technologies

MDPI

*Article*

# BESS-Enabled Smart Grid Environments: A Comprehensive Framework for Cyber Threat Classification, Cybersecurity, and Operational Resilience

**Prajwal Priyadarshan Gopinath [1], Kishore Balasubramanian [1], Rayappa David Amar Raj [1], Archana Pallakonda [2], Rama Muni Reddy Yanamala [3], Christian Napoli [4,5] and Cristian Randieri [4,6,*]**

[1] Amrita School of Artificial Intelligence, Amrita Vishwa Vidyapeetham, Coimbatore 641112, Tamil Nadu, India; cb.sc.u4aie24214@cb.students.amrita.edu (P.P.G.); cb.sc.u4aie24227@cb.students.amrita.edu (K.B.); rd_amarraj@cb.amrita.edu (R.D.A.R.)
[2] Department of Computer Science and Engineering, National Institute of Technology Warangal, Warangal 506004, Telangana, India; ap23csr1r06@student.nitw.ac.in
[3] Department of Electronics and Communication Engineering, Indian Institute of Information Technology Design and Manufacturing (IIITD&M) Kancheepuram, Chennai 600127, Tamil Nadu, India; yanamalamunireddy@iiitdm.ac.in
[4] Department of Computer, Control, and Management Engineering "Antonio Ruberti", Sapienza University of Rome, 00185 Rome, Italy; cnapoli@diag.uniroma1.it
[5] Department of Computational Intelligence, Czestochowa University of Technology, ul. Dąbrowskiego 69, 42-201 Czestochowa, Poland
[6] Department of Theoretical and Applied Sciences, eCampus University, Via Isimbardi 10, 22060 Novedrate, Italy
* Correspondence: cristian.randieri@uniecampus.it

## Abstract

Battery Energy Storage Systems (BESSs) are critical to smart grid functioning but are exposed to mounting cybersecurity threats with their integration into IoT and cloud-based control systems. Current solutions tend to be deficient in proper multi-class attack classification, secure encryption, and full integrity and power quality features. This paper proposes a comprehensive framework that integrates machine learning for attack detection, cryptographic security, data validation, and power quality control. With the BESS-Set dataset for binary classification, Random Forest achieves more than 98.50% accuracy, while LightGBM attains more than 97.60% accuracy for multi-class classification on the resampled data. Principal Component Analysis and feature importance show vital indicators such as State of Charge and battery power. Secure communication is implemented using Elliptic Curve Cryptography and a hybrid Blowfish–RSA encryption method. Data integrity is ensured through applying anomaly detection using Z-scores and redundancy testing, and IEEE 519-2022 power quality compliance is ensured by adaptive filtering and harmonic analysis. Real-time feasibility is demonstrated through hardware implementation on a PYNQ board, thus making this framework a stable and feasible option for BESS security in smart grids.

**Keywords:** smart grid; distributed energy resources; anomaly detection; total harmonic distortion; artificial neural network; RSA encryption



Academic Editor: Lipo Wang

Received: 21 July 2025
Revised: 13 September 2025
Accepted: 17 September 2025
Published: 20 September 2025

**Citation:** Gopinath, P.P.; Balasubramanian, K.; Raj, R.D.A.; Pallakonda, A.; Yanamala, R.M.R.; Napoli, C.; Randieri, C. BESS-Enabled Smart Grid Environments: A Comprehensive Framework for Cyber Threat Classification, Cybersecurity, and Operational Resilience. *Technologies* **2025**, *13*, 423. https://doi.org/10.3390/technologies13090423



