SuRaksha: AI-Powered Blockchain Framework for HVAC Tamper Detection and Authentication in Smart Classrooms

Sushil Kumar Singh (Member, IEEE)[1,*], Krunal Vaghela[1], Ashish Khanna[2], Bal Virdee[3], Manish Kumar[1,*]

***Abstract*— Smart Classrooms (SCR) are reshaping the learning experience with their interactive technology and personalized knowledge, leading to improved student engagement by seamlessly integrating digital gadgets. In this rapidly evolving landscape, the integrity and efficiency of Heating, Ventilation, and Air Conditioning (HVAC) systems are essential to the futuristic student's life. This paper introduces SuRaksha: AI-Powered Blockchain Framework for HVAC Tamper Detection and Authentication in Smart Classrooms. Leveraging the power of ensemble learning (EL) at the intelligent and connection layer of the proposed framework, our approach employs IoT sensors to collect comprehensive data from HVAC appliances. The EL algorithms then analyze the collected data to detect any instances of tampering in real-time. At the security layer, robust authentication mechanisms are implemented to verify the integrity of the HVAC data before securely storing it on the cloud. This multi-layered framework enhances the detection and authentication processes and ensures the reliability and security of HVAC operations in intelligent classroom environments. Extensive experiments and validations demonstrate the efficacy of the proposed framework in identifying tampering incidents and providing a secure, authenticated, and reliable system for modern educational facilities. The validation outcomes of the proposed framework demonstrate excellent performance, with an average processing time of 3.725 Secs and 99.84% accuracy for Smart Classrooms compared to existing works.**

***Index Terms*— Blockchain, AI, HVAC, Tamper Detection, Smart City, Ensemble Learning, Privacy, and Security.**

I. Introduction

Smart classroom, Smart classroom (SCR) is an innovative and creative educational domain that fuses advanced communication technologies to improve learning incidents [1]. These classrooms are connected with interactive whiteboards and electronic gadgets, digital projectors, and internet-enabled IoT and sensor devices; they encourage an exciting and dynamic environment for teachers and students. SCR also promotes collaborative learning and teaching, allowing students to collaborate on academic projects and share thoughts seamlessly. Data analytics provides discernment into student performance, enabling educators to identify fields for progress and consequently adjust their teaching approaches [2]. Moreover, utilizing Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), and advanced sensor devices offers automatic periodic tasks, streamlining classroom administration. This technology-driven approach improves academic outcomes and qualifies students for a future in an increasingly futuristic digital world. Enhanced security characteristics provide a safe learning environment, while energy-efficient systems contribute to sustainability objectives [3]. SCR represents a significant educational advancement, delivering numerous advantages beyond traditional teaching methods.

Security, privacy, and authentication are necessary for intelligent and smart classrooms, especially concerning HVAC techniques [4]. These systems regulate the indoor climate to maintain a comfortable and conducive learning environment. However, HVAC systems are vulnerable to tampering and unauthorized access by cyber attackers or insider threats. Such breaches can disrupt the functionality of educational institutions, increase operational costs, and potentially cause system damage. These issues ultimately hamper seamless classroom activities. Also, probable reasons should be figured out in case of such incidents to protect SCR activities. These malicious activities should be detected and require robust authentication protocols to ensure that only authorized users can access, modify, or adjust the settings of HVAC. Additionally, implementing secure data transmission and storage methods helps protect and secure sensitive information about classroom usage and environmental requirements. Ensuring the integrity of HVAC operations enhances energy efficiency and sustainable environments and contributes to secure, productive learning circumstances where privacy concerns are effectively addressed [5].

Artificial Intelligence (AI) significantly enhances the management of HVAC systems in smart classrooms [6]. AI techniques (for instance ML and Deep Learning (DL)) can analyze environmental as well as classroom data such as the strength of the students, classroom size, area occupancy, floor, and face of the classroom to optimize temperature and air quality in real-time, ensuring a comfortable learning atmosphere. Predictive maintenance capabilities allow AI to identify potential HVAC tamper detection and alert the response team so that all countermeasures can be taken seamlessly. It helps in reducing downtime and maintenance costs. Additionally, AI helps improve energy efficiency by learning usage patterns and adjusting HVAC settings, accordingly, reducing energy consumption and lowering operational costs [7]. AI enhances comfort and efficiency and contributes to a sustainable and effective SCR environment.

Sushil Kumar Singh (Member, IEEE) is with the Department of Computer Engineering at Marwadi University, Rajkot, India, and is a postdoc researcher at the Center for Communications Technology at London Metropolitan University, United Kingdom, Manish Kumar and Krunal Vaghela are with the Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India. (Email: krunal.vaghela@marwadieducation.edu.in). Ashish Khanna (Member, IEEE) is with the Department of Computer Science and Engineering at Maharaja Agrasen Institute of Technology (GGSIPU), India. (Email: ashishkhanna@mait.ac.in). Prof. Bal Virdee (Member, IEEE) is the Centre for Communications Technology research group director at London Metropolitan University, United Kingdom (Email: b.virdee@londonmet.ac.uk). Corresponding Authors: Sushil Kumar Singh, and Manish Kumar (Emails: {sushilkumar.singh, manishkumar.gupta}@marwadieducation.edu.in)

TABLE I
SUMMARY OF COMPARISON WITH EXISTING RESEARCH STUDY

Research Study	Technology	Ensemble Approach	Data Authentication	Security	HVAC Tamper Detection	Data Imbalance Solution	Environment
Jianhua et al. [11]	Reinforcement Q-Learning, Markov Model	×	✓	✓	×	×	Smart Campus
Sanchez et al. [12]	IoT, Cybersecurity	×	×	✓	×	×	Smart Learning
Shareviski et al. [13]	User-centered Cyber Security	×	×	✓	×	×	Classroom
Abdalzaher et al. [14]	IoT, Machine Learning	×	×	✓	×	×	Smart System
Saharkhizan et al. [15]	Deep Recurrent Neural Network	✓	×	✓	×	×	IoT Devices and System
Jadav et al. [17]	AI and Blockchain	✓	×	✓	×	×	Healthcare Management System
Dutta et al. [21]	Blockchain, AI, PoAh 2.0	×	✓	✓	×	×	IoMT Edge
Proposed Work	Blockchain, PoAh, Ensemble Learning	✓	✓	✓	✓	✓	Smart Classrooms

