Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Improving Access Control Decisions using Deep Learning and Contextual IoT Features

Djamel Hamdadou[1], Djamel Amar Bensaber [2]
LabRI-SBA Laboratory, Ecole Superieure en Informatique, Sidi Bel Abbes, Algeria
[1] *d.hamdadou@esi-sba.dz*
[2] *d.amarbensaber@esi-sba.dz*

ARTICLEINFO

Received: 26 Dec 2024
Revised: 14 Feb 2025
Accepted: 22 Feb 2025

ABSTRACT

Securing IoT environments has become more complex because it requires the combination of several technologies, from physical devices and wireless transmission to mobile and cloud architectures. Traditional access control models that rely solely on credentials or roles are inflexible and ineffective in intelligent and dynamic environments. To address these limitations, we proposed a more advanced access control model that exploits the power of machine learning to solve problems relating to access control decision-making. In particular, we propose Deep Learning context Based Access Control (DLCBAC) byleveraging significant advances in deep learning technology as a potential solution to this problem. The context-aware approache enable fine-grained control over data and resources, tailoring access permissions based on the specific circumstances surrounding the access request.We experiment with a real-world dataset collected from real IoT envirenoment. Our evaluation results suggest that a DLCBAC could recommend granting or denying permission with 99.9% accuracy.

Keywords: IoT security,access control,context aware, IRIL-SHS dataset, Deep Learning Context Based Access Control (DLCBAC).

INTRODUCTION

With the rapid progress of Internet of Things (IoT) technology and the widespread deployment of smart devices, IoT platforms have become deeply integrated into critical sectors such as smart homes, transportation, industrial control systems, healthcare infrastructure and city management.

Access control is a fundamental security layer. It determines which users or devices can access which resources. It also determines the conditions under which they can access those resources.

IoT environments require adaptive security mechanisms that consider user context. Access control in these environments is no longer a matter of evaluating static roles or enforcing hardcoded rules. As device ecosystems become more complex and interconnected, access policies must consider a variety of dynamic contextual factors, such as time of day, user behavior, device status, sensor inputs, inferred intent, and social norms. For example, imagine a child in a smart home wants to watch TV on a school night. Although the system may be configured to restrict entertainment use after 9 p.m, the system may also need to consider if the child has finished their homework and if an emergency situation such as an active fire alarm. These nuanced decisions cannot be rigid rule sets or keyword-based matching cannot reliably handle these nuanced decisions, underscoring the need for more intelligent and flexible semantically aware access control mechanisms.

Although classical models [1] such as discretionary access control (DAC), mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) provide structured mechanisms for permission assignment. However, they are largely static, which often fail to capture the nuanced and dynamic nature of access decisions, where contextual factors such as user location, device type, time of day, and environmental conditions can significantly influence the appropriate level of access, making them poorly suited to the dynamic and heterogeneous nature of IoT environments.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To address these challenges, deep learning (DL) techniques have emerged as effective tools for detecting unauthorized access. Incorporating DL algorithms into access control enables the system to adapt more effectively to changing environments and improve access management.

The project focuses on a deep learning-based model for access control, which aims to improve decision-making processes. The model will be trained and evaluated using real contextual data from the IRIL-SHS dataset, with performance metrics improving authorisation and access management through a contextual-based approach.

This paper is structured as follows: Section 2 reviews related work, Section 3 details the methodology, Section 4 presents the framework design, Section 5 evaluates performance, and Section 6 concludes with future directions.

RELATED WORK

Authorisation involves granting users access rights to an IoT system, such as a physical sensor device. These users may be machines, humans, or services. For instance, data collected by sensors should only be delivered to and accessed by authorised users, authorised objects and service requesters [2]. In other words, an action should only be performed if the requester has the necessary authorisation. The main challenge of authorisation in IoT environments is successfully granting access in an environment where humans and physical sensors (things) must both be authorised to interact with the IoT system [3].

Various access control models have been proposed to address the diverse requirements of IoT environments. In particular, access control models, such as Mandatory Access Control (MAC) [1] ABAC [4] and RBAC [5], have been adapted for this environments. In an attempt to overcome these challenges, the authors in [6] introduce a dynamic authorization system that integrates roles, tasks, and user trust levels to offer scalable and fine-grained access control in cloud settings. Another related method proposed by Habiba et al. [7] involves a dynamic access control framework that incorporates policy conflict resolution and authorization validation to enhance security in cloud computing, but their effectiveness is often limited due to the IoTs dynamic and multi-tenant nature.

