Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 20 No. 2 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijim.v20i02.58623

PAPER

AI-Driven Hybrid Batch Authentication for UAV-Assisted Mobile IoT Networks

Soukaina Essafi[1](✉), Ahmed El-Yahyaoui[1], Ali Ouacha[1], Iyad Lahsen-Cherif[2]

[1]Mohammed V University in Rabat, Morocco

[2]INPT, CS department, Rabat, Morocco

soukaina_essafi@um5.ac.ma

ABSTRACT

The rapid evolution of the Internet of Things (IoT) has led to a dramatic increase in the number of connected devices. Consequently, it is no longer feasible to deliver high-quality services using terrestrial infrastructure alone. Unmanned aerial vehicles (UAVs) are increasingly being used to improve the capacity and efficiency of IoT networks due to their maneuverability, economy, and flexibility. In resource-constrained IoT environments, UAVs typically employ batch authentication to securely and efficiently manage simultaneous access requests. However, if even a single signature is invalid, batch authentication will fail, which compromises the system's availability and reliability. This paper introduces a hybrid dynamic access control architecture that combines batch verification techniques with machine learning (ML) algorithms to detect fraud (i.e., identify invalid signatures) before the batch verification process in order to enhance its efficiency. The experiment's findings show that using artificial intelligence (AI) before the batch verification process can improve its efficiency and reduces the computational load.

KEYWORDS

Internet of things (IoT), unmanned aerial vehicle (UAV), batch authentication, artificial intelligence (AI), machine learning (ML)

1 INTRODUCTION

The Internet of Things (IoT) involves a wide range of connected devices that generate and share various types of data. This data is used to develop transformative applications, such as industrial manufacturing, health and environmental monitoring, autonomous vehicles, and more [1], [2]. Unmanned aerial vehicles (UAVs) are among the new solutions for large-scale IoT deployment. UAVs are attracting a great deal of interest due to their flexible deployment, high mobility, and low cost [3], [4]. Moreover, UAVs can perform a variety of tasks, including collecting data, conducting video surveillance, transporting cargo, and so on [5], [6], [7]. Consequently, UAVs are increasingly being used in IoT applications, including, but not limited to, disaster management, smart agriculture, smart cities, surveillance, and security

Essafi, S., El-Yahyaoui, A., Ouacha, A., Lahsen-Cherif, I. (2026). AI-Driven Hybrid Batch Authentication for UAV-Assisted Mobile IoT Networks. *International Journal of Interactive Mobile Technologies (iJIM)*, 20(2), pp. 150–163. https://doi.org/10.3991/ijim.v20i02.58623

Article submitted 2025-09-11. Revision uploaded 2025-11-25. Final acceptance 2025-11-26.

monitoring [8], [9]. In situations involving natural disasters that endanger people's safety, UAVs can perform critical tasks that would otherwise be carried out by human workers [5]. Furthermore, as shown in Table 1, UAVs offer additional opportunities in the context of the IoT. UAVs in an IoT scenario can improve IoT network performance [5]. However, the large number of access requests in drone-assisted IoT environments poses significant challenges in terms of both security and system performance, especially in resource-constrained environments. To overcome these challenges, UAVs typically use batch verification, which allows multiple access requests to be verified simultaneously. Compared to using traditional individual verification methods, this technique is significantly more cost-effective in terms of resource consumption [10]. Nevertheless, batch authentication is susceptible to failure if even a single invalid signature is detected, resulting in the entire batch being rejected. This wastes resources, makes the IoT network vulnerable to attacks, and compromises the availability of critical UAV-based IoT services [11].

Table 1. UAV opportunities in the IoT [3]

Opportunities	Examples
Ubiquitous connections	• Extend communication networks
Aerial intelligence	• Avoidance of collisions • Object recognition • Communication relay
Self-maintenance of communications	• Self-maintenance of topology and routing • Surveillance and anti-eavesdropping
Sensor powering and deployment	• Sensor powering • Sensor recycling

In this context, various approaches employ classical methods that are computationally intensive. These approaches are not well-suited to the limitations of IoT devices [11]. To overcome these limitations, we propose an intelligent, lightweight, AI-based mechanism that can identify and filter invalid signatures. This allows for the efficient filtering of suspicious requests before batch verification, which reduces computational costs and improves system performance.

The structure of this paper is outlined as follows: Section 2 reviews related work. Section 3 describes the proposed solution. Section 4 presents the experimental setup. Section 5 presents the results, and Section 6 provides a summary of the paper.

2 RELATED WORK

Due to the increasing number of connected devices and the necessity of secure communication, extensive research papers have been conducted on authentication in the IoT. Many approaches have been proposed to improve privacy and security in resource-constrained IoT environments. This section provides an overview of the relevant literature on batch verification, invalid signature detection, and AI-based approaches for anomaly detection in the context of the IoT, which are the three pillars of this research.

In [12] and [13], the authors regard the technique of batch verification as an ideal solution for improving verification efficiency. Batch verification of lots of digital signatures minimizes the required verification time and computational load [14]. This concept is therefore beneficial in an IoT environment, where devices have limited computation resources and operate under real-time constraints [15], [10]. This method

enables efficient and scalable authentication while ensuring security, which results in enhanced IoT network performance versus individual verification [15], [10].

Table 2 summarizes existing studies on authentication in the context of the IoT, focusing on those based on the batch verification technique.

