduction, and power consumption of cloud data-centres and IoT devices. There is no research work available in the Scopus database to address low latency and a low delay between IoT devices and fog/cloud data-centres. Even, none of the researchers is working to improve the security of the educational system. Therefore, a secure framework for the education system is proposed which efficiently achieve all of the above said es- sential requirements. Bonomi et al. [3] proposed a hierarchical based distributed architecture that performs processing at the edge of the network using fog Computing. They presented a novel dimension of IoT which adds to Big Data and Analytics. Byrne et al. [5] combined Internet of Things with analytic in the constructionist 21st-century learning model. Authors use sample data set of some students and applied above-said tech- nologies to collect the result towards the benefits of students for their performance. Shi et al. [23] used fog Computing from the perspective of the healthcare. They discussed major characteristics and services provided by fog Layer. Zhu et al.

[31] proposed a four-tier framework which was concentrated on the factors in the smart learning environment for the smart education of 21 century. They also proposed a radical 3 tier architecture along with its key functions for emphasizes the role of smart computing in smart education. Abolfazli et al.

[1] provided a pervasive penetration of cloud computing with the analysis of the rapidly growing cloud market. Mohamed et al. [20] proposed integrated framework using CoT and fog Computing for smart city application. They also implemented and demonstrated the same using various examples related to the smart city. Koch et al. [14] presented an architecture and algorithm for digital teaching platforms that make a balance between the local cloud resources and federated respectively. They also implemented the architecture of the system and get the result using various practical scenarios. Giordano et al.[11] designed a platform that performed computations by placing the physical entities near the computation resources using adaptive and decentralized algorithms. liu et al. [17] provides the survey on various existing protocols for RFID and pointed

the related problems and technical challenges. Mehmood et al [19] proposed a framework that leverages supercomputing, Internet of Things, deep learning and big data for teaching and learning in a smart society. The evaluation is done with the help of different datasets. Yang et al. [25] proposed an architecture for data streaming by examining the most popular properties of several typical applications. Authors also analyzed the design space of data streaming with the consideration of essential properties where both new design difficulties and the issues that arise from leveraging existing techniques are investigated. Zhang et al. [28] proposed an IoT-based "iLocate" which locates objects at high levels of accuracy with ultra- long distance transmission. Virtual reference tags are used to achieve fine-grained localization accuracy. Their empirical study and real project deployment showed the efficiency of the proposed system with respect to the localization accuracy and the data transmission rate.

Islam et al. [13] developed a system to evaluate the technical skills of the students, the researchers, the engineers, and the faculties of a university by implementing IoT devices across the campus. Peng et al.[22] proposed the economical spectral efficiency (ESE) to reduce the wired/wireless front haul cost of cloud paradigm. They formulate the power consumption in data transmission. to deal with this non-convexity, an algorithm is proposed based on both outer and inner loops. Zhou et al. [30] studied long-term evolution-advanced (LTE-

A) networks based on novel architectures such as cloud radio access network (C-RAN) for the deployment of D2D commu- nications. They proposed an algorithm which provides energy- efficient resource allocation through joint channel selection and power allocation. It also uses a hybrid structure C-RAN. Yin et al.[26] proposed a storage scheme to overcome the storage challenges of cloud named ASSER. For improving the reliability, data is stored in two parts. first is a full copy and the other is a certain amount of erasure-coded segments. ASSER delivers stably efficient I/O performance at much lower storage cost than the other comparatives. Yu et al. [27] reduced the operational cost of cloud data-centres with the help of fog devices. Authors also formulated a fog-assisted operational cost minimization problem and design a parallel and distributed load balancing algorithm with low compu- tational complexity based on proximal Jacobian alternating direction method of multipliers. Finally, extensive simulation results show the effectiveness of the proposed algorithm. Chen et al. [7] recommended a good demand response with electric vehicles (F-DREVs) for the cloud-based energy management service and formulated linear based programming model by using various experimental result performances are evaluated. Fiander et al. [10] proposed a structure of new metrics able to determine performance and energy efficiency of cloud computing communication systems, operations and protocols. The metrics have been examined for the most frequent data centre architectures including 3 tier and various other architectures. He et al. [12] proposed a novel digital machine consolidation framework for obtaining better energy efficiency Improved Under-loaded Decision (IUD) protocol and Minimum Average Usage Difference (MAUD) protocol. Cloudsim has been used for real data simulation in the cloud by using various parameters. Authors also proved that the proposed protocol can reduce the energy consumption of cloud data centres in comparison with existing protocols. Zhang et al. [29] implemented the idea of active learning for industrial IoT big data. They proposed an adaptive dropout deep computation model with crowdsourcing to (1) design a distribution function for setting the dropout rate and (2) employ an outsourcing selection algorithm based on maximum entropy. Their results demonstrate that the proposed model effectively prevented the over-fitting and aggregated the labelled samples for industrial IoT big data feature learning. Liu et al. [16] formulated a two- layer gateway-assisted detection and defence decision problem involving multiple IDSs using an evolutionary game in order to improve the intrusion detection strategy for lowering energy usage and reducing alarm communications.

