Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(7):132-142

Research Article ISSN: 2394 - 658X

Enhancing Cloud Security Governance with AI and Data Analytics

Sai Sandeep Ogety

Independent Researcher
Raleigh, United States, ogetysaisandeep04@gmail.com

ABSTRACT

The group of real-world physical devices like sensors, machines, vehicles and various "things" connected to Internet is called as Internet of things (IoT). The major challenge in IoT is that it is fully dependent on the cloud for all kinds of computation, which leads to high latency in the IoT devices. To overcome this latency issue, the Serverless edge computing and AI approaches were introduced newline. Serverless edge computing allows moving the data goverence and managing closer to the Serverless edge of the device. ICT's three pillars namely computing, network and storage faces some challenges in terms of goverence and structuring the data while using formal Cloud computing methods. To propose a framework on IoT devices data by combining two things which is mainly focused on IoT data goverence and data security goverence goverence. To design modified auto-encoder algorithms (AI) for goverence of data in Serverless edge computing architecture. To investigate the present scenario of the data accessing techniques, then to design an effective auto-encoder model to process the huge amount of raw data generated from IoT devices time-to- time (Transforming data to Serverless edge) in the Serverless edge Computing. To consider different types of attacks on IoT data, to investigate the different policies of security and to design a model for Access Control for IoT data by considering the above important processes which can solve the current problems in IoT data access and security. In the performance analysis, Latency minimization, Network Management, Cost Optimization, Data Management, Energy Management, and Resource Management are analysed at the service level and Serverless edge computing based IoT security challenges and self-protection system for IoT specifically in detection, prediction and response mechanisms discussed.

Keywords: Serverless edge computing, Access policies, AI, Data goverence.

INTRODUCTION

In recent years, billions of smart devices such as Mobile Phones, Sensors etc. are connected to the internet in the form of Internet of Things (IoT) which are increasing in a very high rate. IoT combines with other Internet applications involving People, Services, Media and Business to support the development of Serverless edge based economy and digital society. Faster development of IoT devices and sensors make life easier and makes everything accessible from where we are. IoT is a method, which connects humans and peripheral devices to the internet through internet that is, Internet of Everything (IoE). Security is the most critical requirement in IoT environment because IoT is vulnerable to attacks for several reasons, because the volume of IoT devices are increasing day-by- day and these devices are located in both the managed and the unmanaged environment. The growth of IoT is predicted as, by the end of 2020 there will be 16 billion connected devices and an average of 6 devices per person on earth. Nearly 40 Zettabytes of data will be exchanged over the network (Vermesan et al, 2011). By 2023, the number of IoT connected device users will reach 5.3 billion (i.e.) 66 percent of global population. As per Cisco Forecast the data produced from several IoT devices will be in multiples of Zetta Bytes (Wang WY & Wang Y, 2020) and its economic impact of Serverless edge work automation will be in the range of $5 to $7 trillion per year by 2015 (Mujawar, Anjum, et al. 2018). This rapid development in data leads to the challenging of goverence data, storage, computing, security and maintenance. IoT data will be generated as streams in most of the application. Some of the streaming data applications are traffic monitoring, health care predictions, temperature conditions etc. Data produced from IoT connected devices are large in volume, continuously produced over the time period and suddenly rises to very high speed in network and reaches the peak. So, IoT data can also be called as Real Time Big Data (Rathore et al 2015). This exponential growth of IoT provides a large set of opportunities to users and manufacturers through new business models, new revenue

generation, increasing operational efficiency. It will enable a wide applicability in many application sectors such as healthcare, inventory, environmental monitoring to mention a few.

Internet of Things shares the existing networking infrastructures along with minor modifications. The IoT allows multiple off the shelf products to connect with its network and accept almost all kind of communication protocols, i.e., RF, Bluetooth, Zig Bee, and IEEE 802.11. IoT data goverence consists of three different levels (Bhandari et al, 2017),

1. Data acquisition
2. Data Aggregation
3. Data Analysis

Data acquisition is the bottom-most layer in the hierarchy. This level consists of different sensors, which are deployed in the widespread area viz automotive utilities, health care, industrial control, power grid, climate observation, and oil mining. Sensor modules are used in this environment and role of these sensors are vital because the entry process is based on these sensor values only.

The data acquired by the sensors are aggregated at this stage. The values from the multiple sensors are merged, and the accumulated data will be transmitted to the centralized goverence using any one of the wireless protocols.

This data analysis is the top layer in the reference architecture, which is a data-centric application interface to help the user by analyzing the aggregated data. Generally, data analytics is application specific. Few of them are Cloud analytics tools like Cloud storage, and web servers, Bigdata analytics tools such as Weka and Hadoop and Control systems like SCADA will analyze the data.

IoT impact on business fields will be more in the coming years as per the survey from McKinsey's report. The economic impact of IoT based services will boom the growth of many sectors into a new level. The annual economic effect of IoT will be between $2.7 and $6.2 trillion in 2025. The following fig.1 shows the impact of IoT on various sectors in 2025. Since AI and AI may be appropriate for parts of many applications, this indeed will lead to increase in demand of AI and AI products in huge numbers. These approaches directly and indirectly have a strong impact on growth of industries on economic things.

The other reasons to move on to Serverless edge computing is as follows:

- Centralized cloud computing cannot makeup with the explosive growth of data on Serverless edge devices. (D. Boru et al, 2015)
- Long network delay- sudden increase in the cloud centre due to flow of massive data from Serverless edge device leads to network transmission bandwidth delay (Q. Fan, N. Ansari,2018).