Table 2. Review of related work

Ref	Methods	Results	Benefits
[15]	The authors introduce a trust model for IoT networks that minimizes the computational workload on gateway nodes by distributing signature authentication to reliable nodes. The approach uses batch verification of ECDSA-based signatures to reduce verification time and improve network efficiency.	The model outperforms existing solutions by reducing the workload and latency of verification.	Reduces the computational load. Improves efficiency
[14]	This work proposes a lightweight, batch-based authentication solution for the Internet of Drones (IoD). The proposed system uses physical unclonable functions (PUFs) to protect the identities of drones from attack, thereby enhancing security.	As set out in the paper, the proposed scheme provides robust security and efficient batch authentication.	Enhanced security, reduced resource consumption
[10]	The authors propose a elliptic curve-based, certificate-less signature (CLS) scheme for the IoT that focuses on batch verification and identification of invalid signatures.	As set outlined in the paper, the proposed approach offers a high Level of security and more efficient verification than related schemes.	Fault signature identification Improved batch authentication
[16]	This work proposes a lightweight, batch authentication approach leveraging edge computing to improve security and efficiency in resource-constrained IIoT environments.	the paper finds that the proposed scheme is a promising solution for enhancing the security and efficiency of IIoT environments.	Reduces the computational load.
[17]	This paper presents a lightweight, batch-based authentication solution to ensure secure communication between vehicles.	The study's findings suggest that the proposed lightweight batch authentication scheme could significantly enhance the security and efficiency of IoV communications.	Reduces the computational load, energy consumption, and communication overhead.
[18]	In this paper, the authors introduce SEAS, a new authentication solution for the IoT that is secure and robust. SEAS uses zero-knowledge proofs (ZKP) and batch authentication methods.	The paper concludes that the proposed SEAS solution is an efficient, scalable, and secure authentication scheme for large-scale IoT environments that is based on zero-knowledge proofs and a batch verification method.	Grant the anonymity of devices. Reduces verification times, computational costs, and energy consumption.

The works mentioned in Table 2 share a common weakness: they focus primarily on batch verification without providing effective and lightweight methods for detecting invalid signatures within a batch before the batch verification process to avoid batch verification failure. This drawback can have significant consequences, as invalid signature(s) delay the verification process and increase resource costs.

Traditional invalid-signature detection techniques are often inadequate for UAV-assisted IoT networks for several reasons. For one, existing techniques are computationally complex, and their static nature makes them ineffective at detecting advanced threats and constantly evolving attack patterns [10], [11], [19], [20].

In the IoT context, the challenge of identifying invalid signatures is even more significant given the specific characteristics of the IoT, including resource constraints. Furthermore, the lack of effective methods for identifying invalid signatures undermines the robustness of the system, particularly in UAV-assisted IoT contexts where the secure and rapid transmission of data is critical. This highlights the need for efficient, lightweight, adaptive, and intelligent solutions that can optimize the batch

verification process and reduce the computational load. Recent advancements in machine learning (ML), especially in intrusion detection, provide innovative solutions in this context. ML can enhance the security of the IoT ecosystem by providing intelligent systems capable of detecting and predicting both existing and emerging threats, even zero-day ones [21]. Furthermore, ML can detect abnormal activity and adapt to new types of threats, which can provide a more proactive and intelligent security mechanism than traditional techniques [22], [23], [24].

3 MATERIALS AND METHODS

3.1 AI for anomaly detection in the IoT context

As shown in Figure 1, AI can greatly enhance the performance and efficiency of IoT systems by providing intelligent data analysis and autonomous decision-making capabilities [25].