## 1. Introduction

Battery Energy Storage Systems (BESSs) are increasingly becoming part of the operation of smart grids, playing an important role in voltage stabilization, frequency control,

and peak load management, and facilitating integration of renewable energy sources Ref. [1]. However, as BESS infrastructure relies increasingly on IoT devices, cloud platforms, and networked communication systems, its vulnerability to cyber-physical attacks has increased exponentially. This growing reliance has resulted in a novel kind of attack on sensitive systems, leaving critical energy infrastructure exposed to a wide range of cybersecurity threats Ref. [2]. Cyberattacks on BESSs can be generally divided into three main categories, each affecting system stability in distinct ways. The first category includes data integrity attacks such as False Data Injection (FDI) and Bad Data Injection (BDI) that maliciously corrupt critical parameters such as State of Charge (SoC), voltage levels, or power references. The data corruption can mislead the energy management algorithms and result in grid operation disruptions. The second category consists of Denial-of-Service (DoS) attacks that try to saturate or disable communication channels between elements, degrading necessary decision-making or rendering controls unresponsive. The third category is firmware modification attacks, modifying system logic, introducing anomalous behavior, or subverting power quality via voltage instability or harmonic distortion. These threat categories show the diversity of the security issues that smart grids that incorporate BESSs need to address. Although several studies have investigated anomaly detection and intrusion detection systems for mitigating these risks, the majority of the current methods are narrow in scope. Most of them are simply required to perform binary classification between attack and normal types, without the level of specificity required to distinguish between different types of cyberattacks. Furthermore, these models are often trained on unbalanced datasets and do not deal with cryptographic security to secure communication lines. Real-time verification, which is essential for practical deployment, is rarely considered. Here, the current study presents a systematic and applicable approach to protect BESSs from various cyberattacks. The system combines machine learning models for multi-class attack classification, resolves dataset imbalance using SMOTE for binary classification, and interprets features through dimensionality reduction methods like PCA. For protecting data transmission, a double-layer encryption strategy is implemented by combining Elliptic Curve Cryptography (ECC) with a hybrid Blowfish–RSA algorithm. Anomaly detection based on Z-scores and redundancy checks is employed to ensure data integrity, while power quality is dynamically ensured as per IEEE 519-2022 standards via adaptive filtering and harmonic monitoring. The complete design is experimented on in real time with deployment on an edge-computing-based PYNQ-Z2 hardware to establish the proof of feasibility within actual BESS applications. This comprehensive approach covers the deficits in the work carried out heretofore in consolidating the detection of attacks, secure transmission, the integrity of the system, and validation from the hardware as one implementable solution toward increasing BESS–smart grid resilience.

## 2. Literature Review

Battery Energy Storage Systems (BESSs) are a crucial component of contemporary power grids, intelligent distribution networks, and the integration of renewable energy. Their capacity to facilitate frequency regulation, peak load management, and grid stability renders them essential for future energy infrastructures. Nonetheless, the increasing dependency on IoT-based control, cloud computing, and distributed architectures poses significant cybersecurity risks. Cyber threats, such as False Data Injection attacks (FDIA), Denial-of-Service (DoS) attacks, Man-in-the-Middle (MitM) attacks, and firmware modifications, considerably threaten the efficiency of BESSs and the stability of the grid. Multiple studies have investigated cyberattack detection systems, secure communication strategies, and cryptographic solutions to alleviate these risks and improve BESS resilience. The identification of cyberattack surfaces and risk factors in BESSs has been a primary research

subject matter. Ref. [3] introduces AI-driven intrusion detection employing clustering, Artificial Neural Networks (ANNs) Ref. [4], and state estimation (SE) algorithms. This study is deficient in hybrid encryption algorithms, such as AES + RSA or ECC, and lacks real-time implementation, which would be crucial for improved security. Likewise, Ref. [5] examines FDIA, DoS, and firmware attacks, highlighting the significance of blockchain in maintaining data integrity. But it fails to tackle multi-class attack classification, hence constraining its practical applicability.