Serverless edge computing based IoT protocols do not take into consideration the Serverless edge computing as IoT was conceived with Cloud as a source for performing analytics. IoT involves heterogeneous type of data which can be health, agriculture, energy etc., not a single standard routing mechanism has been developed so far for existing IoT. Handling such heterogeneous data from different sensors or end devices require minimal level of analytics for predicting the data pattern and autonomously coordinating among the Serverless edge computing routers for fast data goverence and exchange among the objects. Further the data Serverless edge computing captures the IoT data, data analysis are playing a vital role in areas like Smart Factories, Smart Cities, Business Grid applications, Smart Health Care etc. Un- Doubtfully cloud architecture is a solution to deal with huge amount of data, where the data can be processed, stored, retrieved and referred for further instances. Even then it has some shortfalls in goverence the live data as a stream. Generally the data comes from IoT devices will be behaving like streams and it will be having following characteristics (i) it will be continuously produced with unlimited flows (ii) data characteristics and behaviours will not be constant resulting in non-identical and changing behaviour over period of time. Over investigating these characteristics IoT data characteristics can be referred as real-time big data, the IoT data goverence Serverless edge computing architecture shown in figure 1.

RELATED WORK

Zhao Zhuoran et al (2018) work focuses on surveying the relationship between IoT edge server and AI, as well as applications of AI models in edge Servers and Cloud structures and also work presented in by Alencar Brenno et al (2020). They proposed a new platform called FoT-Stream in IoT which can be used to process and analyze data streams from IoT in real time in Fog. This method uses the Wavelet transform and Concept Drift methods, both of these techniques are used to observe data behaviours and decomposition. This framework was applied in smart buildings and the outcome of this research gives low goverence delay, no need of constant connection of internet, low network delay. If the behaviour of the data changes continuously then the system fails to stick to its policy and have to transmit all data to the cloud which affects the security performance of the framework.

Tuli, Shreshth, et al (2020) concludes that reasonable configuration of Serverless edge computing environment and constant optimization of Convolutional Neural Network and goverence of image and graphic, we can overcome the problems that are caused from network bandwidth, end cloud delay and privacy threats. Serverless edge Intelligence works by combining Artificial Intelligence (AI) and Serverless edge computing technology to deliver intelligent services to Serverless edge devices to improve quality of intelligent services. TAC3 architecture is used to provide a

light-weight Serverless edge Computing Node (ECN) and the design idea of Tile-Architecture is to organize computing, interconnection resources and storage in to tile units which are simple, and reusable connected by a high energy and scalable on-chip network.

The large development in IoTs technologies is used for the creation of huge raw data streams in big data environments. The raw data streams in big data systems improve the calculation complexity and resource usage in cloud enabled data mining systems. The pattern based data sharing ideas are introduced by ur Rehman et al (2015) in big data environments. This method allows local data goverence at nearby data sources and converts raw data streams into Serverless edge patterns. The Serverless edge patterns contain dual utility of local Serverless edge patterns for instant actions and for participatory data sharing in big data environments. A new two stage method is designed by Thirumalai et al (2020) for IoT cloud data stored cisco based single stage encryption but not defined in algorithm analysis.

Kos, Anton, et al. (2015) discuss the Dataflow programming model in the Bigdata goverence, and they also elaborated the model which improves the execution time, power and space. They claim that the data flow model systems perform very well when compared to the control flow systems with speed-up, less power consumption and lesser space requirements than the control flow. Researchers have proposed publish/subscribe broker based multitier architecture to reduce latency in the Serverless edge computing environment. In this method distributed topology are difficult to attached cloud it created unbalanced dataset.

Table 1: Serverless edge computing with AI approaches for IoT data

S. No.	Author	Methods	Remarks	Inference
1	Aydin et al. (2015)	Scalable and distributed architecture for IoT sensor data cloud storage.	Iot sensors Data stored in cloud using distributed architecture and previous direct cloud storage parameters compared.	Reduce the storage time
2	Mulani, Nazneen, et al (2015)	Privacy issues while storing and recovering in sensors data in cloud.	Protocol based IoT data stored in cloud with COBWEB clustering security method.	Security issues high time duration comparatively direct methods.
3	Zhu, Yong, et al et al (2020)	design methodology of Tile-Architecture Cluster Computing Core	Cloud computing for cluster-based architecture implemented also compared existing clustering methods.	power, memory and time savings are compared to existing clustering architecture.
4	Yi et al. (2016)	A distributed IoT topology aware unstructured peer-to-peer file caching infrastructure	Iot sensor data stored using distributed peer-to- peer topology based and compute storage time.	minimum unbalanced dataset.
5	Thirumalai et al (2020)	Two stage security methods implemented for iot sensor data for cloud and compared to RSA and KESS methods.	Basic two stage duel RSA encryption method implemented and existing ESRKGS and ENPKESS are compared.	Key Generation, encryption time, and decryption time more memory is drawbacks.
6	Alencar Brenno et al (2020).	FoT-Stream in IoT analyze data streams from IoT in real time in Fog computing.	FOG computing used receive the data form iot Serverless edge devices. Analysis the data in before and after applying Haar wavelet transforms methods.	Produce better result in cloud.

Ji, Changqing, et al (2012),

- Dataflow programming model in the Big data goverence is proposed
- • Map reduced optimization method used in Big data environment for bioinformatics data.
- • Data Transfer Bottlenecks, Iterative Optimization, Join Query Optimization and Online
- Performance of proposed system produce better result. Storage management privacy and computation analysis are main challenges.

Tuli, Shreshth, et al (2020),

- Health Fog topology and Convolutional Neural Network algorithm used in medical dataset in fog computing environment

- Heart patients data set are stored in cloud and analysis the Ensemble AI and Convolutional Neural Network classification methods data are used.
- Bandwidth, accuracy, time, latency and power consumed are calculated in training, test correct and test incorrect datasets. Main challenges latency configuration.