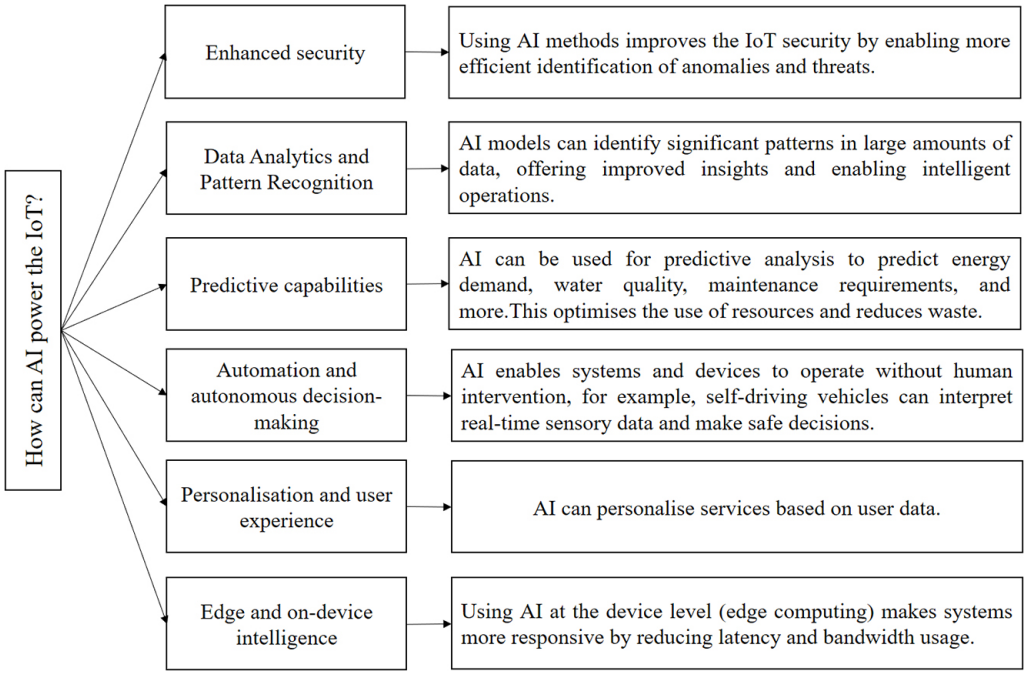

Fig. 1. The benefits of AI in IoT systems

3.2 System overview

Our architecture consists of numerous sensors deployed in isolated areas to collect data, as well as a drone that flies over these areas as shown in Figure 2. Each sensor has a pair of cryptographic keys used to sign its messages. When the UAV initiates communication, the sensors respond with signed access requests. The drone uses a batch authentication technique to ensure that only authorized objects can interact with it. To prevent and minimize batch verification failures and prevent the waste of resources, we propose using a ML model to detect and filter invalid signatures before batch verification. This model uses the random forest algorithm to analyze signature features and detect anomalies.

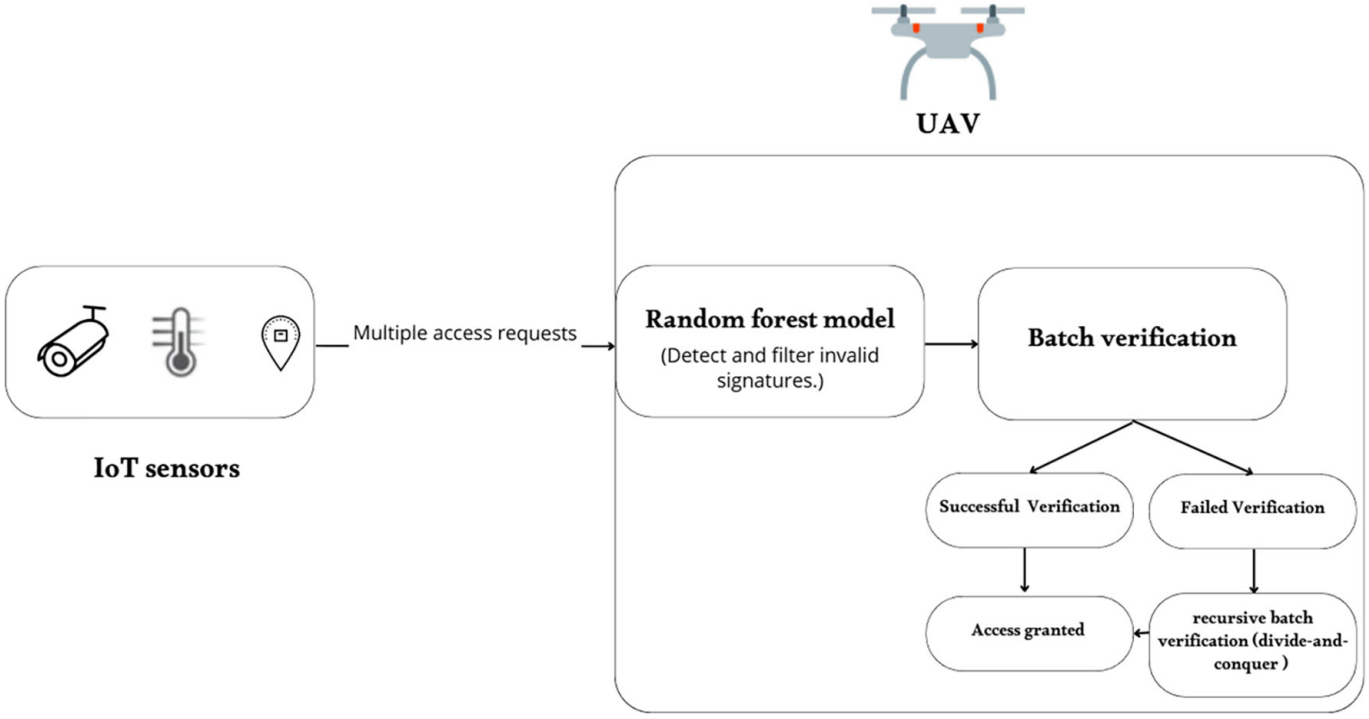

Fig. 2. System overview

3.3 Model implementation pipeline

An experimental setup was designed to evaluate the proposed model's performance, as shown in Figure 3. The findings are presented in Figure 8.

Fig. 3. Model implementation pipeline [26], [27], [28]

Dataset description. In the absence of a public real digital signature database, we evaluated our proposed model using the BotNeTIoT-L01_label_NoDuplicates.csv file from the BoTNeTIoT-L01 dataset [29], which is often used in intrusion detection systems that integrate ML methods. It contains no duplicate or missing values, and its variables are numeric. It contains 2426574 instances and 25 variables. One of these columns is a feature (label) that is used for prediction. Its value is either 0 or 1: 0 if no attack is detected and 1 if an attack is detected. The dataset description is shown in Figure 4.