III. PROPOSED MODEL

The architecture of the proposed framework is depicted in Figure 1. It uses a three-layered architecture. The first layer consists of educational IoT devices those collect the data and submit to the second layer on the basis of the action required. These IoT devices sense the environment and send observed values to the fog layer via gateways for further processing. The second layer has a secure fog manager that works as a router between the first layer and cloud data-centres located at the third layer. The third layer is responsible to process and store the less-time sensitive data as well as processed data coming from secure fog manager. In order to provide the security to educational data, OCB authenticated encryption method is adopted. In addition, a modified DSR protocol is proposed that provide secure and fast communication between layers. All three layers are explained in detail along with the OCB method and proposed modified DSR protocol.

IoT Devices Layer: IoT Devices Layer composed of various sensors and devices used in the educational system. The IoT enabled educational devices are placed in this layer are responsible to collect the data from the various distributed geographical location. All IoT devices distributed across the campus of university/college to collect the data and submit to the fog layer. For the same, various wireless communication mediums can be used to transfer the educational data such as 3G/4G/CDMA/GPRS. Sensor nodes at this layer such as mobile devices, tablets, IoT enabled board, smart pens, attendance tracking systems, security cameras, doorbells and locks are connected with IoT gateways. The educational data is collected and forwarded to the secure fog manager.

Fog Layer: This layer is monitored by the secure fog manager that analyzes and classifies the data on the basis of time sensitivity. The data is categorized by the secure fog manager as real-time sensitive and less-time sensitive data. The fog manager is the core component that manages resources of the fog layer in such a way that Quality of Service (QoS) and resource utilization are optimized. The real-time data is pro- cessed by the fog nodes that are closest to the devices those are generating the data. The second type of data that can tolerate minutes of processing is called less-time sensitive data, sent to the cloud data-centres for processing and further analysis. The resources of fog nodes can be provisioned on-demand from geographically distributed routers and switches etc. The real time-sensitive applications that need immediate processing are processed at the fog layer. This layer is responsible for the preliminary processing to be completed and appropriate decision making. The processing and storage requirements

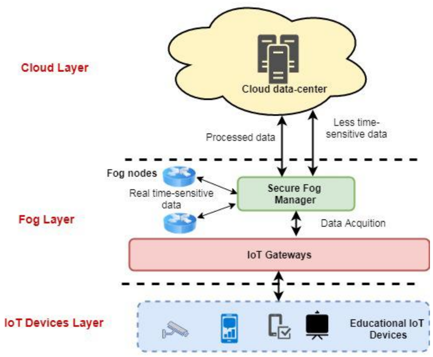

Fig. 1. A Secure IoT based Educational Cloud-Fog Architecture

of the real-time applications are fulfilled by aggregating the computing capabilities of network elements residing at the fog layer. The processed data or results are stored in the repository of the cloud data-centres. On the other hand, the less-time sensitive data categorized by the layer is directly sent to the cloud servers.

Cloud Layer: This layer consists of cloud servers and data-centres those provide processing and storage to the applications computing at cloud layer. The less-time sensitive data and processed data coming from the fog layer is processed and stored respectively. The processed data put less overhead on the cloud servers and data-centres whereas the less-time sensitive data is fully handled by the cloud servers and data-centres.

A. Security aspect of the proposed framework

The security of the proposed framework is provided in two folds. (1) the data transfer between layers must be secure and faster along with minimum energy consumption of devices located at the corresponding layer and (2) security of processed data at both the fog layer and cloud layer. For secure and fast data transfer between layer the secure DSR protocol is proposed with modifications whereas OCB method is used to provide data privacy and authenticity at both layers.