Fotiou, Nikos, et al (2018),

- Automatic IoT data analysis using big data analytics.
- IoT sensor datas are stored using FIESTA IoT platform.
- Time, privacy, accuracy and energy driver in strategy layer performance are discussed. Noise data and temperature cause the problem in data store in cloud.

Zhao Zhuoran et al (2018),

- Relationship between IoT Serverless edge server and AI Approaches
- AI approaches DNNs/CNNs with Fused Tile Partitioning methods used cloud in image data.
- Deep learning approaches reduce memory without accuracy sacrifice but Computation time consumed more main drawbacks.

Rehman, Muhammad Habib, and Aisha Batool (2015),

- Pattern based data sharing in cloud computing based big data environments
- In image data pattern classification for Serverless edge Discovery approach implemented in bigdata remote environments.
- Proposed approach effectively Handles six v's to reduce data complexity, Serverless edge availability and Complete personal data control. Implementation for Mobile Social Network application difficult.

PROBLEM FORMULATION

Goverence of Streaming data delay: Most of the IoT applications work on real time environment and needs quicker response time for decision making. Since Cloud is connected to many Serverless edge devices and placed somewhere far away from the end devices, it can't react instantly for real time applications. Latency will be high and there will be a delay in response time. Some of the scenarios like traffic monitoring, autonomous driving cars will come under this shortfall (Li et al, 2018).

Network Load: Many devices are trying to connect to the Cloud at a time, which generates large amount of data at the Serverless edge which in turn have high speed transfer of data to cloud infrastructure which becomes bottleneck for Cloud infrastructure (Chen Jiasi and Xukan Ran, 2019).

Bandwidth: The transfer of huge amount of data from Serverless edge device to cloud leads to a sharp increase in network transmission bandwidth load which results in long network delay. Other shortcomings such as privacy, security is there in goverence of IoT data in cloud apart from the mentioned things. Data goverence as its in high need, Serverless edge computing emerged as a platform for data goverence. Serverless edge computing migrates Cloud services such as networking, computing, storage capabilities and resources nearer to the end devices i.e., Serverless edge network (Wang Xiaofei, et al, 2020).

Response technique: the suitable AI approach is need to provide intelligent decision making to activate the suitable response in the IoT environment. The intelligence is distributed on the fog nodes which are closer to the location of end devices, to select appropriate response at a faster rate. It not only selects appropriate response but also the timely response (Tolba Amr, and Zafer Al-Makhadmeh, 2020).

Research Objectives:

DL based Data Access Framework deployment:

• To investigate the present scenario of the data accessing techniques, then to design an auto encoder model to process the huge amount of raw data generated from IoT devices time-to- time (Transforming data to Serverless edge) either in the Cloud or Serverless edge or FOG computing.

• To consider different types of attacks on IoT data, to investigate the different policies of security and to design a model for Access Control for IoT data.

• To propose a framework by considering the above important processes which can solve the current problems in IoT data access and security.

Proposed Methodology:

Algorithm 1: Determine C using iterative algorithm

Input: Arrival and Service Rate Requested

Output: Number of Container

C → Container System

C → Increment C

Latency L → Mul (Time * Container * Service rate + Decrement C)

Probability State P → Summation N varies from 0 to L for Pn;

Algorithm 2: Serverless Edge based Data analytics

Initialize Active Destination AD, Probed Destination PD, Obsolute and backoff time;

```
Impedance Function ( );
        Arg Min (Wj)
Proportional Random ( );
        Random R with Probability 1/Wd;
Scheduling ( );
        Select Random 'd'
If Probability P = P U {d}
Else
   d = Arg Min (P);
On Receive Response ( );
Consider latency value depend on d;
If (Impedance Compared random proportional)
        Calculate the Weighted Destination.
Else
    If (Data belongs to P)
        Calculate Probability 'P'
        If (Latency <= 2 Min (Wj belongs to A)
                Argument (j) where as for all j to argument
                Calculate bd = Min (b) and Latency
        Else
                Calculate bd;
     Else
        Calculate Wd based on latency
                Condition if (Wd > 2) with A and Wj
```