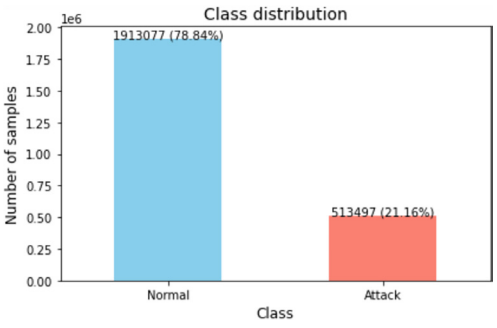

Fig. 4. The dataset's class distribution and the number of samples

Since the dataset is high-dimensional, we only used 10% of it to train our model in order to reduce computational cost and training time.

In order to evaluate the effectiveness of our model, we consider an invalid signature as equivalent to an attack. This assumption is based on the lack of publicly available real datasets providing samples of cryptographic signatures labelled as valid or invalid in IoT environments. It is also based on the fact that invalid signatures in real authentication systems are typically caused by unauthorized data manipulation or key compromise, both of which constitute attacks targeting data authenticity or integrity. Therefore, treating an invalid signature as an attack may enable the simulation of real-world malicious scenarios, even in the absence of a specific dataset.

Dataset preprocessing. The model was developed using the Python programming language and the Jupyter Notebook IDE. To manipulate the data and visualize the results, the following Python libraries were used: pandas, Numpy, matplotlib, and sklearn. Next we standardized the data using RobustScaler, as this method is more effective than the standard z-score technique at minimizing the effect of outliers in the dataset [30]. Then we employed the Synthetic Minority Oversampling technique (SMOTE) to address the class imbalance in the dataset. SMOTE is a technique designed to overcome class imbalance. It generates additional synthetic instances of the minority class to ensure a balanced distribution of classes in datasets and improve model performance [31].

Feature extraction. Feature selection can significantly improve the performance of the model by accelerating the training phase and reducing the risk of model under-fitting or overfitting.

To train our model, we selected the 10 most important variables using the Mutual Information (MI) technique.

The results of the MI analysis are shown in Figure 5.

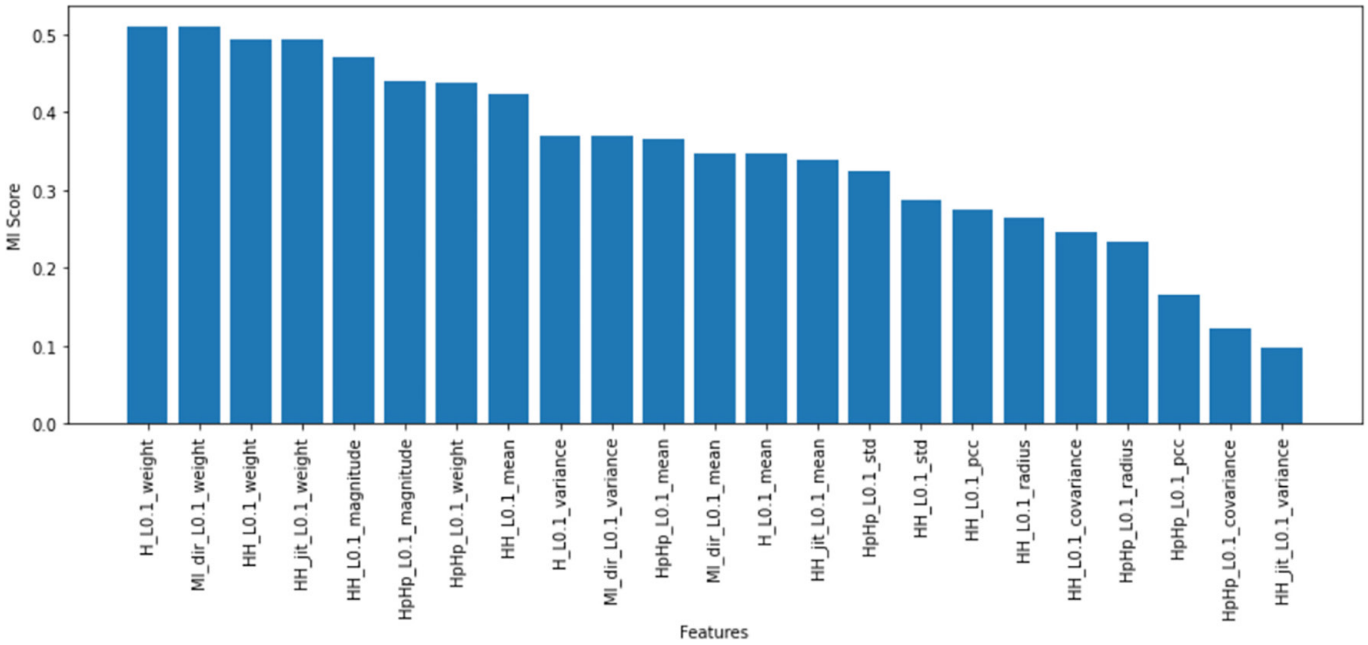

Fig. 5. The mutual information scores of each feature in the dataset

Used model. Several ML algorithms can be used in the context of our work. Each has its own particular strengths and weaknesses as shown in Table 3.