The anomaly detection approaches based on state estimation, as proposed by Refs. [6,7], enable the identification of long-term patterns in cyberattacks. However, these techniques fail to consider multi-class cyberattack classification, which is essential for recognizing the many attack types influencing BESS operations. Furthermore, Ref. [8] examines load-altering attacks in Automatic Generation Control (AGC)-integrated BESSs utilizing machine-learning-based detection methods. The study is important for grid frequency security research; nevertheless, it lacks secure connection protocols like SSL/TLS or ECC, rendering BESS data transmissions vulnerable to cyber threats. Cyberattacks on BESS operations can severely impair State of Charge (SOC) computation, energy distribution, and overall grid stability. Refs. [9,10] highlight the techniques employed by adversaries to manipulate BESS charge–discharge cycles using ANN-based stealth attacks and AI-driven MitM assaults, leading to unexpected disruptions. Although this research demonstrates the viability of adversarial AI in cyberattacks, it fails to include secure key exchange protocols or encryption-based countermeasures. Machine-learning-driven anomaly detection and intrusion detection systems (IDSs) have been thoroughly investigated for the cybersecurity of BESSs. Comparable concerns regarding the robustness and adaptability of AI-based classifiers under adverse conditions have also been highlighted in the UAV domain, where obstacle and aircraft detection techniques face challenges such as fog, low light, and motion blur Ref. [11]. Refs. [12,13] present ensemble-learning-based detection frameworks that attain accuracy rates of 98.98% and 96.17% for FDIA and DoS attack categorization, respectively. Nonetheless, these models are confined to binary categorization, hence limiting their capacity to identify a broader spectrum of attack types. Furthermore, Ref. [14] presents an AdaBoost-based model for State of Charge forecasting aimed at cyberattack detection. The study shows a 14% false positive rate, highlighting the necessity for enhanced accuracy and cryptographic security validation.

Conversely, Ref. [15] utilizes an autoencoder-based methodology for anomaly detection to identify stealth cyberattacks in actual BESS environments. The study, although effective for real-time cybersecurity monitoring, is deficient in entropy analysis, Chi-square randomness testing, and cryptographic resilience evaluation, rendering it vulnerable to advanced attacks. Traditional AI models mostly emphasize binary anomaly detection; however, recent advances highlight multi-class classification to address a variety of cyber threats. Ref. [16] introduces a Two-Layer Random Forest (TLRF) model for the detection of FDIA, replay attacks, and poisoning attacks, attaining high accuracy with real-world datasets. However, the study excludes encryption-based safeguards, making it prone to unwanted tampering. Despite significant advancements in threat detection, many studies fail to adopt secure data transfer methods. Ref. [17] presents a blockchain-based security framework that uses smart contracts to improve BESS security and reduce single points of failure. Nevertheless, the study fails to incorporate machine-learning-based anomaly detection, which is essential for preemptive cyberattack mitigation. Additionally, Ref. [18] presents a robust multi-agent optimization framework designed to counteract hostile node interference and guarantee secure operation of BESSs. FPGA-based deployment in anomaly detection is discussed in one study that uses parallelism and programmable hardware to provide high-speed, low-latency processing Refs.[19–21]. When it comes to identifying anomalous patterns in massive data streams, these systems effectively support AI/ML

models. This method is appropriate for real-time security and monitoring applications as it maintains a balance between accuracy, throughput, and resource usage. The lack of end-to-end encryption renders real-time data transfer susceptible to attackers. Although cryptographic security is broadly acknowledged as essential, few researchers employ encryption-based countermeasures. Refs. [22,23] address blockchain authentication but do not assess hybrid encryption methods like AES + RSA or ECC. Future research in BESS cybersecurity is expected to benefit from the integration of hybrid encryption techniques with AI-augmented intrusion detection systems, hence facilitating comprehensive end-to-end protection. Simultaneously, exploring lightweight encryption techniques is essential for providing low-latency, real-time monitoring. The current literature predominantly relies on simulated environments; future research is expected to focus on the real-world implementation and validation of attack detection frameworks. Furthermore, integrating BESS security within the comprehensive smart grid cybersecurity framework is crucial for averting substantial and widespread disruptions. Despite breakthroughs in threat modeling, AI-driven anomaly detection, and cryptographic techniques, significant challenges remain, particularly in the execution of hybrid encryption, real-time attack detection, and the evaluation of secure communication protocols. This paper presents a robust, AI-driven framework for detecting attacks associated with cryptographic security, anomaly detection, and real-time secure communication. The development of future technologies depends on the effective execution of adaptive AI-driven security protocols and scalable techniques that enhance the reliability of Battery Energy Storage Systems (BESSs) within smart grids and renewable energy systems. This paper presents a robust, AI-driven framework for detecting attacks associated with cryptographic security, anomaly detection, and real-time secure communication. Progress in the future relies on the effective execution of adaptive AI-driven security protocols and scalable solutions that enhance the reliability of BESSs with smart grids and renewable energy systems. The overview of the proposed work is shown in Figure 1 and addresses all the drawbacks and the highlights, and the major contributions of this paper are as follows:

- This paper proposed a two-layer classification method to detect cyberattacks in BESSs with an accuracy of 99.89% in binary classification with Random Forest and 99.92% in multi-class classification with LightGBM. The Random Forest model was successfully deployed on a PYNQ board, establishing its feasibility for real-time edge-based applications.
- Feature importance was evaluated with PCA and Random Forest and identified SoC, battery power, voltage, and THD as important indicators of attack situations. This allowed for effective dimensionality reduction and enhanced detection rates through importance factor prioritization.
- A secure communication framework was developed, incorporating Elliptic Curve Cryptography (ECC) and hybrid (Blowfish + RSA) methods for encryption of data, ensuring both computational efficiency and effective data confidentiality for BESS systems.
- The proposed encryption methods were validated by rigorous tests, comprising IV uniqueness, bit-flipping resistance, replay attack mitigation, and side-channel protection. Results validated strong security against cryptographic and statistical attacks.
- Power quality was maintained in accordance with IEEE 519 requirements by adaptive filtering and Total Harmonic Distortion monitoring. Data integrity was maintained using anomaly scoring and redundancy checks, facilitating rapid identification of manipulation and system abnormalities.

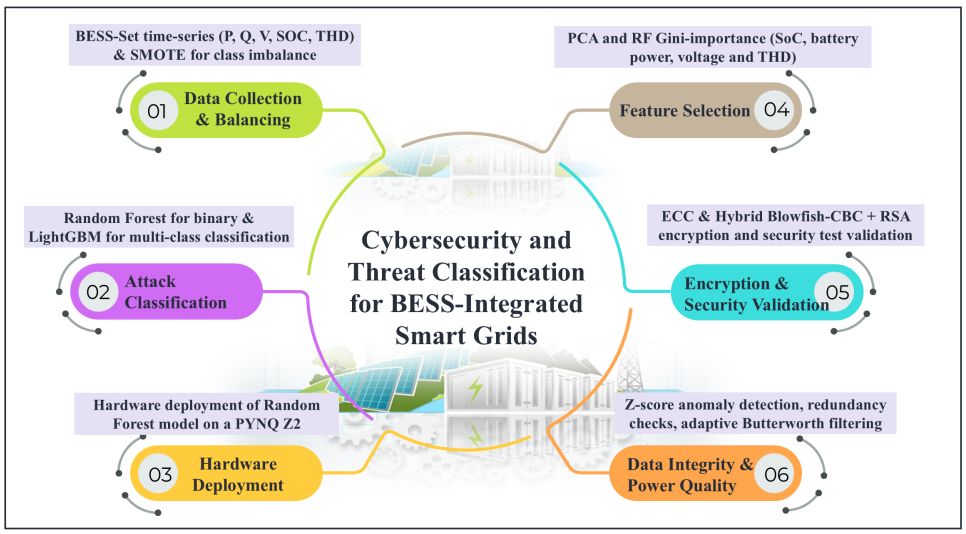


**Figure 1.** Overview of proposed work.

To address these challenges, we utilize the BESS-Set dataset, a high-resolution benchmark recently developed specifically for cybersecurity research in Battery Energy Storage Systems. It is tailored to capture both normal operations and diverse cyberattack scenarios, including False Data Injection, Bad Data Injection, and firmware tampering. The comprehensive labeling of operational parameters (voltage, SoC, THD, power flows) make it particularly suitable for developing and validating machine-learning-driven intrusion detection systems. The dataset facilitates exploration of advanced hybrid detection techniques while filling the critical empirical validation gap. The following section demonstrates the features of the dataset and its use in the suggested methodology. While this study focuses on the cybersecurity of Battery Energy Storage Systems (BESSs), it is important to emphasize that such vulnerabilities are not unique to BESSs but reflect a broader challenge across IoT ecosystems. The integration of distributed devices, cloud platforms, and edge controllers in IoT environments exposes critical infrastructures to similar categories of attacks, including False Data Injection, Denial-of-Service, and firmware modifications. Consequently, new security paradigms are required that combine AI-driven threat detection with robust cryptographic mechanisms. Recent approaches, such as blockchain-enabled cybersecurity frameworks using Elliptic Curve Cryptography (ECC) and the black-winged kite model Ref. [24], highlight the potential of integrating decentralized trust, lightweight cryptography, and adaptive AI models. Our proposed framework aligns with these advancements by integrating machine learning for multi-class attack detection with cryptographic safeguards, thus contributing not only to BESS security but also offering insights applicable to the wider IoT security landscape.