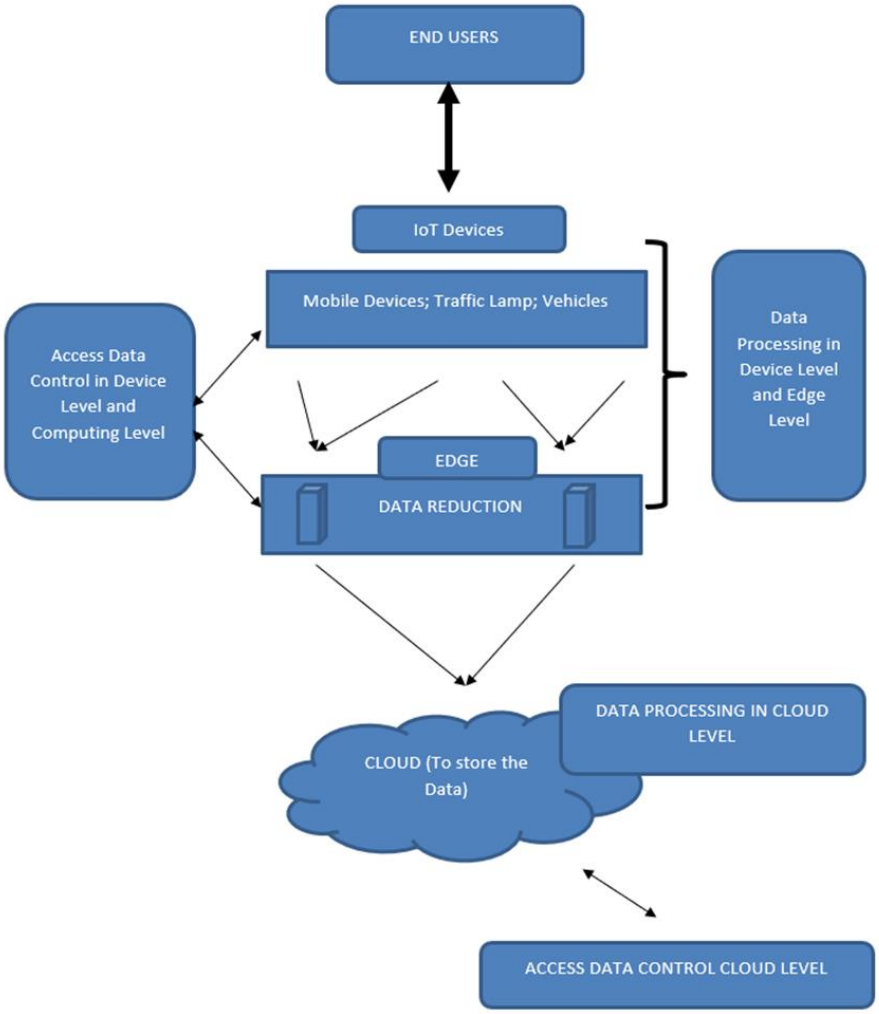

Figure 1: Proposed Edge based Data Analytics Framework

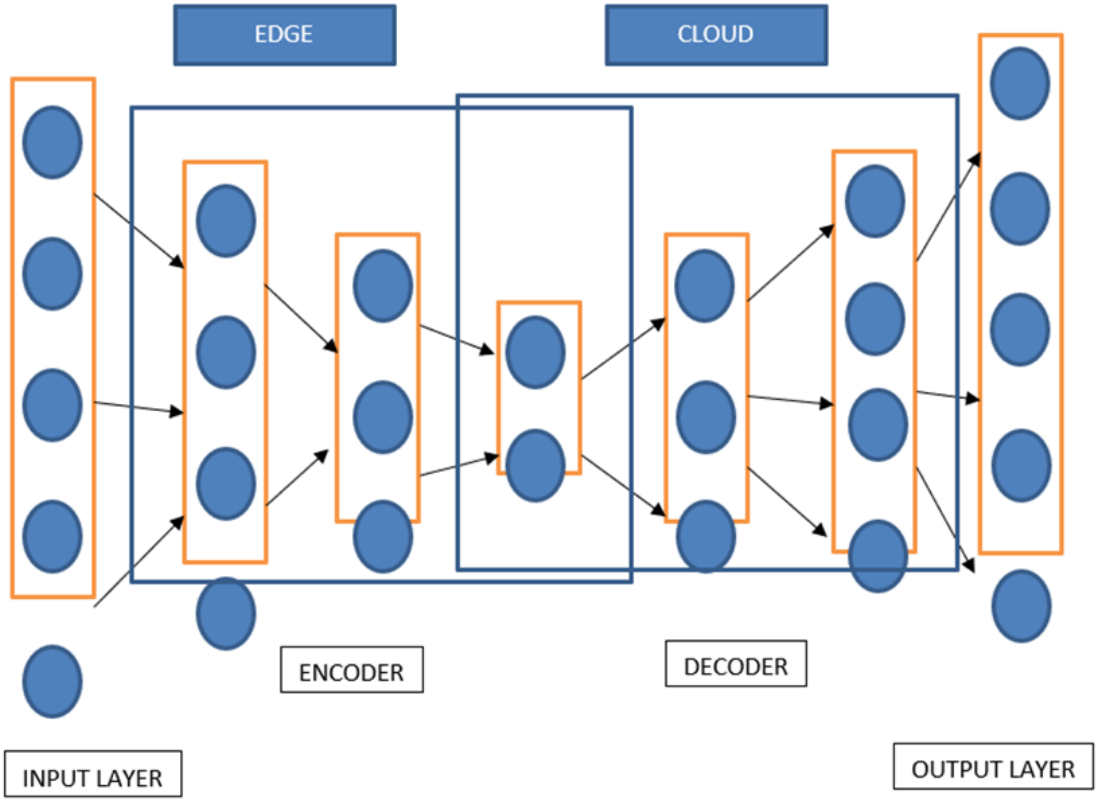

Figure 2: Auto Encoder in Edge Architecture

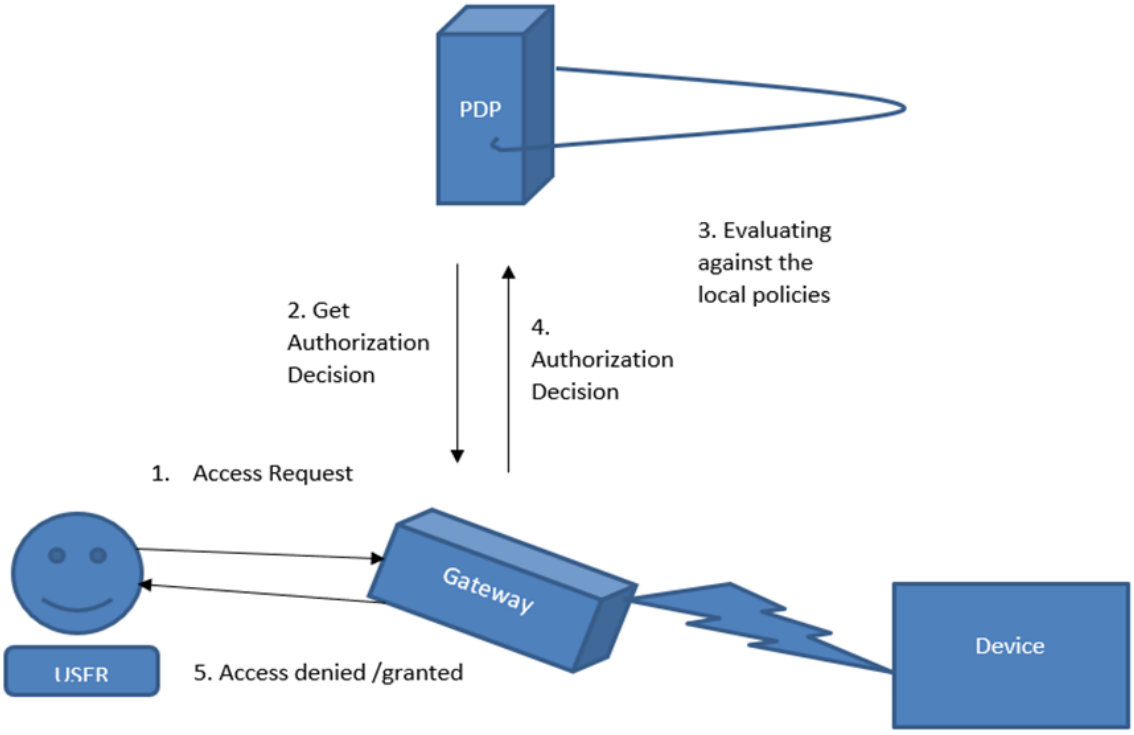

Figure 3: Security Access based on centralized approach

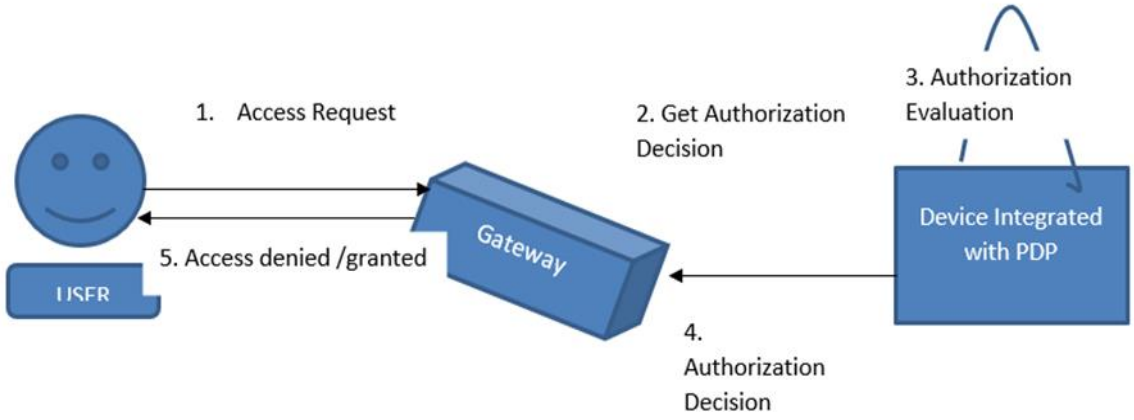

Figure 4: Security Access based on Distributed approach

Algorithm 4: Modified Auto-Encode for Reducing the Data
Input: Data 'd'
Output: Original Data Extraction
Initialize the data 'd'
Data are processed through the hidden layer
Auto encoder to learn to data representation 'R(d)'
AUTO ENCODER:
R(d) → Compress the data
Compress the data based on Random and Random Shuffle Function;
Bit Interleaving Process
Compress data → Abstract Data Representation
Reconstructing the data (Decoder)
Compress the data based on Random and Random Shuffle Function;
Reverse Bit Interleaving Process
Abstract Data Representation → Original Data

PERFORMANCE ANALYSIS

The following performance evaluation criteria were used to assess the effectiveness of the proposed solution to improve the policy decision point. First, the confusion matrix was defined in Table 1 using the decision-making results. DAA defines the quantity of samples that can be accessed correctly, DAR = the number of samples incorrectly denied access, DRA = the quantity of samples incorrectly allowed access samples, and DRR = the number of correctly refused access samples.