Table 3. Comparison of different AI approaches [22], [25], [32], [33]

IA Approaches	Concepts	Strengths	Weaknesses	Key IoT Security Use Cases
Supervised – support vector machines, – decision trees, – Random Forest.	Models are trained based on a dataset comprising both features (input variables) and their corresponding targets (output labels) [34]. Useful for classification or (and) Regression purposes.	Predictions with high accuracy when they are trained using well-labelled data. Easy to implement. Robustness against noise.	Reliance on labeled data constrained by dataset availability, requires regular updates, and limited capacity for adaptability (Their training on a static dataset limited their ability to recognize novel patterns/anomalies.). The process of data labelling can be costly in terms of both resources and time. Scalability.	Known anomalies classification, predictive maintenance. Predict potential cyber threats, behavior monitoring.
Unsupervised – K-means – Autoencoders	Algorithms analyze data to find patterns and make predictions without any labeled data [35].	No need for labelled data (uses unlabeled data, enabling it to discover novel patterns.).	Latency concerns	Anomaly detection, identifying abnormal patterns, and data clustering.
Reinforcement Learning – Q-learning	It learns via trial and error based on its interaction with the environment [22], [36] inspired from biological models.	Adaptive and able to learn and recognize evolving patterns. Ideal for making complex decisions.	Computationally intensive.	Useful for making dynamic decisions in environments characterized by uncertainty and constant change, such as robotics and autonomous vehicles.

In this study, we used the RF algorithm for the model training stage. This algorithm was chosen for its specific advantages [37], [38], [27]:

- Ease of implementation,
- Robustness against overfitting,
- Low resource requirements,
- Based on recent studies of ML algorithms in the context of IoT cybersecurity, RF is one of the ML algorithms that offer satisfactory results [39], [40].

Random forest is an ensemble learning technique which uses multiple decision trees to enhance the accuracy of classification or regression analyses. Each decision tree is trained individually using a randomly selected subset of the data and features. The determination of the final output is achieved by aggregating the predictions from all the trees. For classification tasks, the majority vote is used, while for regression tasks, averaging is used. This method improves the accuracy of the model, reduces overfitting and effectively manages high-dimensional data [37], [38], [27].

Model optimization. To optimize the model hyperparameter, we used Optuna with five-fold cross validation to ensure a reliable evaluation of the model's performance.

Optuna [30] is an automated hyperparameter tuning framework used for selecting the optimal hyperparameters combination [41]. Unlike conventional grid search, which explores all possible combinations of parameters exhaustively, Optuna employs a Bayesian probabilistic method to accelerate the optimization process and enhance model performance [42], [43].

Figure 6 displays the hyperparameter search space used to optimize the model's hyperparameters. The optimal parameters obtained after 30 trials are: n_estimators

= 190; max_depth = 19; min_samples_split = 7; min_samples_leaf = 3; max_features = sqrt; and bootstrap = False, as shown in Figure 7.

Parameter	Search Space
n_estimators	50 - 200
max_depth	5 - 20
min_samples_split	2 - 20
min_samples_leaf	1 - 20
max_features	sqrt, log2, None
bootstrap	True, False

Fig. 6. The hyperparameter search space used during the training stage to optimize the random forest model hyperparameters

Parameter	Value
n_estimators	190
max_depth	19
min_samples_split	7
min_samples_leaf	3
max_features	sqrt
bootstrap	False

Fig. 7. The optimal parameters achieved after 30 trials using Optuna with five-fold cross-validation

4 RESULTS AND DISCUSSION

4.1 RF Model

As Figure 8 shows, the experimental outcomes validate the effectiveness of the random forest model, which achieved nearly perfect classification. These results highlight the importance of using ML to improve the security of the Internet of Things.

Metric	Value
Accuracy	0.9997664771
Precision	0.9997666873
Recall	0.9997664771
F1-score	0.9997665187
ROC-AUC	0.9999815335

Fig. 8. Model performance results

4.2 Simulated batch authentication process

In this study, we used Python to simulate the process of authentication batches verification by following the steps in Figure 9. To evaluate our solution's performance, we compared two methods.

Method 1: Batch verification without AI. If the initial verification process fails, a verification process (recursive divide-and-conquer approach) is performed to identify invalid signature(s).

The "divide and conquer" recursive batch verification approach allows for the identification of invalid digital signatures when initial batch verification fails [44].

In "divide and conquer" approaches, a batch of signatures is recursively divided into sub-batches, for verification purposes. If a sub-batch contains no invalid signatures, it is removed from the process. else, the sub-batch is subdivided again until all the invalid signatures are eliminated [44].

Method 2: Verification using AI (our RF model) before batch verification to prevent or reduce the failure rate and minimize resource consumption.

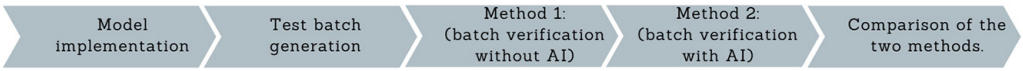

Fig. 9. Model implementation pipeline

We evaluated both methods on a set of 100 simulated signatures with a 10% invalidity rate. During the testing stage, we measured the system's Time required to verify the batch, and the time saved by using AI methods.

This simulation aims to demonstrate how incorporating AI before the batch verification process can improve efficiency. The findings of the experiment shown in Figure 10 provided the necessary comparative data to show the benefits of our solution compared to verification techniques without artificial intelligence.