Proposed modified DSR The proposed modified DSR improves the efficiency of the network. It has two compo- nents that cooperate to permit the revelation and maintenance of source nodes. The root discovery and route maintenance operations are monitored by modified DSR. It is intended to permit uni-directional connections and asymmetric routes with minimum efforts. The proposed modified DSR allows secure data transfer with minimum time delay and provides optimization in energy consumption. It also improves the efficiency of each layer. The modified DSR is implemented at both source and destination node. Following are the steps performed at the source node.

Step 1: Destination nodes are sent route reply packets to the source node which are accepted by the source node.
Step 2: After getting the first route reply, the source node sends data packets.
Step 3: Other route replies are received by the source node. And hop count are compared. If [hop count < original path]
Select new path else
keep it in its route cache.
Following steps are performed at the destination node.

Step 1: Based on the node address, all Route Request packets are accepted.
Step 2: Request are valued by checking the sequence number.
Step 3: New request is stored in a table and initiate route reply.
Step 4: Old request, the path is evaluated.
Step 5: If the path is unique, check whether a number of hops are not exactly or equivalent to the hops in the table.
Step 6: If path hop count is more noteworthy than the access path, drop the packet else start route reply and insert it into route cache.

OCB The OCB has a variety of desirable security properties as compared to other existing standards. It uses a parallel mode for block-cipher which simultaneously provides privacy and authenticity. Following algorithms are used for encryption and decryption respectively.

Encryption

Divide M_{ENCP} into $M_{ENCP}[1]$ $M_{ENCP}[2]$ ... $M_{ENCP}[MAX]$
$L < -EK(0n)$
$R < -EK(N + L)$
for $i < -1$ to MAX
do $B[i] = L + R$
for $i < -1$ to $MAX - 1$
do $M_{DECP}[i] < -EK(M_{ENCP}[i]) + B[i] + B[i]$
$X[MAX] = \text{lgt}(M_{ENCP}[MAX]) + L + B[MAX]$
$Y[MAX] = EK(X[MAX])$
$M_{DECP} = M_{DECP}[1]M_{DECP}[2]....M_{DECP}[MAX]$
$checksum = M_{ENCP}[1] + M_{ENCP}[2].. + M_{ENCP}[MAX - 1] + M_{DECP}[MAX]0 * +A[MAX]$
$T = EK(checksum + B[MAX])$
$ReturnM_{DECP} = M_{DECP}||T$

Decryption

Divide M_{ENCP} into $M_{ENCP}[1]$
$M_{ENCP}[2]...M_{ENCP}$ [MAX]T
$L < -E_K(0^n)$
R¡-$E_K(N + L)$
for i¡-1 to MAX
do B[i]=L+R
for i¡- 1 to MAX-1
$M_{ENCP}[i] = E_K(M_{DECP}[i] + B[i] + B[i])$
$X[MAX] = lgt(M_{DECP}[MAX]) + L + B[MAX]$
$Y[MAX] = E_K(X[MAX])$
$M_{ENCP} = M_{ENCP}[1]M_{ENCP}[2]....M_{ENCP}[MAX]$
$checksum = M_{ENCP}P[1]+M_{ENCP}[2]..+M_{ENCP}[MAX - 1] + M_{DECP}[MAX]0 * +A[MAX]$
$T = EK(checksum + B[MAX])$
$ReturnM_{DECP}$

The message from the source node denoted by M_{ENCP} requires encryption. The encryption key is sym $M_{ENCP}[1] = M_{ENCP}[2] = ...M_{ENCP}[MAX\ 1] = n$.

Here, the value of n is also needs encryption which is selected either by the source or destination and it is non-repeating in nature. On the other hand, the decrypted this message is shown as $M_{DECP} = M_{DECP}[1]M_{DECP}[2]M_{DECP}[3]...M_{DECP}[MAX]$ in the form of cipher text. The checksum is given as $M_{ENCP}[1] + M_{ENCP}[2] + ...M_{ENCP}[MAX\ 1] + M_{DECP}[MAX]0 + A[MAX]$ with offset $B[1] = L + R$.

E_K is applied to the 0^n, which is a fixed string to define the string L.