However, external tampering or spikes in energy consumption require examination and authentication. Blockchain and cryptographic algorithms play a crucial role in securing smart classroom environments by ensuring data integrity and privacy. Blockchain technology provides a decentralized ledger that records all transactions and interactions, making it nearly impossible to alter data without detection. This transparency helps prevent unauthorized access and tampering with sensitive information, such as student records or classroom resources [8]. Cryptographic algorithms further enhance security by encrypting data, ensuring that only authorized users can access or modify it. Together, these technologies create a robust framework that protects the digital infrastructure of smart classrooms, fostering a secure and trustworthy learning environment. Integrating AI, blockchain, and cryptographic algorithms in smart classrooms creates a secure and authentic learning environment. AI enhances operational efficiency by analyzing data to optimize classroom conditions and detect anomalies [9]. Blockchain technology ensures transparency and immutability, recording all transactions and interactions in a decentralized ledger, which prevents unauthorized modifications. Cryptographic algorithms provide robust data encryption, protecting sensitive information from breaches. These technologies enable secure authentication, real-time monitoring, and data integrity, fostering a trustworthy and efficient educational setting where privacy is maintained and system tampering is minimized.

Ensuring tamperproof and efficient HVAC systems is paramount with the increasing adoption of SCR environments. These systems play a critical role in maintaining comfortable learning conditions, but they are vulnerable to tampering and unauthorized access, leading to energy inefficiency and compromised indoor air quality. SuRaksha is an innovative AI-powered blockchain framework designed to enhance the security and integrity of SCR HVAC systems. By combining artificial intelligence and blockchain technology, SuRaksha detects tampering and authenticates system operations, ensuring optimal performance and reliability. Our system saves detailed records on a secure cloud platform to ensure that the real reasons behind HVAC faults or anomalies are preserved. This cloud-based approach facilitates easy access and analysis of historical data, aiding in physical investigations and improving security protocols. The motivation behind SuRaksha is to address the dual challenges of maintaining HVAC system security and providing energy efficiency in educational environments. Traditional methods often need more real-time detection and response. By leveraging AI for anomaly detection and blockchain for secure, transparent data management, SuRaksha offers a robust solution that enhances the sustainability and safety of SCR.

A. Related Work

Dimitriadou and Lantis [10] have discussed technological advancement in education and highlighted the benefits of emerging technology like AI and IoT in smart classrooms. Jianhua [11] discusses the necessity of network security in smart campuses and the eradication of brute force attacks using ML techniques like the Markov model and reinforced Q learning algorithm. Similarly, Sanchez et al. [12] have discussed a pedagogical approach to teaching and learning IoT cybersecurity. Similarly, Sharevski et al. [13] have discussed secure design for IoT and the amalgamation of cybersecurity needs in classrooms and labs. Abdalzaher et al. [14] provide ideas of technologies like Machine Learning (ML) in securing IoT-based systems, which are usually integrated to develop intelligent classrooms. In addition, Saharkhizan et al. [15] have employed ML techniques like K-Nearest Neighborhood (K-NN), Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), and Random Forest for detecting cyberattacks using network traffic or data. Since these techniques are data-driven processes, many researchers are also highlighting the application of Deep Learning (DL), such as Long Short Term Memory (LSTM) or Gated Recurrent Unit (GRU) approaches in handling highly complex or temporal relations like detecting cyberattacks [16]–[18]. Lian et al. [19] discussed using highly efficient ML techniques to detect intrusion, and they applied Decision Tree (DT)-based Ensemble Learning (EL). Here, various DT performances are aggregated and formed using an ensemble technique. Thus, these AI-based techniques can efficiently secure any IoT-based smart solution. Apart from that, only a few research studies are available that discuss the real problem of smart classrooms, and issues related to HVAC in small ones still need to be explored, as shown in Table I.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3560077