	Method	Detection Time (s)	Tame saved
0	Method 1	0.072003	-
1	Method 2	0.018998	0.053006 s

Fig. 10. The computational time required for detecting invalid signatures using Methods 1 and 2, without and with AI, respectively, as well as the time saved when AI is used

Although using AI in our proposed approach has a significant impact, the full realization of its potential requires addressing several challenges and limitations. One of the most critical and emerging challenges is the vulnerability of AI models to adversarial attacks. Such attacks can alter the input data, thereby compromising the model's effectiveness. Moreover, this study's evaluation was based on a sample size (10%) of the dataset. This decision was primarily driven by computational limitations and the necessity of ensuring the feasibility of the experiments when training and validating the model. Nevertheless, the small sample size could introduce significant challenges, affecting the statistical significance and generalizability of the study's conclusions, as well as the interpretability of the results in a real-world UAV-assisted IoT environment. To address potential sampling bias, we carefully balanced the selected subset of data to preserve the main class distributions and characteristics of the original data. However, evaluating the model's performance on a larger dataset would generate more reliable results and validate its robustness and

applicability in various UAV-assisted IoT scenarios. Furthermore, to gain a deeper insight into the applicability of the proposed solution in real-world UAV-assisted IoT networks, its performance must be evaluated in various scenarios involving various network conditions and multiple batches of different sizes. An in-depth comparative analysis of the proposed model against existing related work is also needed. This will provide further insight into the model's robustness, and applicability, as well as identifying any other potential limitations.

5 CONCLUSION AND FUTURE WORKS

In UAV-assisted IoT networks, a UAV can receive simultaneous access requests from multiple sensors. Individual verification is expensive in terms of both time and resources given UAV's limited resources. To enhance verification efficiency, UAVs use the batch verification technique, which involves verifying multiple signatures simultaneously at once, reducing the time and resources required. However, if even one signature is invalid, the batch verification process will fail, which reduces its effectiveness.

This paper proposes using AI-based invalid signature detection before the batch verification process for UAV-assisted IoT to prevent or reduce batch verification failures. Although the proposed model produces positive results, there are still several challenges to overcome, which suggests that there are interesting areas for future research. One potential area for exploration is federated learning, which enables distributed IoT devices to collaborate on updating models while ensuring that sensitive data remains decentralized, to address privacy issues and reduce communication overhead. Another interesting area of research is explainable AI (XAI), which has the potential to improve the transparency, interpretability, and trustworthiness of AI models. In addition, exploring innovative lightweight optimized AI models, resource-efficient architectural designs, and more advanced optimization techniques, such as feature selection, dimensionality reduction, and model compression techniques like pruning or quantization, to ensure a balance between efficiency and performance. Furthermore, in order to both train and rigorously evaluate the proposed models, it is crucial to develop realistic datasets that reflect a variety of UAV-assisted IoT attack scenarios. Exploring these fields of research further will help to enhance and develop this work.

6 REFERENCES

[1] B. Cremonezi, A. Vieira, J. A. Nacif, and M. Nogueira, "Survey on identity and access management for Internet of Things," pp. 1–40, 2020. https://doi.org/10.21203/rs.3.rs-66793/v1

[2] M. El Hanine, A. El-Yahyaoui, and R. Es-Sadaoui, "Three layer IoT architecture: Attacks and security mechanisms," in *Proc. – 2024 11th Int. Conf. Futur. Internet Things Cloud (FiCloud),* 2024, pp. 32–38. https://doi.org/10.1109/FiCloud62933.2024.00014

[3] Y. Liu, H. N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Comput. Commun.,* vol. 155, pp. 66–83, 2020. https://doi.org/10.1016/j.comcom.2020.03.017

[4] S. Hussain, K. Mahmood, M. K. Khan, C. M. Chen, B. A. Alzahrani, and S. A. Chaudhry, "Designing secure and lightweight user access to drone for smart city surveillance," *Comput. Stand. Interfaces*, vol. 80, p. 103566, 2021. https://doi.org/10.1016/j.csi.2021.103566

[5] N. Cheng *et al.*, "AI for UAV-Assisted IoT Applications: A comprehensive review," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14438–14461, 2023. https://doi.org/10.1109/JIOT.2023.3268316

[6] M. El Hanine, A. El-Yahyaoui, and R. Es-Sadaoui, "The internet of drones: Evolution, applications and security solutions," in *Big Data and Internet of Things, BDIoT 2024*, in Lect. Notes Networks Syst., O. Mahboub, K. Haddouch, H. Omara, M. Hefnawi, Eds., vol. 887, Springer, Cham, 2024, pp. 955–965. https://doi.org/10.1007/978-3-031-74491-4_73

[7] C. Ceocea, V. Prisacariu, and L. Vladareanu, "Aerial mechatronic systems for collection of atmospheric and environmental data," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 10, pp. 139–149, 2020. https://doi.org/10.3991/ijim.v14i10.15257

[8] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. Bin Zikria, "GCACS-IoD: A certificate based generic access control scheme for Internet of drones," *Comput. Networks*, vol. 191, p. 107999, 2021. https://doi.org/10.1016/j.comnet.2021.107999

[9] B. Al-rami, K. M. A. Alheeti, W. M. Aldosari, S. M. Alshahrani, and S. M. Al-abrez, "A new classification method for drone-based crops in smart farming," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 9, pp. 164–174, 2022. https://doi.org/10.3991/ijim.v16i09.30037

[10] H. Xiong, Y. Wu, C. Su, and K.-H. Yeh, "A secure and efficient certificateless batch verification scheme with invalid signature identification for the internet of things," *J. Inf. Secur. Appl.*, vol. 53, p. 102507, 2020. https://doi.org/10.1016/j.jisa.2020.102507