I. PERFORMANCE EVALUATION Constructing a real IoT environment as a test bed for

evaluating the proposed three layer architecture for educational IoT devices is very costly and doesnt provide a controllable en- vironment for conducting repeatable experiments. To overcome this limitation, we simulate it on an open-source simulator called ifogSim. The ifogSim enables the modeling and sim- ulation of fog-computing environment. It easily simulates the educational IoT devices for computing latency of educational devices, delay between layers and energy consumption of each cloud data-centers.

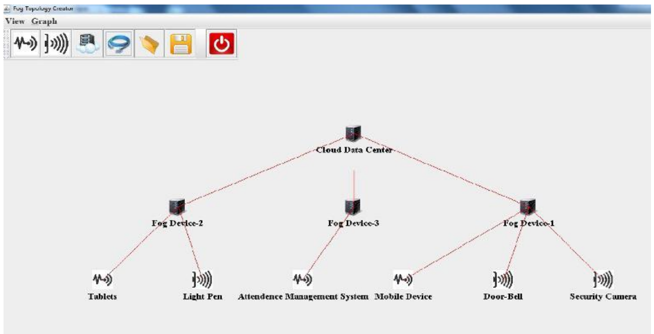

Fig. 2. Topology Simulation for SIECFA

For simulating the environment we design a three level structure as shown in Figure 2. At level 0 cloud servers/ data-centres are placed and in the next level 1, fog devices are places as the gateway, and at the last level, two educational devices are placed. The latency configuration between various components of our proposed framework is considered as listed in Table

I. To obtain correctness of the result during the experiments, various topologies are used with different placement strategies. The configuration of each physical entity such as cloud data- centres, gateways etc. are considered as listed in Table II. The processing capability of each device is expressed in millions of instructions per second (MIPS) whereas bandwidth is measured in the form of Up-link and Down-link. The experiment is

*

performed in a repeatable manner to collect the result. Energy consumption of cloud data-centres is calculated for various strategies. Further, the delay corresponds to each layer is computed to find the total delay in our framework. The latency of all individual devices is also calculated in both situations i.e. when all devices directly interact with cloud and with the presence of fog layer.

A. Complexity Measures

In order to compute the latency for all the packets following metrics are being used:

$$\text{Total latency} = \sum_{K=1}^{N} [\text{Received time(K)} - \text{Sent time(k)}] \quad (1)$$

Here, N is the total number of successfully received packets. Where as the average latency is computed as:

$$\text{Average Latency} = \frac{\text{Total Latency}}{\text{Total Packets Received}} \quad (2)$$

Further, the energy consumption of the proposed framework in the heterogeneous computing environment, the energy con- sumed by each layer is computed. At the IoT device layer and Fog layer, all edge devices are taken into account respectively. The energy consumption by the proposed framework is shown in the following equation:

$$\Delta E = E_{IoTdevicelayer} + E_{Foglayer} \quad (3)$$

- $E_{IoTdevicelayer} = \Sigma(E_{IoTdevicelayer})$ is the energy consumed by all IoT devices in the IoT device layer.
- $E_{Foglayer} = \Sigma(E_{fogdevices})$ is the energy consumed by the fog devices in the Fog Layer.

The computations performed only on cloud increases the en- ergy consumption. On the other hand, our proposed framework performs most of the computations at the fog layer that leads to less overhead on the cloud and improves QoS.

For evaluation of the security aspect of the proposed frame- work, the standard DSR [21] and modified DSR were studied for compression in NS-2 simulation environment. Figure 3 shows a simulation of modified DSR in NS-2. The NS-2 was chosen because it is a descriptive simulator, which has been widely utilized and tested, and it is a simulator that inserts in deep services, also supporting the measurement of energy consumption and application delays. The total 25 number of nodes were fixed those move inside the simulation part of 1000 m-2000 m. The nodes move with a maximal speed of 25 m/s and in line with the random way-point flexibility model. In this model, a node randomly selects an area in the ruse area and a velocity for the next move, which is uniformly allocated between 0 and the maximal velocity. Subsequently, the node