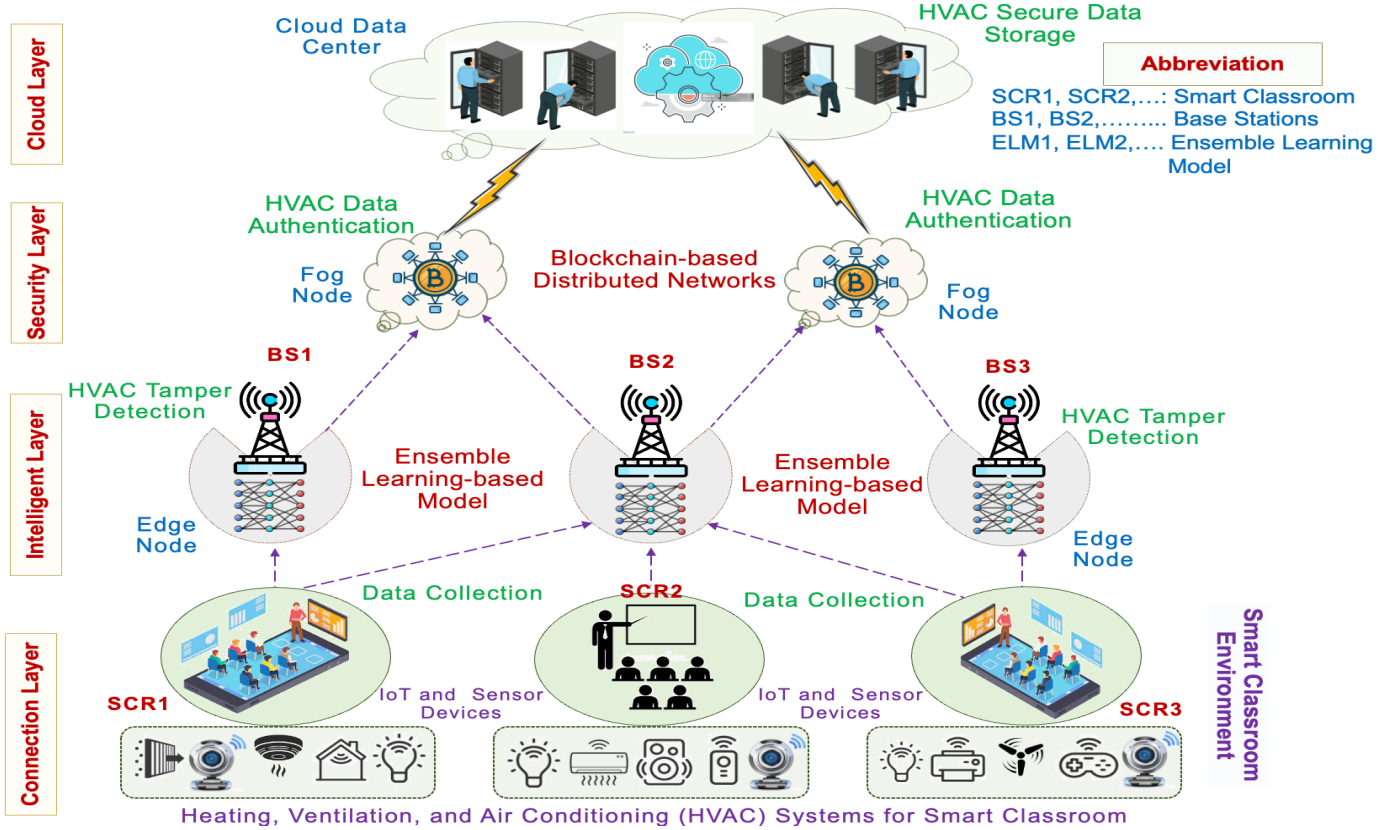

Fig. 1: Proposed AI-Powered Blockchain Framework Overview for Smart Classroom

Here, we have employed Decision Tree (DT)-based Ensemble Learning (EL) to detect external tampering in the HVAC of smart classrooms. Also, EL is used for the feature selection, this step not only overcomes the computational complexity but also helps to eradicate overfitting of the proposed classifier. After detecting any tampering, the next challenge is to authenticate these data and then save it on the cloud for future use—research in [20], [21] blockchain-based Proof of Authentication (PoAh) to authenticate these data. The merits of PoAh algorithm is that it is specifically designed for resource-constrained IoT devices. The PoAh-based cryptographic authentication mechanism will secure the HVAC systems of SCR through data authentication. In fact, there are various consensus algorithms in Blockchain Technology, such as Proof of Work (PoW), Proof of Stack (PoS), Proof of Availability (PoA), and others [22], [23]. The PoAh offers more security than other consensus algorithms by verifying miner nodes or trusted nodes, making it suitable for private and permissioned blockchains. This mechanism is particularly beneficial for resource-constrained and authenticated devices, making blockchain applications viable for SCR challenges.

B. *Article Contribution*

The main article contribution is as follows:

- Propose AI-Powered Blockchain Framework for HVAC Tamper Detection and Authentication in SCR.
- Design an HVAC Tamper Detection approach based on Ensemble Learning at the second (Intelligent) layer.
- Develop a Blockchain-based Distributed Network for HVAC Data Authentication at the third (Security) layer of the proposed framework for the secure environment in SCR, then store HVAC data at the last (Cloud) layer.
- Finally, we use subjective and quantitative analysis to validate the proposed framework against existing research studies based on standard parameters such as computational and transactional cost, trust, and security analysis.

C. *Article Structure*

The article's organization is as follows: first, section II describes the Proposed Framework Overview for HVAC Tamper Detection and Authentication in smart classrooms and details the methodological flow structure with a step-by-step explanation. Next, Section III presents the experimental results and security quantitative analysis. Finally, the article concludes in Section IV.

TABLE II
ABBREVIATION TABLE

Symbols	Description	Symbols	Description
$\{SCR_1, SCR_2, ..\}$	Smart Classroom	$\{t_n\}$	Trusted Nodes
$\{IS_1, IS_2 ..\}$	IoT Sensor Devices	$\{PoAh\}$	Proof of Authentication
$HVAC$	Heating, Ventilation, Air Conditioning	DT	Decision Tree
$\{BS_1, BS_2 ....\}$	Base Stations	$\{t_{n_1}, t_{n_2}, t_{n_3}\}$	Transactions
$\{ELM_1, ELM_2, ..\}$	Ensemble Learning Models	$\{t_f\}$	Faith value
$\{A_{Keys}\}$, $\{B_{Keys}\}$	Private and Public Keys	$\{ELTT_1, ELTT$	Ensemble Learning Tampering Transactions