[11] Z. Ren, M. Zhu, X. Li, S. Yuan, Y. Miao, and R. H. Deng, "PIC-BI: Practical and intelligent combinatorial batch identification for UAV assisted IoT networks," in *CCS 2024 – Proc. 2024 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2024, pp. 3645–3658. https://doi.org/10.1145/3658644.3670303

[12] A. S. Kittur and A. R. Pais, "Batch verification of digital signatures: Approaches and challenges," *J. Inf. Secur. Appl.*, vol. 37, pp. 15–27, 2017. https://doi.org/10.1016/j.jisa.2017.09.005

[13] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-to-Peer Netw. Appl.*, vol. 13, pp. 53–63, 2020. https://doi.org/10.1007/s12083-019-0718-9

[14] Y. Zhang, L. Meng, M. Zhang, and W. Meng, "A secure and lightweight batch authentication scheme for Internet of Drones environment," *Veh. Commun.*, vol. 44, p. 100680, 2023. https://doi.org/10.1016/j.vehcom.2023.100680

[15] A. S. Kittur and A. R. Pais, "A trust model-based batch verification of digital signatures in IoT," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 1, pp. 313–327, 2020. https://doi.org/10.1007/s12652-019-01289-z

[16] J. Cui, F. Wang, Q. Zhang, C. Gu, and H. Zhong, "Efficient batch authentication scheme based on edge computing in IIoT," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 1, pp. 357–368, 2023. https://doi.org/10.1109/TNSM.2022.3206378

[17] H. Sikarwar and D. Das, "Towards lightweight authentication and batch verification scheme in IoV," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 5, pp. 3244–3256, 2022. https://doi.org/10.1109/TDSC.2021.3090400

[18] Z. Su *et al.*, "A secure and efficient authentication scheme for large-scale IoT devices based on zero-knowledge proof," *Electron.*, vol. 13, no. 18, pp. 1–22, 2024. https://doi.org/10.3390/electronics13183735

[19] M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, "UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions," *IEEE Trans. Intell. Veh.*, vol. 9, no. 4, pp. 4583–4605, 2024. https://doi.org/10.1109/TIV.2023.3309548

[20] B. D. Deebak and F. Al-turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Computer Communications*, vol. 162, pp. 102–117, 2020. https://doi.org/10.1016/j.comcom.2020.08.016

[21] I. T. Al-Halboosi, B. M. Elbagoury, S. A. El-Regaily, and E.-S. M. El-Horbaty, "A hybrid-transformer-based cyber-attack detection in IoT networks," *Int. J. Interact. Mob. Technol. (iJIM)*, vol. 18, no. 14, pp. 90–102, 2024. https://doi.org/10.3991/ijim.v18i14.50343

[22] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020. https://doi.org/10.1109/COMST.2020.2988293

[23] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: Security and solutions Survey," *Sensors*, vol. 22, no. 19, pp. 1–51, 2022. https://doi.org/10.3390/s22197433

[24] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020. https://doi.org/10.1109/COMST.2020.2986444

[25] O. Aouedi *et al.*, "A survey on intelligent internet of things: Applications, security, privacy, and future directions," *IEEE Commun. Surv. Tutorials*, vol. 27, no. 2, pp. 1238–1292, 2024. https://doi.org/10.1109/COMST.2024.3430368

[26] H. Kayan, Y. Majib, W. Alsafery, M. Barhamgi, and C. Perera, "AnoML-IoT: An end-to-end re-configurable multi-protocol anomaly detection pipeline for Internet of Things," *Internet of Things*, vol. 16, p. 100437, 2021. https://doi.org/10.1016/j.iot.2021.100437

[27] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019. https://doi.org/10.1016/j.iot.2019.100059

[28] P. Probst, M. N. Wright, and A. L. Boulesteix, "Hyperparameters and tuning strategies for random forest," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 9, no. 3, pp. 1–19, 2019. https://doi.org/10.1002/widm.1301

[29] "IoT dataset for Intrusion Detection Systems (IDS)." Accessed: Aug. 10, 2025. [Online]. Available: https://www.kaggle.com/datasets/azalhowaide/iot-dataset-for-intrusion-detection-systems-ids

[30] Z. Elkhadir and M. A. Begdouri, "Enhancing IoT security: A comparative analysis of preprocessing techniques and classifier performance on IoT23 and CIC IoT 2023 datasets," *IAENG Int. J. Comput. Sci.*, vol. 52, no. 4, pp. 995–1010, 2025.