Table 1: Confusion matrix of policy decision point PDP results.

	Predicted Results	
Real Results	**Allowed Access**	**Refused Access**
Allowed Access	D_{AA}	D_{AR}
Refused Access	D_{RA}	D_{RR}

Accuracy Metric: used to evaluate the effectiveness of policy decision points in access control strategies in all scenarios. The percentage is calculated by dividing the number of accurate estimates by the total number. The following formula is used to calculate Accuracy (CM) Using the confusion matrix:

$$Accuracy = \frac{D_{AA} + D_{RR}}{D_{AA} + D_{AR} + D_{RA} + D_{RR}}$$

Precision Metric: is computed by dividing the total number of positive samples by the number of positive samples correctly identified (either correct or not). This is determined by the measure of the total correct samples that were allowed to the expected number of samples that were allowed. It was determined by employing the following formula:

$$Precision = \frac{D_{AA}}{D_{AA} + D_{RA}}$$

Recall Metric: measured as the proportion of positive samples accurately categorised as actual relative to the number of allowed accurate samples. The Recall metric examines the model's identification of samples. Recall increases the actual sample size.

$$Recall = \frac{D_{AA}}{D_{AA} + D_{AR}}$$

F1-score Metric: the F1-score is a harmonic average of Precision and Recall, the two most significant components. F1-score is effectively unbalanced data. The harmonic average differs from the arithmetic mean.