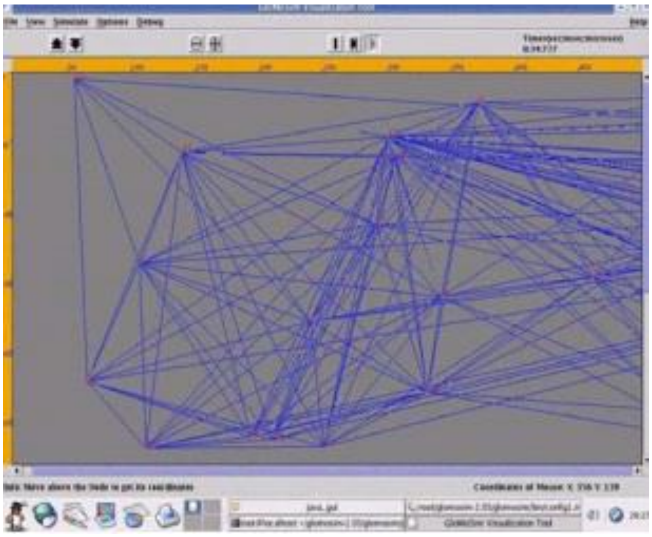

Fig. 3. Modified DSR Simulation

V. RESULTS

The simulation results are compared and analyzed. Figure 5 shows the energy consumption of cloud data-centres in both conditions i.e. with and without fog layer. It clearly shows when the fog layer not in use, the energy consumption of cloud data-centres are very high. Whereas by using fog layer in the proposed framework, the total energy consumption of cloud data-centres became low. The delay of the proposed framework is measured under three different conditions. Firstly, it is calculated between Educational devices and fog devices named as fog layer delay. It is noted here that all computations for both categories of educational data are done at fog devices only. Secondly, the delay is calculated between fog devices and cloud data-centres named as cloud delay. Finally, the total delay is calculated for the proposed framework named as SIECFA delay.

Figure 6 clearly shows the comparison where the SIECFA delay is found as the lowest among both fog layer delay and cloud delay. The other evaluation is performed by all educational IoT devices. Figure 7 shows the latency of each device which clearly shows the latency is reduced with the presence of fog layer.

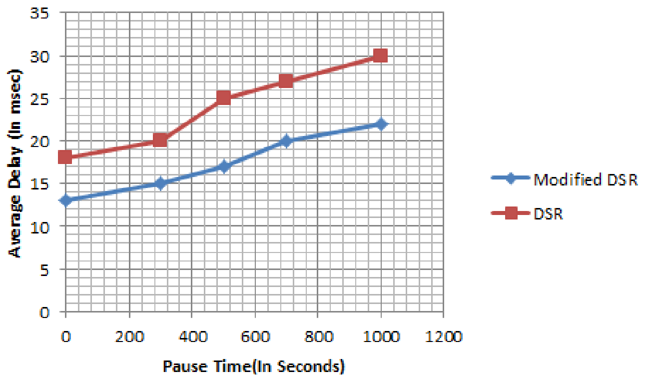

Fig. 4. Comparison of Modified DSR with DSR

TABLE I. LATENCY BETWEEN VARIOUS COMPONENTS.

Source	Destination	Latency (millisec-onds)
Gateway	cloud	100
Mobile devices and tablets	cloud	80
IoT enabled board	Gateway	6
Attendance tracking systems	Gateway	4
Security Cameras	Gateway	8
Doorbell & Locks	Gateway	3

e

VI. CONCLUSION

The the proposed framework architecture facilitates a secure IoT based educational cloud fog architecture. It makes a higher education system, more efficient to achieve better future results. The design of the proposed framework is presented with three layers where the real time monitoring of students data is collected through educational IoT devices. The fog layer efficiently categorize the data into real-time sensitive to be process at fog layer and less-time sensitive data to be process at cloud layer. In addition, OCB method is used to provide security to the processed educational data and modified DSR is proposed that keep secure interaction between fog and cloud layers.