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3560077

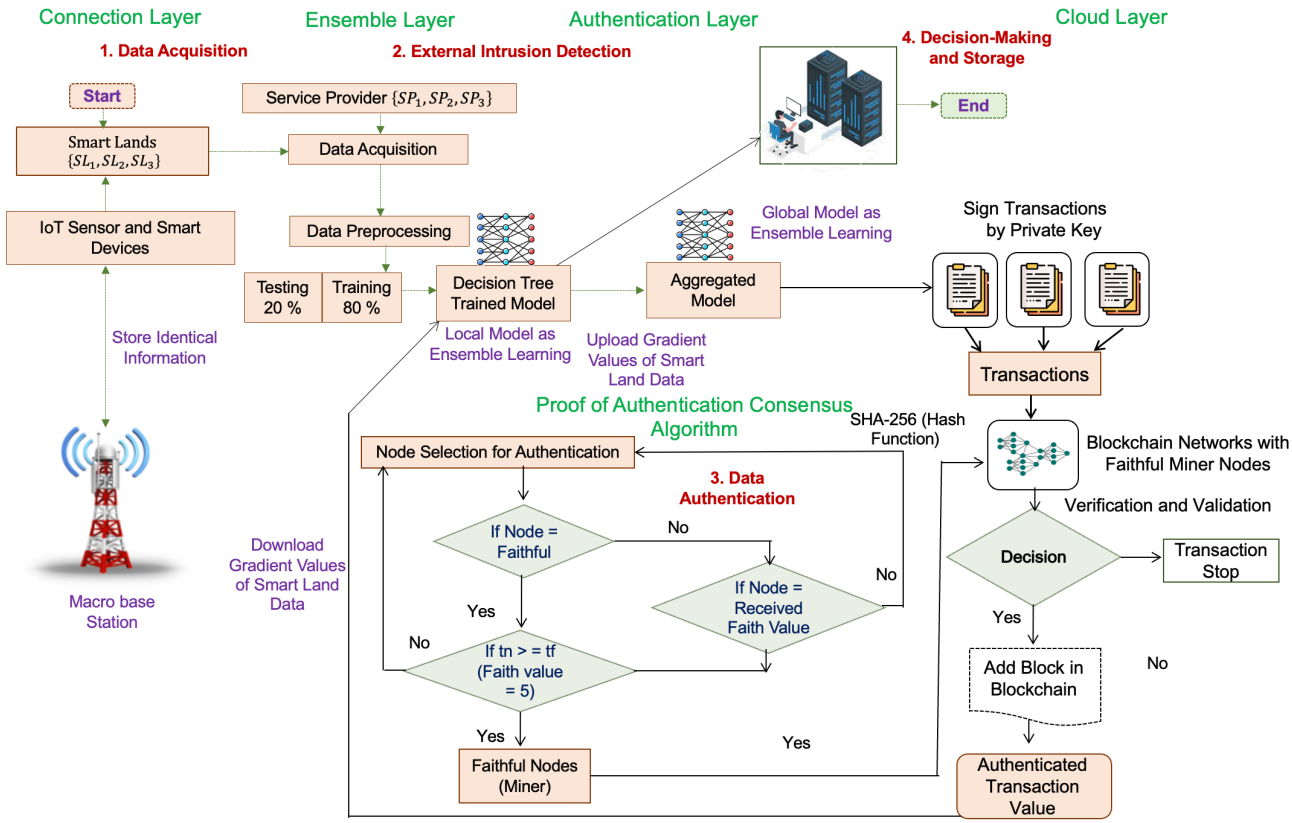

Fig. 2: Proposed HVAC Tamper Detection Framework's Methodological Flow

II. AI-Powered Blockchain Framework for HVAC Tamper Detection and Authentication in Smart Classrooms

This section describes and discusses the proposed AI-Powered Blockchain Framework with methodological flow. HVAC Tamper Detection is described at the Intelligent Layer of the proposed architecture, and HVAC data authentication and verification are illustrated at the security layer. Therefore, we start with an overview of the framework and then go through all the parts conferred step by step. The abbreviation table is shown in Table II.

A. Proposed Secure Architecture Overview

In Fig. 1, we describe the Proposed Idea concept with four layers: Connection, Intelligent, Security, and Cloud. At the first layer, IoT sensor devices such as heating, ventilation, air conditioning, and others are connected to Smart Classrooms. These IoT sensor devices generate data based on smart class requirements. At the Intelligent layer, we are utilizing an ensemble learning-based base station for HVAC Tamper Detection. After that, data is transferred to the next layer (Security Layer), which is leveraged by Blockchain technology. PoAh consensus algorithm is used at the security layer for data authentication. The PoAh offers more security than other consensus algorithms by verifying miner nodes or trusted nodes, making it suitable for private and permissioned blockchains. After data authentication and validation of the smart class data, it is communicated to the upper layer, named the cloud layer, for storing purposes.

B. HVAC Tamper Detection Approach

The proposed Ensemble Learning (EL) algorithm for HVAC tamper detection leverages Decision Tree (DT) and is strategically deployed at the Intelligent Layer of the SCR. The Bagging technique, which combines predictions from multiple DT models, is used as the core of the proposed EL model. This improves the overall performance of the tamper detection system by reducing the impact of overfitting that can occur in individual DT techniques. It benefits in terms of model stability as well as versatility. The EL-based predictive model averaging multiple tree outcomes and providing more stable predictions can be adapted to different problems and can handle large and complex datasets more effectively. The mathematical model delineating bagging with DT is as follows:

Let D be the original dataset of size N, and D_i be the i^{th} bootstrap samples of size N, obtained by random sampling with replacement. The dataset is prepared on the basis of IoT-based sensor data, which monitor the HVAC performance, such as classroom temperature, humidity, and power consumption. The process of creating B bootstrap samples can be represented as,

$$D_i = [(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \cdots, (x_{iN}, y_{iN})] \quad (1)$$

where, $(i = 1,2, \cdots, B)$ and h_i be the i^{th} DT on the i^{th} bootstrap sample D_i.

$$h_i: X \to Y \quad (2)$$

Train each DT model on its respective bootstrap sample.

$$h_i = TrainDT(D_i) \quad (3)$$

For classification tasks, the final prediction $f(x)$ is evaluated by a majority vote among the predictions of individual trees and it is determined as,

$$f(x) = MajorityVote(h_1(x), h_2(x), \cdots, h_B(x)) \quad (4)$$

The proposed model is built using DT-based proposed EL, and is employed to the AI-Powered Blockchain Framework for SCR. Also, the performance of the developed HVAC tampered detection model is evaluated on various quantitative metrics as,

$$Accuracy(\%) = \left(\frac{TP+TN}{TP+FN+FP+FN}\right) \times 100 \quad (5)$$

$$Recall = \frac{TP}{TP+FN} \quad (6)$$

$$Specificity = \frac{TN}{FP+TN} \quad (7)$$

$$Precision = \frac{TP}{TP+FP} \quad (8)$$

$$FPP = \frac{FP}{FP+TN} \quad (9)$$

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precison+Recall} \quad (10)$$

$$MCC = \frac{TN \times TP - FN \times FP}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (11)$$

TP, TN, FN, and FP represent True Positive, True Negative, False Negative, and False Positive, respectively. Algorithm 1 presents complete design steps for the tamper detection of SCR.