To address these limitations, researchers have proposed more advanced access control models that incorporate contextual information. These context-aware approaches enable fine-grained control over data and resources, tailoring access permissions based on the specific circumstances surrounding the access request.

Several recent works have explored strengthening access control by leveraging machine learning, particularly in contexts such as IoT, Cloud, or mission-critical environments.

In one of the earliest works, Chang et al [8] proposed a time-aware access control model based on SVM, but limited to synthetic data. With the emergence of the Internet of Things, Outchakoucht et al [9] introduced an approach combining blockchain with Reinforcement Learning techniques to establish more robust access policies, although not experimentally evaluated. Other authors have focused on inferring policies from access logs. Cappelletti et al [10] applied different methods (DT, RF, SVM, MLP) to dynamically infer ABAC rules, based on real data. Similarly, Khilari et al [11] have designed a trust-based control model for Cloud environments, exploiting access histories and user behaviors.In a more critical context (defense, airport, healthcare), Srivastava et al [12] proposed a Risk-Adaptive Access Control (RAdAC) model based on neural networks to assess the reliability of access requests according to their context.

More recently, Liu et al [13] and Karimi et al [14] have worked on the dynamic adaptation of ABAC policies via learning, particularly in Big Data and IoT. These methods seek to improve the decision process (Policy Decision Point) by taking into account the evolution of contextual data.

Noor et al. [15] uses the IRIL-SHS dataset to extract contextual features such as protocol, device status, and timestamps. A Random Forest classifier is applied to detect anomalous access patterns. Although effective, their work relies solely on classical machine learning and predefined thresholds for detection. Nobi et al [16] have developed a deep neural access control (DLBAC) model based on ResNet, evaluated on synthetic and real datasets. This model stands out for its high capacity to learn complex representations of the access context.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Finaly, to enhance security governance, Mupila et al[17] introduces a cognitive AI-driven framework integrating machine learning (ML) models (Random Forest, SVM) with a dynamic policy adaptation layer.

Our approach builds on this by proposing a contextual access control model based on a multilayer neural network (MLP), evaluated on the IRIL-SHS dataset. By integrating contextual attributes such as user profile, time, location and device status to learn complex relationships between this contextual features and access decisions. Unlike previous work, our approach explores the deep structure of the data to enhance decesion accuracy and improve adaptive access decision in sensitive environments such Iot.

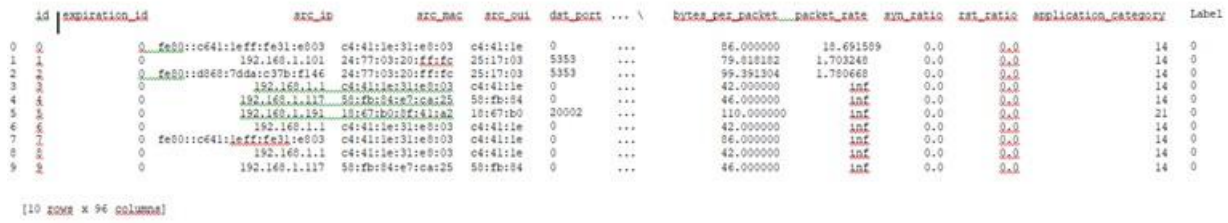
METHODS

In this section, we present the methodology we adopted for designing, training, and evaluating our access control model based on contextual information. Our goal is to develop a system that can automatically permit or deny access requests based on multidimensional contextual data.

Our approach uses a multilayer perceptron (MLP) trained on the IRIL-SHS dataset containing access records annotated with various contextual information, such as user role, location, time, device status, and application category.

Dataset

The IRIL-SHS dataset[15], generated by IoT Research and Innovation Lab (IRIL), offers a realistic benchmark for access scenarios in an intelligent environment. The dataset gathered from the communication of various IoT devices via protocols TCP, DNS, HTTP, TLS, QUIC, MDNS, UDP, and ARP protocols .Each entry represents an access attempt, associated with a set of contextual features and a binary label indicating whether access is authorized (1) or denied (0). The dataset includes detailed labels and metadata such as timestamps, IP addresses, ports, protocols, and application category, stored in PCAP and CSV formats. Figure 1 shows the dataset in CSV format.