[31] A. Fernández, S. García, F. Herrera, and N. V. Chawla, "SMOTE for learning from imbalanced data: Progress and challenges, marking the 15-year anniversary," *J. Artif. Intell. Res.*, vol. 61, pp. 863–905, 2018. https://doi.org/10.1613/jair.1.11192

[32] K. DeMedeiros, A. Hendawi, and M. Alvarez, "A survey of AI-based anomaly detection in IoT and sensor networks," *Sensors*, vol. 23, no. 3, p. 1352, 2023. https://doi.org/10.3390/s23031352

[33] M. H. Alsharif, A. H. Kelechi, K. Yahya, and S. A. Chaudhry, "Machine learning algorithms for smart data analysis in internet of things environment: Taxonomies and research trends," *Symmetry*, vol. 12, no. 1, p. 88, 2020. https://doi.org/10.3390/sym12010088

[34] Z. H. Zhou, "A brief introduction to weakly supervised learning," *Nat. Sci. Rev.*, vol. 5, no. 1, pp. 44–53, 2018. https://doi.org/10.1093/nsr/nwx106

[35] S. Naeem, A. Ali, S. Anam, and M. M. Ahmed, "An unsupervised machine learning algorithms: Comprehensive review," *Int. J. Comput. Digit. Syst.*, vol. 13, no. 1, pp. 911–921, 2023. https://doi.org/10.12785/ijcds/130172

[36] Y. Matsuo *et al.*, "Deep learning, reinforcement learning, and world models," *Neural Networks*, vol. 152, pp. 267–275, 2022. https://doi.org/10.1016/j.neunet.2022.03.037

[37] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: Machine learning for enhanced security," *Sci. Rep.*, vol. 14, no. 1, pp. 1–16, 2024. https://doi.org/10.1038/s41598-024-56126-x

[38] E. Krzysztoń, I. Rojek, and D. Mikołajewski, "A comparative analysis of anomaly detection methods in IoT networks: An experimental study," *Appl. Sci.,* vol. 14, no. 24, p. 11545, 2024. https://doi.org/10.3390/app142411545

[39] N. Hamza, H. Lakmal, M. W. P. Maduranga, and R. P. S. Kathriarachchi, "Malware detection of IoT networks using machine learning: An experimental study with edge IIoT dataset," in *30th Annu. Tech. Conf. Sri Lanka Network*, Colombo, Sri Lanka, 2023.

[40] M. M. Kontagora, S. A. Adeshina, and H. Musa, "A comparative analysis of machine learning models for real-time IoT threat detection with focus on Mirai Botnet," *Open Access Library Journal*, vol. 12, pp. 1–12, 2025. https://doi.org/10.4236/oalib.1112855

[41] Y. Shen, S. Wu, Y. Wang, J. Wang, and Z. Yang, "Interpretable model for rockburst intensity prediction based on Shapley values-based Optuna-random forest," *Undergr. Sp.,* vol. 21, pp. 198–214, 2025. https://doi.org/10.1016/j.undsp.2024.09.002

[42] X. Xiao *et al.*, "An interpretable model for landslide susceptibility assessment based on Optuna hyperparameter optimization and random forest," *Geomatics, Nat. Hazards Risk*, vol. 15, no. 1, p. 2347421, 2024. https://doi.org/10.1080/19475705.2024.2347421

[43] I. Nur Hermawan and A. Rinaldi Dikananda, "Comparing optimization hyperparameter long short term memory for rainfall prediction model," *J. Tek. Inform. C.I.T Medicom*, vol. 16, no. 6, pp. 404–415, 2025.

[44] B. J. Matt, "Identification of multiple invalid signatures in pairing-based batched signatures," in *Public Key Cryptography – PKC 2009,* in Lect. Notes Comput. Sci., S. Jarecki and G. Tsudik, Eds., vol. 5443, 2009, pp. 337–356. https://doi.org/10.1007/978-3-642-00468-1_19

7 AUTHORS

Soukaina Essafi received her Master's degree in Data Engineering and Software Development from the Faculty of Sciences, Mohammed V University in Rabat, Morocco. She is currently a Ph.D. candidate at the same faculty. Her doctoral research focuses on IoT security, including lightweight cybersecurity mechanisms and AI-Based Security Solutions for IoT Networks (E-mail: soukaina_essafi@um5.ac.ma).

Ahmed El-Yahyaoui holds an engineering degree in software engineering from the National Institute of Posts and Telecommunications (INPT), Rabat, Morocco. He earned his Ph.D. in computer security from the National School for Computer Science (ENSIAS), Morocco. He is currently an Associate Professor at the Faculty of Sciences, Mohammed V University in Rabat. His research interests include applied cryptography, encryption, and cloud security (E-mail: a.elyahyaoui@um5r.ac.ma).

Ali Ouacha is a Professor of computer science at the Faculty of Science of Rabat (FSR) Universities Mohamed V (UM5). He received his doctorate degree from the Mohammadia School of Engineering (EMI). Ouacha is a permanent member of the Intelligent Processing and Security of Systems (IPSS) team of Computer Science Department at the FSR. His research is currently focused on optimizing the performance of routing protocols in an Internet of Things (IoT), Mobile Edge Computing (MEC) and Mobile Ad-hoc Networks environment. He is the author and co-author of several publications in international journals and conferences. Ouacha is a member of the organizing committees of several scientific events (Conferences and Congresses). He is also a member of the Technical Program Committee (TPC) of several international conferences and journals (E-mail: a.ouacha@um5r.ac.ma).

Iyad Lahsen-Cherif received the Ph.D. degree from Paris-Saclay University, in 2016. In 2017, he was a Temporary Teaching and Research Assistant (ATER) with the Laboratoire de Recherche Informatique (LRI), Paris-Sud University. From 2019 to 2022, he was an Artificial Intelligence Research Scientist with the Thales Group. Prior to 2019, he was a Research Scientist with Orange Labs, France. He is currently a Professor with INPT, Rabat, Morocco. His expertise includes machine/deep learning and GenAI for networks, cybersecurity, healthcare, and GeoAI systems (E-mail: lahsencherif@inpt.ac.ma).