Algorithm 1: Ensemble Learning-based HVAC Tamper Detection Model

Input: Providing HVAC tampering-based data and its response, i.e., D = [($x_{1,}$, $y_{1,}$), ($x_{2,}$, $y_{2,}$), ..., ($x_{N,}$, $y_{N,}$)] for the training of the proposed EL model.
Output: Classifying HVAC tampering.
Start:

1: Load IoT-based HVAC dataset 'D'

2**:** Define Input features X and Target labels Y (i.e., tampered data) X = D (:, 1:end-1); Y = D (:, end);

3**:** $x_{norm}^{i} = \frac{X_i - X_{min}}{X_{max} - X_{min}}$; scaling feature [0-1].

4**:** Apply RusBoost ensemble learning to handle class imbalance and rank features by importance. Helps to select features i.e., $X\_selected$.

5**:** Train the proposed EL Model using ($X_{selected}, Y_{train}$) data.

6**:** Evaluate and cross-validate the trained model using unknown data i.e. Y_{test}.

7. Compute the confusion matrix and performance metrics.

End;

Algorithm 1 highlights using a Random Under-Sampling Boosting (RusBoost) technique to handle class imbalance and select the most important features that impact tampering. The importance of each feature is calculated, and features with importance above the median are chosen. The proposed EL technique using the Bagging method with DT is built on the features chosen and evaluated using 5-fold cross-validation, and the cross-validation loss is calculated. Also, the function fitcensemble is used to train the proposed classification model in MATLAB.

C. Blockchain-based Tamper Data Authentication Mechanism

In the proposed AI-powered blockchain framework, Blockchain networks utilize numerous trusted miner nodes to ensure robust Authentication and Validation. The Proof of Authentication (PoAh) consensus algorithm leverages these nodes for tasks such as HVAC tamper data authentication within the Smart Classrooms (SCR) at the framework's security layer, effectively addressing security and privacy concerns. Gradient values derived from SCR data are aggregated into batches of transactions, as depicted in Fig. 2. Private keys $\{A_{keys}\}$ are then assigned to these blocks, which are subsequently broadcast across the Blockchain network. Trusted miner nodes employ the SHA-256 algorithm to verify and validate these blocks or transactions, solving cryptographic puzzles using private keys. The verification process is further enhanced by assigning "faithful values" to miner nodes, as detailed in Algorithm 2 [24]. By combining trusted miner nodes with private key mechanisms, the framework ensures secure and reliable Authentication and Validation of SCR data within the Blockchain network.

Algorithm 2: HVAC Tamper Data Authentication

Input: Ensemble Learning Tampering Transactions $\{ELTT_1, ELTT_2, ELTT_3..\}$ of Smart Classroom, Faithful Miner Nodes, Private Keys $\{A_{keys}\}$, Public Keys $\{B_{keys}\}$.
Output: Authenticated and Validated HVAC External Threat Values for SCR
Process:
1: **Start:**
2: $\{tn_1, tn_2, tn_3, \ldots, tn_i\} \leftarrow All\ Block$;
3: Blocks$\{Tx_1, Tx_2, Tx_3, \ldots, Tx_i\} \leftarrow \{A_{keys}\}$;
4: Blocks $A_{keys} \rightarrow^{Broadcast}$ Network $\{TrN_1, TrN_2, TrN_3, ..\}$
5: Select Faithful Nodes ==→ Authentication and Validation
6: **if** (Miner Node = = faithful)
7: **if** ($t_n >= t_f$ (Faith value = 5));
8: Nodes are faithful
9: **else** 4th Step.
10: **else if** (Normal Node ← Received miner faith value);
11: **else** 6th to 7th Steps;
12: **else** 4th Step.
13: Faithful Miner Nodes←Checks Blocks A_{Keys} ← with B_{Keys} (SHA256 Algorithm);
14: **if** (Validation ==True)
15: Block addition in Blockchain Networks;
16: **else** Unauthorized Transaction;
17: **END;**

III. Performance and Security Quantitative Evaluation

This section highlights the simulation environment, details of data involved in the experiments, and the subjective and quantitative outcomes of the proposed framework. It consists of the performance of the EL-based classifier as a tamper detection at the edge node as well as the results of the PoAh consensus algorithm at the Fog node of SCR. Table III exhibits the details of software as well as hardware specifications used in this research work for developing a tamper detection model as well as authentication. We conducted a case study involving two classrooms to analyze energy usage patterns and HVAC performance. Power consumption data was recorded every 15 minutes from February to July 2024, enabling detailed temporal analysis. Additionally, various attributes were recorded, including time, date, day, student strength, area-wise occupancy, classroom floor and orientation, humidity, CO2 levels, and power consumption. Tampering incidents were identified by analyzing deviations in average power consumption over time, and these instances were labeled accordingly. The developed dataset comprised 34,944 rows and 11 columns, where the first 10 columns represent the last one is the categories of tampered data. The collected data is divided

in the ratio of 70:30 for training and testing of the proposed EL-based classifier.

TABLE III
SIMULATION ENVIRONMENT

Specification/Parameters	Particulars
Hardware Specification	• 12th Generation Intel Core-i5-12400 CPU • 16 GB RAM • 2.50 GHz clock frequency
Software Environment	• MatLab 2024a (bulding fault detection model) • Hyperledger Fabric 1.3, VMware 14 Pro, Node.js v8.9.1 (for PoAh-based SCR tamper authentication).
HVAC Parameters	• Time, date, day, student strength, area-wise occupancy, classroom floor, orientation, humidity, CO2 levels and power consumption.