	id	expiration_id	src_ip	src_mac	src_oui	dst_port	... \	bytes_per_packet	packet_rate	syn_ratio	rst_ratio	application_category	Label
0	0	0	fe80::c641:1eff:fe31:e803	c4:41:1e:31:e8:03	c4:41:1e	0	...	86.000000	18.691589	0.0	0.0	14	0
1	1	0	192.168.1.101	24:77:03:20:ff:fc	25:17:03	5353	...	79.818182	1.703248	0.0	0.0	14	0
2	2	0	fe80::d868:7dda:c37b:f146	24:77:03:20:ff:fc	25:17:03	5353	...	99.391304	1.780668	0.0	0.0	14	0
3	3	0	192.168.1.1	c4:41:1e:31:e8:03	c4:41:1e	0	...	42.000000	inf	0.0	0.0	14	0
4	4	0	192.168.1.117	58:fb:84:e7:ca:25	58:fb:84	0	...	46.000000	inf	0.0	0.0	14	0
5	5	0	192.168.1.191	10:67:b0:3f:41:a2	10:67:b0	20002	...	110.000000	inf	0.0	0.0	21	0
6	6	0	192.168.1.1	c4:41:1e:31:e8:03	c4:41:1e	0	...	42.000000	inf	0.0	0.0	14	0
7	7	0	fe80::c641:1eff:fe31:e803	c4:41:1e:31:e8:03	c4:41:1e	0	...	86.000000	inf	0.0	0.0	14	0
8	8	0	192.168.1.1	c4:41:1e:31:e8:03	c4:41:1e	0	...	42.000000	inf	0.0	0.0	14	0
9	9	0	192.168.1.117	58:fb:84:e7:ca:25	58:fb:84	0	...	46.000000	inf	0.0	0.0	14	0

[10 rows x 96 columns]

figure1: IRIL-SHS dataset

The data were collected over six days in a medium-sized smart home setup. This dataset consists of 608,500 records of real-time traffic, including both attacks (unauthorized access) and normal events with 96 columns (features). Table 1 shows the list of features category.

Category	features Examples
Network identifiers	src_ip, dst_ip, src_port, dst_port, protocol
Bidirectional flows	bidirectional_packets, bidirectional_bytes
Temporal statistics	duration_ms, mean_piat_ms, min_ps, max_ps
TCP protocols & flags	syn_packets, ack_packets, fin_packets, etc.
Application metadata	application_name, user_agent, content_type
Context	time_of_day, day_of_week, application_category
Label (target)	0 (unauthorized) / 1 (authorized)

Table 1: list of features category.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

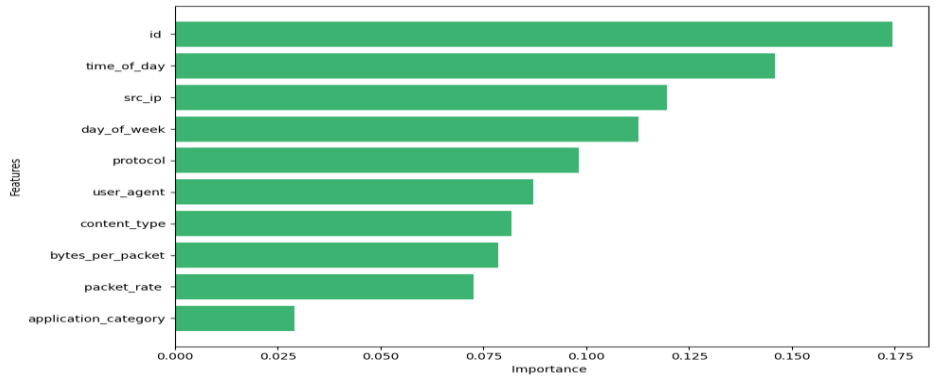
Research Article

Data Preprocessing

The IRIL-SHS dataset comprises 608,500 real-time traffic records. To examine the generalisation capacity of the model and avoid overfitting, all redundant records were eliminated from the dataset to reduce the impact of imbalance. The first steps in the data pre-processing process are converting categorical data into numerical information and removing any anomalies and incorrect data from the dataset. We then encoded the categorical features using an ordinal encoder, thereby increasing the feature count.

Contextual features selection

We selected a set of attributes that gave the best performance. Feature selection speeds up training by reducing the number of features and eliminating undesirable or "noisy" ones. A feature selection method based on ensemble learning, also known as an extremely randomized tree classifier, is used for this model. Table 2 illustrates the 10 contextual features that have an impact on our model.



2	src_ip	0.119591
3	day_of_week	0.112727
4	protocol	0.098203
5	user_agent	0.087174
6	content_type	0.081843
7	bytes_per_packet	0.078566
8	packet_rate	0.072634
9	application_category	0.028960

Table 2: Contextual features importance of IRIL-SHS dataset.