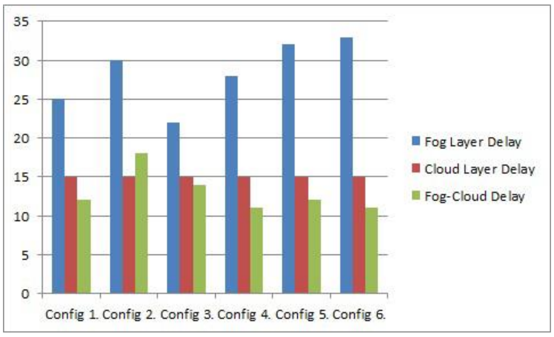

Fig. 6. Computation Delay in fog/cloud system

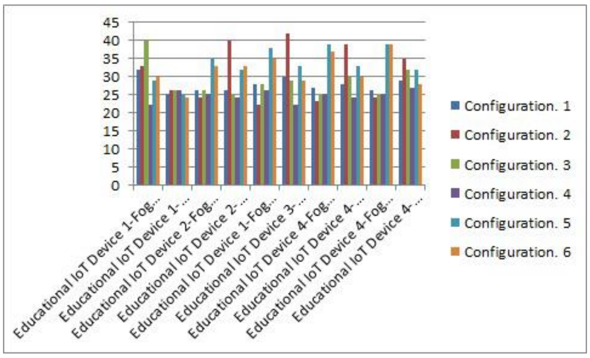

Fig. 7. Latency of various Educational IoT Devices

TABLE II. CONFIGURATION OF IOT DEVICES

Physical entity	Processing Capability (MIPS)	RAM (MB)	Uplink Bandwidth	Downlink Bandwidth	Level
cloud	44000	4000	100	10000	0
Gateway	2000	4000	10000	10000	1
Mobile Devices and Tablets	500	2000	10000	2500	1
IoT enabled board	100	1000	10000	10000	2
Attendance tracking systems	100	1000	10000	10000	2
Secuiry Cameras	100	2000	10000	10000	2
Doorbells & Locks	100	500	10000	10000	2

References

[1] Saeid Abolfazli, Zohreh Sanaei, Ali Tabassi, Steven Rosen, Abdullah Gani, and Samee U Khan. Cloud adop- tion in malaysia: Trends, opportunities, and challenges. *IEEE Cloud Computing*, 2(1):60–68, 2015.

[2] Ayhan Bilsel and O Oral. Role of education, science and technology in developing countries. In Frontiers in Edu- cation Conference, 1995. Proceedings., 1995, volume 2, pages 4c4–11. IEEE, 1995.

[3] Flavio Bonomi, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. Fog computing: A platform for internet of things and analytics. In Big Data and Internet of Things: A Roadmap for Smart Environments, pages 169–186. Springer, 2014.

[4] Christopher Brewster, Ioanna Roussaki, Nikos Kalatzis, Kevin Doolin, and Keith Ellis. Iot in agriculture: Design- ing a europe-wide large-scale pilot. IEEE Communica- tions Magazine, 55(9):26–33, 2017.

[5] Jake Rowan Byrne, Katriona OSullivan, and Kevin Sulli- van. An iot and wearable technology hackathon for pro- moting careers in computer science. IEEE Transactions on Education, 60(1):50–58, 2017.

[6] Carl K Chang, Sorel Reisman, and Edmundo Tovar. Advances in learning technologies. Computer, 50(5):14– 17, 2017.

[7] Yu-Wen Chen and J Morris Chang. Fair demand response with electric vehicles for the cloud based energy manage- ment service. IEEE Transactions on Smart Grid, 2016.

[8] Ruilong Deng, Rongxing Lu, Chengzhe Lai, Tom H Luan, and Hao Liang. Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption. IEEE Internet of Things Journal, 3(6):1171–1181, 2016.

[9] Pedro Miguel Salgueiro dos Santos. Wireless protocols and channel estimation for data gathering with mobile nodes. 2017.

[10] Claudio Fiandrino, Dzmitry Kliazovich, Pascal Bouvry, and Albert Y Zomaya. Performance and energy efficiency metrics for communication systems of cloud computing data centers. IEEE Transactions on Cloud Computing, 5(4):738–750, 2017.

[11] Andrea Giordano, Giandomenico Spezzano, and Andrea Vinci. Smart agents and fog computing for smart city ap- plications. In International Conference on Smart Cities, pages 137–146. Springer, 2016.

[12] Kejing He, Zhibo Li, Dongyan Deng, and Yanhua Chen. Energy-efficient framework for virtual machine consol- idation in cloud data centers. China Communications, 14(10):192–201, 2017.

[13] Tarikul Islam, Subhas Chandra Mukhopadhyay, and Na- gender Kumar Suryadevara. Smart sensors and internet of things: A postgraduate paper. IEEE Sensors Journal, 17(3):577–584, 2017.