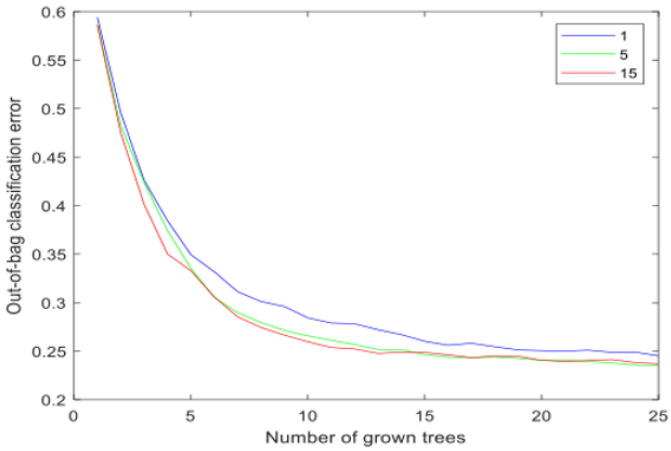

Fig. 3: Classification error at different leaf sizes

A. Subjective Evaluation

Initially, we need to determine the optimal leaf size to build a decision tree (DT) for the ensemble learning (EL)-based classifier. Figure 3 illustrates the classification error across various leaf sizes, indicating that a leaf size of 5 is more efficient than sizes 1 and 15, as it results in the minimum classification error. For this experimental task, we utilized 25 decision trees. Subsequently, we measured the feature importance score using RusBoost-based EL techniques, as highlighted in Figure 4. This figure reveals that feature number 2 (i.e., date) has the least impact on tamper detection, whereas feature 10 (i.e., the average change in power consumption) has the highest impact, scoring around 0.6, which is the highest among all attributes. These steps help reduce programming complexity, training time, and overfitting by eliminating unnecessary features. Figure 5 shows the accuracy level of the proposed tamper detection model with all attributes included and with features like 2 and 5 removed from the training model. The results demonstrate that removing these features has a negligible impact on the model's performance.

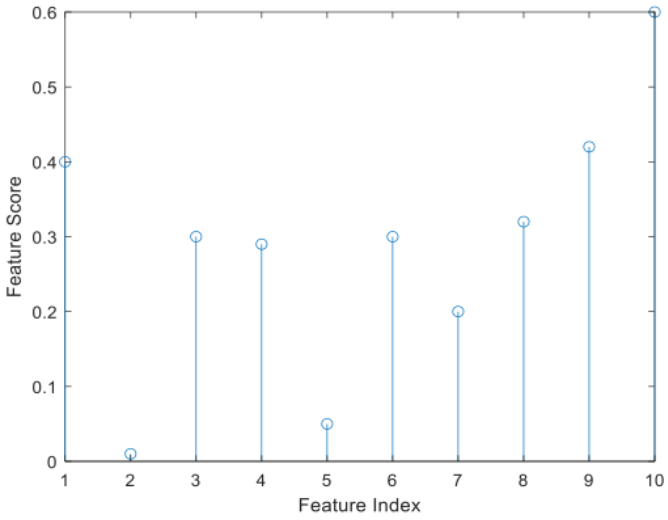

Fig. 4: Feature score of different attributes

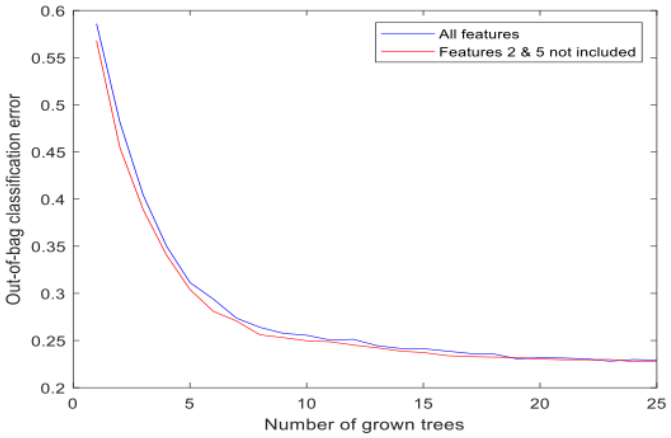

Fig. 5: Classification error at different sets of prediction

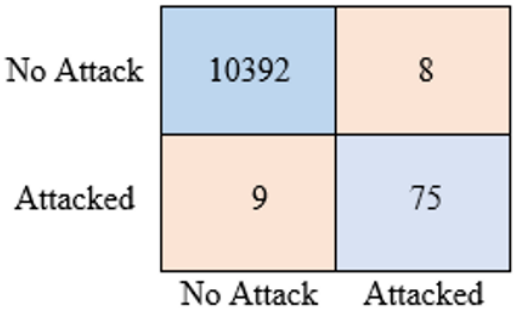

Fig. 6: Confusion matrix of HVAC tampered detection model

Figure 6 presents the confusion matrix of the EL-based HVAC tamper detection model. It highlights both tampered and non-tampered instances, labeled as 'Attacked' and 'No Attack' in the figure. The blue-colored blocks indicate correctly classified events, while the light pale blocks represent misclassified events after testing the proposed tamper detection model. For instance, the total number of 'No Attack' events was 10,400. Out of these, our model correctly predicted 10,392 instances as 'No Attack,' but incorrectly identified 8 instances as 'Attack.' Similarly, the model accurately classified 75 instances as 'Attacked,' but misclassified 9 instances as 'No Attack.'