MODEL ARCHITECTURE

The deep learning model used for this approche is built using TensorFlow. We have designed an artificial neural network of the Multilayer Perceptron (MLP) type. It consists of an input layer containing a vector of contextual features, two dense hidden layers of 64 neurons for the first layer and 32 neurons for the second layer wiche using ReLU activation and an output layer with a sigmoid activation function. The model is compiled with binary cross entropy loss and the Adam optimizer. This relatively simple architecture effectively learns to distinguish between authorized and unauthorized access. The Training is performed with split 30% of data for validation.

Given a slight imbalance between classes (Access allowed vs. Access denied), we applied a class weight during training to avoid a bias in favor of the majority class.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

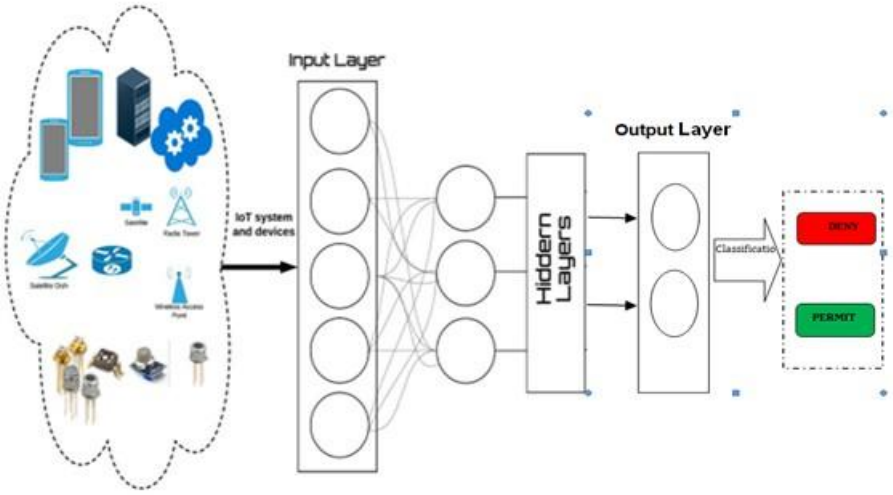


Figure.3: Architecture of our model

5. RESULATS

Based on contextual features, the categorization model predicts whether incoming traffic will be allowed or denied. As the proposed model predicts access rights and determines the correlation among the 10 variables. The chosen attributes showed a high correlation with a value close to or equal to -1 or 1.The model was trained for 10 epochs. The training and validation losses are presented below.

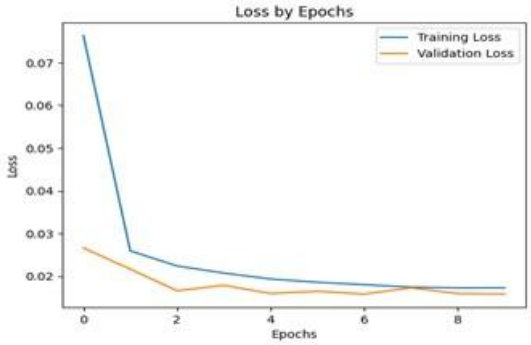


Figure.4: Loss function for DLCBAC

The performance of the model was evaluated using standard metrics: accuracy, recall, F1-score, and confusion matrix. It achieved an accuracy of 99.7%, recall of 99.9%, and F1-score of 99.9%.The classification report for the test set is presented in the table 3.

	precision	recall	f1-score	support
0	0.94	1.00	0.97	63777
1	1.00	0.99	1.00	57923
accuracy			0.99	121700
macro avg	0.98	1.00	0.99	121700
weighted avg	0.99	0.99	0.99	121700

Tabel 3. Classification report for the test set

The model demonstrates very good enough performance with high precision and recall, making accurate decisions in most instances.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The results show that neural networks are well-suited to modeling complex dependencies in contextual data. The proposed architecture generalizes well and reduces false positives. An improvement would be to integrate a dynamic weighting mechanism based on context criticality.

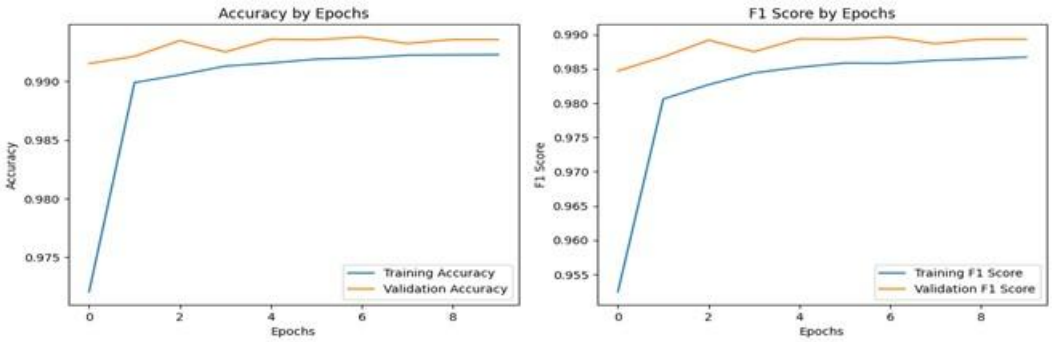


Figure.5: training and validation metrics for deep learning context access control.