## 3. Dataset Description

The BESS-Set dataset Ref. [25] is a thoroughly organized and broad time-series dataset developed to promote cybersecurity research in Battery Energy Storage Systems (BESSs). The growing integration of Distributed Energy Resources (DERs) into modern smart grids has led to increased cybersecurity concerns about energy storage components. BESS-Set is designed to facilitate the development of robust cybersecurity solutions, encompassing intrusion detection systems (IDSs), anomaly detection algorithms, and attack mitigation tactics, which are essential resources for researchers and professionals. The dataset consists of multiple CSV files, each representing a distinct operational scenario that includes both normal system operations and various cyberattacks. The BESS-Set dataset is sampled

at 1-second intervals, recording important operating parameters such as active power (P), reactive power (Q), battery voltage, Total Harmonic Distortion (THD), and State of Charge (SOC). Each data point is assigned a binary label indicating the presence of an attack: 0 indicates normal operation, while 1 indicates the presence of a cyberattack. This labeling schema facilitates the utilization of supervised learning methods for anomaly and attack detection. The dataset comprises nine files classified into normal data and diverse cyberattack scenarios. A summary of various attack types, their classifications, and descriptions is provided in Table 1. The detailed description of each feature (column) in the dataset is provided in Table 2. The BESS-Set dataset used in this study is simulated and is specifically designed for research purposes. It offers high-resolution, well-labeled data that is ideal for exploring anomaly detection and attack classification. However, it does not fully reflect the challenges of real-world BESS installations, such as noisy sensor data, communication delays, and hardware faults. While our results show the strong potential of the proposed framework, validating it on real BESS testbeds will be an important step in future work to confirm its robustness in practical conditions.

**Table 1.** BESS-Set: attack categories and characteristics.

| Cyberattack | Attack Name | Type | Description |
|---|---|---|---|
| Bad Data Injection | BadData_P_Exceeds | P Exceeds Limits | Active power setpoints exceed safe operational thresholds, causing instability. |
| | BadData_Q_Exceeds | Q Exceeds Limits | Reactive power manipulated beyond limits, affecting voltage and power quality control. |
| | BadData_P_Oscillations | P Oscillations | Active power fluctuates due to Man-in-the-Middle (MitM) attack, destabilizing grid performance. |
| | BadData_Q_Oscillations | Q Oscillations | Reactive power oscillations disrupt voltage control and system balance. |
| False Data Injection | FalseData_P_Tampering | P Tampering | False active power readings mislead system operation and response algorithms. |
| | FDI_BDI_SOC_Tampering | SOC Tampering | Alters State of Charge (SOC) values, causing incorrect decisions in battery energy management. |
| Firmware Modification | Firmware_Harmonics_Tampering | Tampering | Firmware manipulation introduces harmonic distortions, potentially violating IEEE power quality standards. |
| | Battery Voltage Tampering | Voltage Tampering | DC/DC converter parameters are modified, increasing the risk of overvoltage and battery degradation. |