Table IV.
PERFORMANCE METRICS OF HVAC TAMPERED DETECTION MODEL

TECHNIQUES	ACCURACY	RECALL	SPECIFICITY	PRECISION	FPR	F1-SCORE	MCC
DT	0.9244	0.8433	0.908	0.887	0.0137	0.8085	0.802
PROPOSED DT-BASED EL	0.9984	0.893	0.999	0.904	0.00008	0.898	0.845

TABLE V.
POAH AUTHENTICATION TIME DURATION

Iteration (Number of Transaction)	10	20	30	40	50	60	70	80	90	100
Time (Sec.) in block validation	3.25	3.49	3.93	3.56	3.10	4.10	4.44	3.61	3.94	3.83

TABLE VI.
COMPUTATIONAL COST ANALYSIS

Iterations (Number of Transaction)	Iteration (Number of Transaction)	10	20	30	40	50	60	70	80	90	100
Computational Cost	NON-EL	200	380	490	760	1000	1100	1170	1220	1400	1520
	PROPOSED DT-BASED EL	280	260	470	740	790	880	1010	1120	1350	1500

B. Quantitative Analysis

Similarly, Table IV presents the performance comparison between the proposed DT-based EL model and the conventional DT-based classification model. In addition to accuracy, various performance metrics were evaluated, including recall, specificity, precision, false positive rate (FPR), F1-Score, and Matthews Correlation Coefficient (MCC). These metrics were assessed based on the confusion matrix mentioned in Figure 6. The proposed EL-based model achieved an accuracy of 99.84% (0.9984), significantly outperforming the conventional DT-based classifier, which had an accuracy of 92.44%. Other performance metrics also demonstrate a similar pattern, indicating the superior performance of the EL-based model over the conventional DT-based classifier. The proposed DT-based EL model demonstrates superior performance due to its ability to aggregate multiple DT, thereby reducing overfitting and enhancing overall model robustness and accuracy.

As part of Blockchain Technology, we implemented an extended version of the consensus algorithm, Proof of Authentication (PoAh). To simulate the proposed secure architecture, we utilized six nodes, three of which are trusted nodes in the decentralized and distributed Blockchain network, conducting 100 iterations. Through these iterations, we analyzed performance results and ensured SCR data authentication as gradient values at the intelligent layer, aggregated using an ensemble learning model. Each block size was set to 35 bytes. All network nodes employ public keys to encrypt gradient transactions and create signature certificates using private keys and node IDs assigned to trusted nodes. These trusted nodes validate blocks with authentic signatures using their private keys while deploying their public keys. Upon confirmation, the trusted nodes broadcast the validated blocks to all nodes in the blockchain-based network, ensuring all nodes maintain and validate a replica in their ledger.

The PoAh consensus mechanism facilitates SCR authentication as gradient values, detailed in Table V, based on various transactions over specific time durations. The average time for block gradient authentication using the PoAh consensus mechanism is 3.775 seconds, achieved with up to 100 iterations while adhering to all steps outlined in Algorithm 2 of the proposed framework. Furthermore, we compared the computational cost of the proposed secure SuRaksha framework with traditional architectures (Non-EL), demonstrating its superiority, as presented in Table VI. At 100 iterations, the proposed framework achieves a computational cost of 1500 ms, which is lower than the Non-EL approach (1520 ms), proving its scalability. The computational cost per transaction is defined as:

$$T_{comp} = T_{data} + T_{feature} + T_{EL} + T_{Blockchain} \quad (12)$$

Computational cost are based on the summation of data collection time, feature extraction processing time, ensemble learning inference time, and blockchain (PoAh) authentication time.

C. Discussion

To address the challenge posed by class imbalance, which can affect the model's performance, we employed the RusBoost (Random Undersampling with Boosting) technique. RusBoost effectively mitigates class imbalance by undersampling the majority class while applying adaptive boosting to improve the model's ability to classify minority-class instances. This approach reduces bias by ensuring that the classifier is not overly influenced by the dominant class, thereby enhancing the detection rate for attacks. To evaluate the model's robustness, we assessed its performance using metrics beyond accuracy, such as recall, precision, F1-score, false positive rate (FPR), and Matthews Correlation Coefficient (MCC), ensuring a balanced assessment of performance across both classes. The results demonstrate that our approach maintains high classification performance despite the dataset imbalance, achieving an impressive accuracy of 99.84% with a well-balanced recall and precision.

Furthermore, by integrating authentication within the tamper detection pipeline, we minimized false positives and false negatives caused by compromised or spoofed data sources. In real-time security enforcement, if authentication fails, the system immediately flags suspicious activities, triggering security interventions before HVAC operations can be compromised. Our framework also presents the potential to apply AI-powered ensemble learning (EL) and blockchain-

based authentication to other Smart Classroom (SCR) components, such as smart lighting, interactive whiteboards, and security systems. However, the outcomes may vary due to differences in data characteristics, computational requirements, and operational complexity across these systems. Future work will focus on expanding the dataset to include geographical and diverse environmental conditions and developing an adaptive learning mechanism to enhance the model's performance across varied scenarios. Additionally, optimizing the computational efficiency of the framework will be prioritized to ensure seamless deployment in real-world environments.

IV. Conclusion

In this article, we proposed SuRaksha: An AI-Powered Blockchain Framework for HVAC tamper detection and authentication in Smart Classrooms. Leveraging the capabilities of ensemble learning (EL) at the intelligent and connection layers of the framework, our approach utilizes IoT sensors to gather extensive data from HVAC appliances. The EL algorithms analyze this data in real time to detect tampering instances, while SCR data authentication is ensured through the PoAh consensus algorithm, which aggregates gradient values as part of Blockchain technology. We assessed the framework's performance using metrics such as accuracy, average processing time, recall, precision, FPR, F1-score, MCC, and computational cost, showing significant improvements over existing methods. The proposed framework achieves an average processing time of 3.775 seconds and an accuracy of 99.84%. Future work will focus on enhancing this research by incorporating more SCRs features and advanced algorithms to improve generalization of the proposed framework and reduce the average processing time.

Acknowledgment

This research was supported by a Research Seed Grant from Marwadi University, Rajkot, Gujarat (MU/R&D/22-23/MRP/FT13). The technical aspects were additionally supported by the Center for Communications Technology at London Metropolitan University, London, UK, under the supervision of Prof. Bal Virdee.