CONCLUSION AND FUTURE WORK

In this paper, we propose an Internet of Things (IoT) access control system to improve decision-making using a Multi-Layer Perceptron (MLP) to detect access as deny or permit, leveraging the IRIL-SHS2023 dataset for evaluation. The proposed framework addresses critical security management gaps in IoT environments by offering a robust, scalable, and adaptive solution. The results demonstrate that a neural network applied to contextual data from the IRIL-SHS environment effectively detects unauthorized access. The feasibility of using a context-based AI model for access control as an alternative to traditional models paves the way for future advances in intelligent system security.Future work may include real-time data stream integration and the use of recurrent networks (e.g., LSTM) to improve reactivity in access control decisions.

REFRENCES

[1] Natarajan Meghanathan.(2013). Review of access control models for cloud computing. Computer Science &Information Science 3,1, pp.77–85.
[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi.(2017) .Internet of Things security: A survey,Journal of Network and Computer Applications, vol. 88, pp. 10-28.
[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini.(2015).Security, privacy and trust in Internet of Things: The road ahead, Computer networks, vol. 76, pp. 146-164.
[4] C.D.Nassar Kyriakidou, A.M. Papathanasiou, I. Pittaras, N. Fotiou, Y. Thomas, and G.C. Polyzos.(2024). Attribute-Based Access Control Utilizing Verifiable Credentials for Multi-Tenant IoT Systems.In IEEE 4th.
[5] Lan Zhou, Vijay Varadharajan, and Michael Hitchens.(2013). Achieving secure role-based access control on encrypted data in cloud storage.IEEE transactions on information forensics and security 8, 12, 1947–1960.
[6] Saima Mehraj and M Tariq Banday.(2021). A flexible fine-grained dynamic access control approach for cloud computing environment. Cluster Computing 24, 2, 1413–1434.
[7] Mansura Habiba, Md Rafiqul Islam, ABM Shawkat Ali, and Md Zahidul Islam.(2016).A new approach to access control in cloud. Arabian Journal for Science and Engineering 41, 1015–1030.
[8] Chang, C. Y., et al. (2006).A novel access control model with time constraint. Proc. of the Int. Conf. on Networking, pp. 1–6.
[9] Outchakoucht, A., et al. (2017).Blockchain-based access control model. International Journal of Advanced Computer Science and Applications, vol. 8, no.7, pp. 417–424.
[10] Luca Cappelletti et al. (2019).On the quality of classification models for inferring abac policies from access logs. In Big Data. IEEE.
[11] Khilar, P. M., et al. (2019).Trust-Based Access Control in Cloud Computing Using Machine Learning: Intelligent Edge, Fog and Mist Computing**.** Cloud Computing for Geospatial Big Data Analytics,pp.55-79.
[12] Srivastava, G., et al. (2020). Machine Learning Based Risk-Adaptive Access Control System to Identify Genuineness of the Requester.Modern Approaches in Machine Learning and Cognitive Science, pp. 129-143.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[13] Liu, X. Du, and N. Wang.(2021). Efficient access control permission decision engine based on machine learning.Security & Communication Networks.
[14] Karimi, L., M. Aldairi, J. Joshi, and M. Abdelhakim.(2021). An automatic attribute based access control policy extraction from access logs. IEEE TDSC,
[15] Noor, Zainab, Sadaf Hina, Faisal Hayat, Ghalib A Shah.(2023).An intelligent context-aware threat detection and response model for smart cyber-physical systems, Internet of Things 23 100843.
[16] Nobi, Mohammad Nur., Ram Krishnan, Yufei Huang, Mehrnoosh Shakarami, and Ravi Sandhu.(2022).Toward deep learning based access control.In ACM CODASPY.
[17] Francis K. Mupila, Himanshu Gupta, Akashdeep Bhardwaj. (2025).AI-Driven Adaptive Access Control in Multi-Cloud Environments: A Cognitive Security Framework.Journal of Information Systems Engineering and Management, 10(28s), pp.425-441.