[14] Fernando Luiz Koch, Marcos Dias de Assuncao, CH Car- donha, Marco Aure´lio Stelmar Netto, and Tiago T Primo. An architecture and algorithm for context-aware resource allocation for digital teaching platforms. IBM Journal of Research and Development, 59(6):1–1, 2015.

[15] Kaoru Kurosawa. Power of a public random permutation and its application to authenticated encryption. IEEE Transactions on Information Theory, 56(10):5366–5374,2018.

[16] Jianhua Liu, Jiadi Yu, and Shigen Shen. Energy-efficient two-layer cooperative defense scheme to secure sensor- clouds. IEEE Transactions on Information Forensics and Security, 13(2):408–420, 2018.

[17] Xiulong Liu, Xin Xie, Kun Wang, Heng Qi, Jiannong Cao, Song Guo, and Keqiu Li. Pinpointing anomaly rfid tags: Situation and opportunities. IEEE Network, 2017.

[18] Yang Liu, Jonathan E Fieldsend, and Geyong Min. A framework of fog computing: Architecture, challenges and optimization. IEEE Access, 2017.

[19] Rashid Mehmood, Furqan Alam, Nasser N Albogami, Iyad Katib, Aiiad Albeshri, and Saleh M Altowaijri. Utilearn: A personalised ubiquitous teaching and learning system for smart societies. IEEE Access, 5:2615–2635, 2017.

[20] Nader Mohamed, Jameela Al-Jaroodi, Imad Jawhar, Sanja Lazarova-Molnar, and Sara Mahmoud. Smartci- tyware: A service-oriented middleware for cloud and fog enabled smart city services. Ieee Access, 5:17576–17588, 2017.

[21] Carlos Montenegro, Mario Murillo, Freddy Gallegos, and Jose Albuja. Dsr approach to assessment and reduction of information security risk in telco. IEEE Latin America Transactions, 14(5):2402–2410, 2016.

[22] Mugen Peng, Yayun Wang, Tian Dang, and Zhipeng Yan. Cost-efficient resource allocation in

cloud radio ac- cess networks with heterogeneous fronthaul expenditures. IEEE Transactions on Wireless Communications, 2017.

[23] Yingjuan Shi, Gejian Ding, Hui Wang, H Eduardo Ro- man, and Si Lu. The fog computing service for health- care. In Future Information and Communication Tech- nologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium on, pages 1–5. IEEE, 2015.

[24] Taiyang Wu, Fan Wu, Jean-Michel Redoute´, and Mehmet Rasit Yuce. An autonomous wireless body area network implementation towards iot connected healthcare applications. IEEE Access, 5:11413–11422, 2017.

[25] Shusen Yang. Iot stream processing and analytics in the fog. arXiv preprint arXiv:1705.05988, 2017.

[26] Jianwei Yin, Yan Tang, Shuiguang Deng, Ying Li, Wei Lo, Kexiong Dong, Albert Zomaya, and Calton Pu. Asser: An efficient, reliable, and cost-effective storage scheme for object-based cloud storage systems. IEEE Transactions on Computers, 2017.

[27] Liang Yu, Tao Jiang, and Yulong Zou. Fog-assisted operational cost reduction for cloud data centers. IEEE Access, 5:13578–13586, 2017.

[28] Daqiang Zhang, Laurence Tianruo Yang, Min Chen, Shengjie Zhao, Minyi Guo, and Yin Zhang. Real-time

[29] locating systems using active rfid for internet of things.IEEE Systems Journal, 10(3):1226–1235, 2016.

[30] Qingchen Zhang, Laurence Tianruo Yang, Zhikui Chen, Peng Li, and Fanyu Bu. An adaptive droupout deep com- putation model for industrial iot big data learning with crowdsourcing to cloud computing. IEEE Transactions on Industrial Informatics, 2018.

[31] Zhenyu Zhou, Mianxiong Dong, Kaoru Ota, Guojun Wang, and Laurence T Yang. Energy-efficient resource allocation for d2d communications underlaying cloud- ran-based lte-a networks. IEEE Internet of Things Jour- nal, 3(3):428–438, 2016.

[32] Zhi-Ting Zhu, Ming-Hua Yu, and Peter Riezebos. A research framework of smart education. Smart Learning Environments, 3(1):4, 2016.