References

[1] Zhang, M., & Li, X. (2021). Design of smart classroom system based on Internet of things technology and smart classroom. *Mobile Information Systems*, *2021*(1), 5438878.

[2] Badshah, A., Ghani, A., Daud, A., Jalal, A., Bilal, M., & Crowcroft, J. (2023). Towards smart education through internet of things: A survey. *ACM Computing Surveys*, *56*(2), 1-33.

[3] Singhal, S., Betgeri, S., & Singh, S. K. (2024). Strategies for Mitigating Security Concerns in IoT-Enabled Smart Cities. In *Secure and Intelligent IoT-Enabled Smart Cities* (pp. 239-273). IGI Global.

[4] Zhou, S. L., Shah, A. A., Leung, P. K., Zhu, X., & Liao, Q. (2023). A comprehensive review of the applications of machine learning for HVAC. *DeCarbon*, 100023.

[5] Teng, S. Y., Touš, M., Leong, W. D., How, B. S., Lam, H. L., & Máša, V. (2021). Recent advances on industrial data-driven energy savings: Digital twins and infrastructures. *Renewable and Sustainable Energy Reviews*, *135*, 110208.

[6] Selvaraj, R., Kuthadi, V. M., & Baskar, S. (2023). Smart building energy management and monitoring system based on artificial intelligence in smart city. *Sustainable Energy Technologies and Assessments*, *56*, 103090.

[7] Yayla, A., Świerczewska, K. S., Kaya, M., Karaca, B., Arayici, Y., Ayözen, Y. E., & Tokdemir, O. B. (2022). Artificial intelligence (AI)-based occupant-centric heating ventilation and air conditioning (HVAC) control system for multi-zone commercial buildings. *Sustainability*, *14*(23), 16107.

[8] Ebrahim, M., Hafid, A., & Elie, E. (2022). Blockchain as privacy and security solution for smart environments: A Survey. *arXiv preprint arXiv:2203.08901*.

[9] Khan, H. U., Abbas, M., Alruwaili, O., Nazir, S., Siddiqi, M. H., & Alanazi, S. (2024). Selection of a smart and secure education school system based on the Internet of Things using Entropy and TOPSIS approaches. *Computers in Human Behavior*, 108346.

[10] E. Dimitriadou and A. Lanitis, "A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms," Smart Learning Environments, vol. 10, no. 1, 2023, doi: 10.1186/s40561-023-00231-3.

[11] D. Jianhua, "Optimization of Smart Campus Cybersecurity and Student Privacy Protection Paths Based on Markov Models," Applied Mathematics and Nonlinear Sciences, vol. 9, no. 1, pp. 1–22, 2024, doi: 10.2478/amns.2023.2.01336.

[12] J. Sánchez, A. Mallorquí, A. Briones, A. Zaballos, and G. Corral, "An integral pedagogical strategy for teaching and learning iot cybersecurity," Sensors (Switzerland), vol. 20, no. 14, pp. 1–35, 2020, doi: 10.3390/s20143970.

[13] F. Sharevski, P. Treebridge, and J. Westbrook, "Experiential User-Centered Security in a Classroom: Secure Design for IoT," IEEE Communications Magazine, vol. 57, no. 11, pp. 48–53, 2019, doi: 10.1109/MCOM.001.1900223.

[14] M. S. Abdalzaher, M. M. Fouda, H. A. Elsayed, and M. M. Salim, "Toward Secured IoT-Based Smart Systems Using Machine Learning," IEEE Access, vol. 11, no. February, pp. 20827–20841, 2023, doi: 10.1109/ACCESS.2023.3250235.

[15] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8852–8859, 2020, doi: 10.1109/JIOT.2020.2996425.

[16] M. Kumar, C. Kim, Y. Son, S. K. Singh, and S. Kim, "Empowering Cyberattack Identification in IoHT Networks With Neighborhood-Component-Based Improvised Long Short-Term Memory," IEEE Internet of Things Journal, vol. 11, no. 9, pp. 16638–16646, 2024, doi: 10.1109/JIOT.2024.3354988.

[17] D. Jadav et al., "A Trustworthy Healthcare Management Framework Using Amalgamation of AI and Blockchain Network," Mathematics, vol. 11, no. 3, pp. 1–20, 2023, doi: 10.3390/math11030637.

[18] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545–2554, 2022, doi: 10.1109/JIOT.2021.3077803.

[19] W. Lian, G. Nie, B. Jia, D. Shi, Q. Fan, and Y. Liang, "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," Mathematical Problems in Engineering, vol. 2020, 2020, doi: 10.1155/2020/2835023.

[20] D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks," pp. 1–26, 2020, [Online]. Available: http://arxiv.org/abs/2001.07297

[21] Dutta, J., & Puthal, D. (2024). PoAh 2.0: AI-empowered dynamic authentication based adaptive blockchain consensus for IoMT-edge workflow. *Future Generation Computer Systems*, *161*, 655-672.

[22] M. A. Manolache, S. Manolache, and N. Tapus, "Decision Making using the Blockchain Proof of Authority Consensus," Procedia Computer Science, vol. 199, pp. 580–588, 2021, doi: 10.1016/j.procs.2022.01.071.

[23] G. A. F. Rebello, G. F. Camilo, L. C. B. Guimarães, L. A. C. de Souza, G. A. Thomaz, and O. C. M. B. Duarte, "A security and performance analysis of proof-based consensus protocols," Annales des Telecommunications/Annals of Telecommunications, vol. 77, no. 7–8, pp. 517–537, 2022, doi: 10.1007/s12243-021-00896-2.

[24] Singh, S. K., Kumar, M., Khanna, A., & Virdee, B. (2024). Blockchain and FL-based secure architecture for enhanced external Intrusion detection in smart farming. *IEEE Internet of Things Journal*.