$$F1 - score = \frac{Precison * Recall}{Precision + Recall}$$

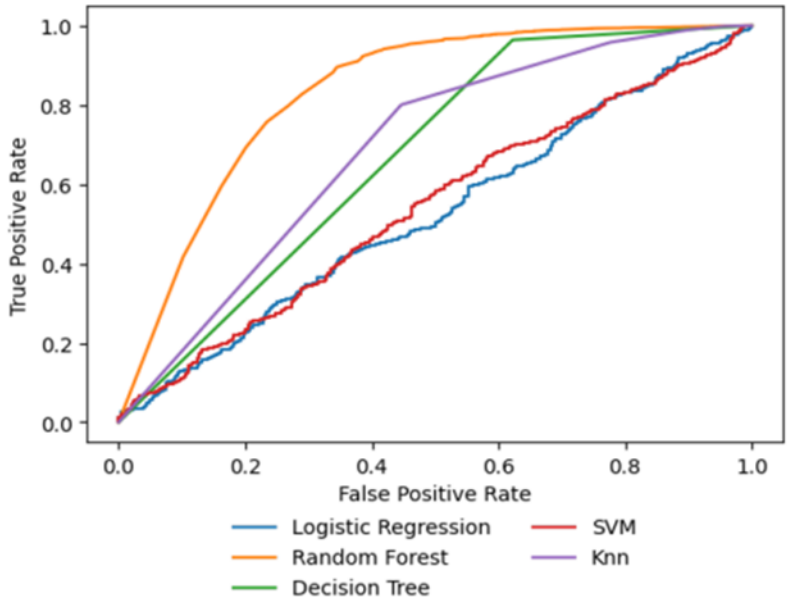

Figure 4: Analyzing ROC curve results before data balancing for all algorithms.

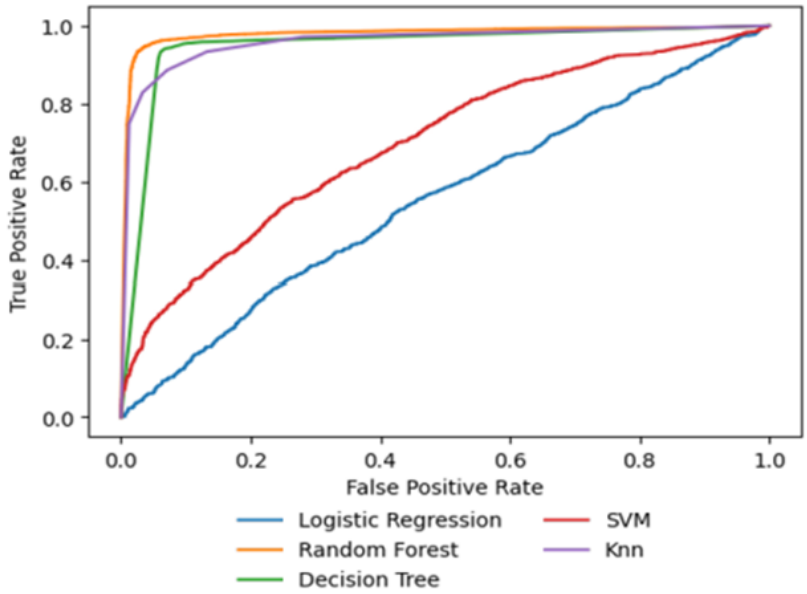

Figure 5: Analyzing ROC curve results after data balancing for all algorithms.

Based on the experimental results illustrated in Figures 4 and 5, it can be concluded that the receiver operating characteristic (ROC) curve is unchanged with the dissemination of the sample group. Consequently, the performance (ROC) of the algorithms was poor prior to the data balancing method.

Table 3: AUC values of different algorithms.

Methods	RF	KNN	DT	LR	SVM
AUC-Unbalanced Dataset	0.83	0.69	0.67	0.52	0.54
AUC-Balanced Dataset	0.98	0.96	0.95	0.55	0.70

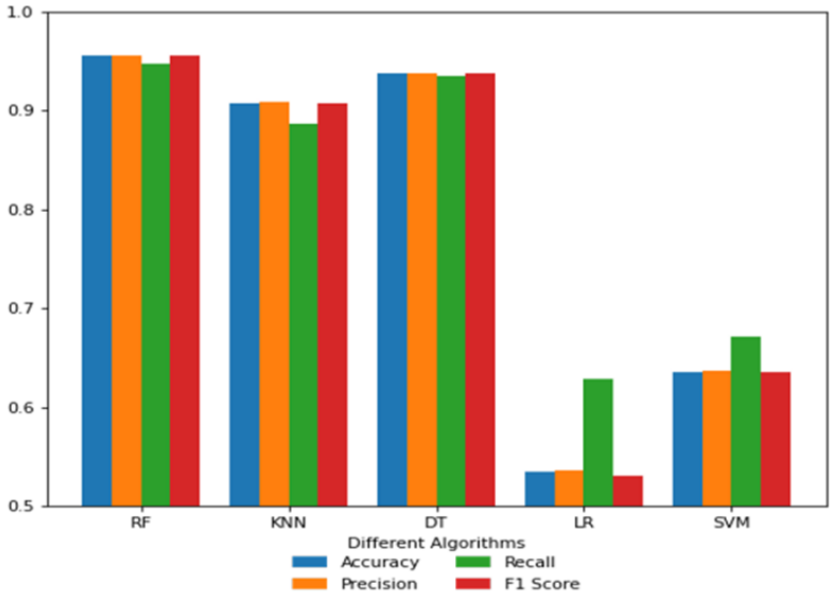

Figure 6: Analyze the performance metrics of various methods after data goverence (balancing method).

As shown in Figure 6, logistic regression (LR) performs the worst, followed by support vector machines (SVM). Consequently, k-nearest neighbours (KNN), decision tree (DT) and random forest (RF) have comparable performance and values.

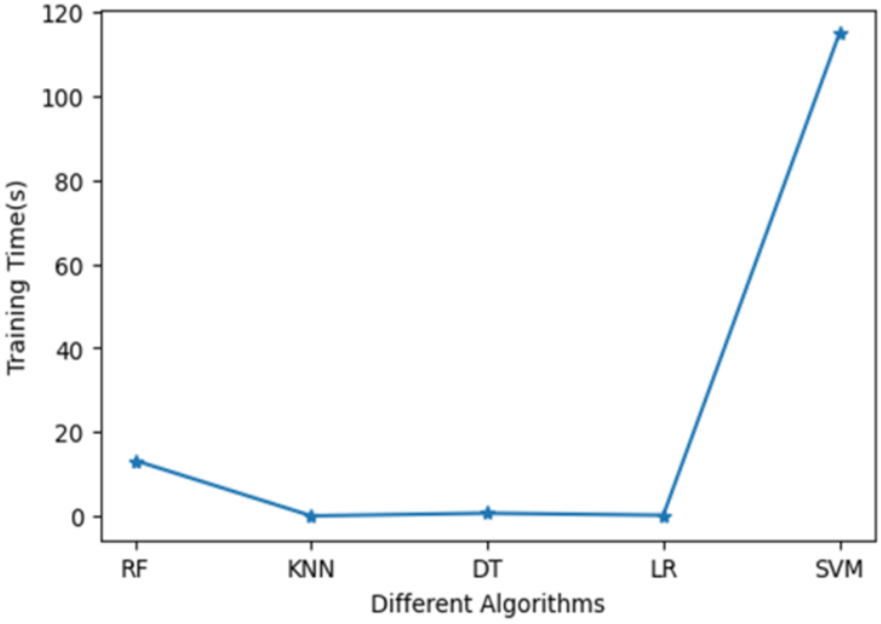

Figure 7: Analyze training times results of different methods after data balancing

Time is a crucial aspect of access control security, as it enables timely and dynamic updates to the system's access control policy, as well as prompt responses to access requests, therefore preventing the access control system from becoming a bottleneck. As a result, as depicted in Figure 7, the training time of the model was analysed along with the update time necessary for a policy decision point (PDP) to approve or deny an access request. The SVM algorithm required more training time than the other techniques, whereas the LR, KNN and DT algorithms required the same amount of time.

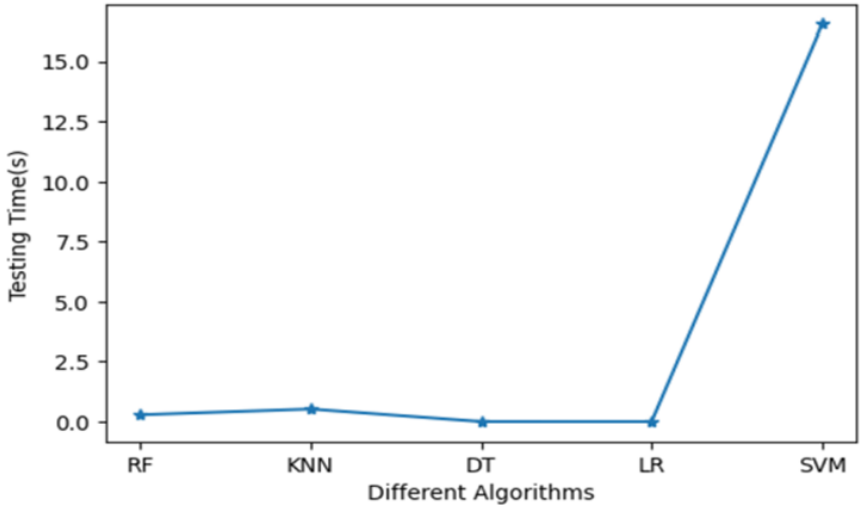

Figure 8: Analyzethe testing times results of different methods after data balancing

Additionally, Figure 8 demonstrated that after applying data balancing techniques, the testing time results of various methods were analyzed, focusing on security access decision-making. The methods considered for analysis included random forest (RF), k-nearest neighbours (KNN), decision tree (DT), logistic regression (LR), and support vector machine (SVM). The analysis aimed to evaluate the performance of these methods in terms of their testing times after data balancing.

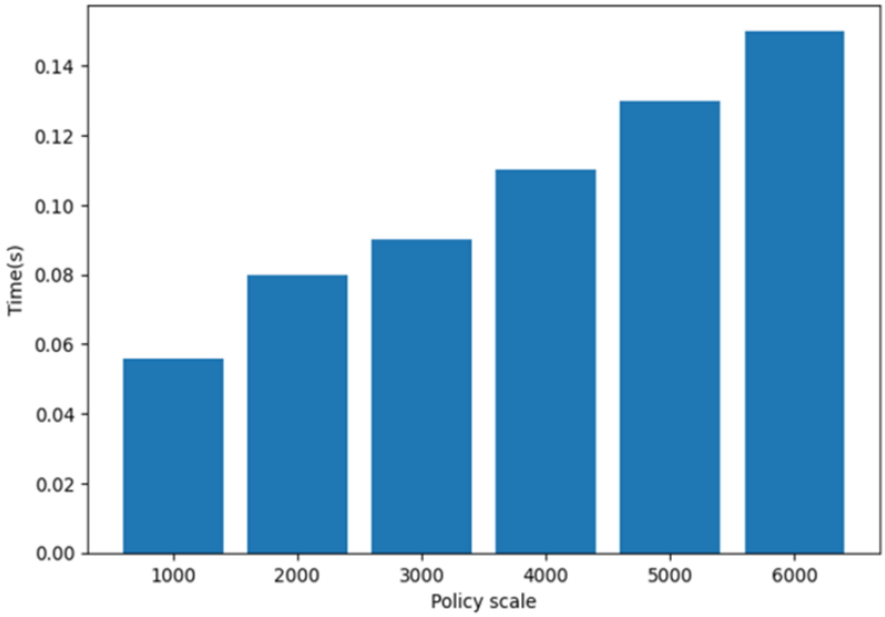

Figure 9: Analyze time under different policy scales

Figure 9 depicts the outcomes of an experiment analysing the flexibility of PDP based on ML in terms of policy size over time. The access control response per second to complex policies was used to evaluate flexibility. In the experiment, random requests for policy sizes ranging from 1000 to 6000 were sent and the time cost was approximately 0.15 s when the policy scale was 6000. It appears that the model responded positively to the size of the policy.

CONCLUSION

To propose a framework on IoT devices data by combining two things which is mainly focused on IoT data goverence and data security goverence goverence. To design modified auto-encoder algorithms (AI) for goverence of data in Serverless edge computing architecture. To investigate the present scenario of the data accessing techniques, then to design an effective auto-encoder model to process the huge amount of raw data generated from IoT devices time-to-time (Transforming data to Serverless edge) in the Serverless edge Computing. To consider different types of attacks on IoT data, to investigate the different policies of security and to design a model for Access Control for IoT data by considering the above important processes which can solve the current problems in IoT data access and security. In the performance analysis, Latency minimization, Network Management, Cost Optimization, Data Management, Energy Management, and Resource Management are analysed at the service level and Serverless edge computing based IoT security challenges and self-protection system for IoT specifically in detection, prediction and response mechanisms discussed.

REFERENCES

[1]. Alencar, Brenno M., Ricardo A. Rios, Cleber Santana, and Cássio Prazeres. "FoT- Stream: A Fog platform for data stream analytics in IoT." Computer Communications (2020).

[2]. Aydin, G., Hallac, I. R., & Karakus, B. (2015). Architecture and implementation of a scalable sensor data storage and analysis system using cloud computing and big data technologies. Journal of Sensors, 2015.

[3]. Bhandari, S., Sharma, S. K., & Wang, X. (2017, December). Latency minimization in wireless IoT using prioritized channel access and data aggregation. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.

[4]. Chen, J., & Ran, X. (2019). AI With edge Computing: A Review. Proceedings of the IEEE, 107(8), 1655-1674.

[5]. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, A. Zomaya, Energy-efficient data replication in cloud computing datacenters, Cluster Comput., 18 (2015), 385–402

[6]. Fotiou, N., Siris, V. A., Mertzianis, A., & Polyzos, G. C. (2018, June). Smart IoT Data Collection. In 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 588-599). IEEE.

[7]. Kos, A., Tomažič, S., Salom, J., Trifunovic, N., Valero, M., & Milutinovic, V. (2015). New benchmarking methodology and programming model for big data goverence. International Journal of Distributed Sensor Networks, 11(8), 271752.

[8]. Moreira, F., Ferreira, M. J., & Cardoso, A. (2017, July). Higher education disruption through IoT and Big Data: A conceptual approach. In International Conference on Learning and Collaboration Technologies (pp. 389-405). Springer, Cham.

[9]. Mujawar, A., Kumar, S., Krishnan, S. S., & Sawant, A. (2018). IoT: Green Data Center Strategies. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(5), 170-174.

[10]. Mulani, N., Pawar, A., Mulay, P., & Dani, A. (2015). Variant of cobweb clustering for privacy preservation in cloud db querying. Procedia Computer Science, 50, 363- 368.

[11]. Q. Fan, N. Ansari, Application Aware Workload Allocation for edge Computing based IoT, IEEE Int. Things J., 5 (2018), 2146–2153.

[12]. Rathore, M. M. U., Paul, A., Ahmad, A., Chen, B. W., Huang, B., & Ji, W. (2015). Real-time big data analytical architecture for remote sensing application. IEEE journal of selected topics in applied earth observations and remote sensing, 8(10), 4610-4621.

[13]. Thirumalai, C., Mohan, S., & Srivastava, G. (2020). An efficient public key secure scheme for cloud and IoT security. Computer Communications, 150, 634-643.

[14]. Tuli, S., Basumatary, N., Gill, S. S., Kahani, M., Arya, R. C., Wander, G. S., & Buyya, R. (2020). HealthFog: An ensemble AI based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Future Generation Computer Systems, 104, 187-200.

[15]. Vermesan, O., Blystad, L. C., Zafalon, R., Moscatelli, A., Kriegel, K., Mock, R., ... & Perlo, P. (2011). Internet of Energy–connecting Energy anywhere anytime. In Advanced microsystems for automotive applications 2011 (pp. 33-48). Springer, Berlin, Heidelberg.

[16]. Wang, W.Y.C., & Wang, Y. (2020). Analytics in the era of big data: the digital transformations and value creation in industrial marketing.

[17]. Yi, G., Park, J. H., & Choi, S. (2016). Energy-efficient distributed topology control algorithm for low-power IoT communication networks. IEEE Access, 4, 9193-9203.

[18]. Zhao, Z., Barijough, K. M., & Gerstlauer, A. (2018). Deepthings: Distributed adaptive AI inference on resource-constrained iot edge clusters. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 37(11), 2348-2359.

[19]. Zhu, Y., Jiang, Z., Mo, X., Zhang, B., Al-Dhelaan, A., & Al-Dhelaan, F. (2020). A study on the design methodology of TAC3 fedge computing [J]. Mathematical Biosciences and Engineering, 17(5), 4406-4421.