**Table 2.** BESS-Set CSV column names and descriptions.

| Category | Column Name(s) | Unit/Type | Description |
|---|---|---|---|
| Battery State | SoC | % | State of Charge of the battery, indicating energy level. |
| DC Measurements | V_dc_bat, I_dc_bat | V, A | DC voltage and current at the battery terminals. |
| | V_dc_link | V | Voltage of the DC link connecting battery and inverter. |
| AC Voltage | V_a, V_b, V_c | V | Line voltages on phases A, B, and C. |
| AC Current | I_a, I_b, I_c | A | Line currents on phases A, B, and C. |
| Frequency | f_a, f_b, f_c | Hz | Frequency measurements on each AC phase. |
| Harmonics | THD_a, THD_b, THD_c | % | Total Harmonic Distortion on phases A, B, and C. |
| Power (Battery) | P_bat, Q_bat | kW, kVAR | Active and reactive power delivered by the battery. |
| Power Reference | P_ref, Q_ref | kW, kVAR | Control system reference setpoints for active and reactive power. |
| Label | label | Categorical | Classification label (e.g., normal, cyberattack type). |

## 4. Proposed Methodologies

This section outlines the techniques and algorithms used, with a focus on balancing the data, classifying attacks, implementing hardware, and ensuring secure communication. For the classification component, several models including Support Vector Machines (SVMs), Artificial Neural Networks (ANNs), TabNet, XGBoost, Random Forest, and LightGBM were initially evaluated on the BESS-Set dataset. As detailed in the Results and Discussion section, Random Forest achieved the best performance for binary classification (99.89% accuracy), while LightGBM yielded the highest accuracy for multi-class classification (99.92%). These

models were therefore selected as the most suitable for the proposed framework, as they combine high accuracy with relatively low computational cost, making them appropriate for real-time embedded classification on platforms such as the PYNQ-Z2. To address class imbalance, Synthetic Minority Oversampling Technique (SMOTE) was applied to both binary and multi-class tasks. For binary classification, oversampling was applied, while for the multi-class LightGBM model, a hybrid resampling strategy was adopted, oversampling minority classes using SMOTE and undersampling majority classes to achieve a balanced training dataset of approximately 10,000 samples per class. Prior investigations in related computer vision applications have highlighted the sensitivity of CNN-based classifiers to dataset structure, emphasizing the need for dataset-specific optimization and validation procedures Ref. [26]. This observation is consistent with findings showing that CNN-based forgery detection systems exhibit substantial performance variability depending on dataset characteristics Ref. [27], further supporting the argument that dataset dependency must be carefully accounted for in security-oriented ML frameworks.

For secure communication, two cryptographic strategies were incorporated. Elliptic Curve Cryptography (ECC) (ECDH + HKDF + XOR) was selected for lightweight key agreement due to its ability to provide strong security with smaller key sizes compared to RSA, thereby reducing computational overhead in communication scenarios. In addition, a hybrid scheme combining Blowfish–CBC for data encryption and RSA (1024-bit) for secure key exchange was implemented. Blowfish was chosen for its fast encryption/decryption speed and flexible key length, while RSA ensured secure distribution of symmetric keys. This dual approach balances efficiency and security, aligning with industrial standards for protecting sensitive BESS operational data.

### 4.1. Synthetic Minority Oversampling Technique (SMOTE) for Data Balancing

An approach to mitigate class imbalance involves generating synthetic instances for the minority class instead of merely replicating existing samples. Our original training set was highly imbalanced, with 24.859 'normal' samples versus only 3.012 attack samples. After applying SMOTE (random_state = 42), it achieved perfect balance (24.859 samples per class), ensuring that minority-class patterns receive equal representation during tree construction. The algorithm operates by selecting each sample from the minority class and determining its $k$-nearest neighbors inside the feature space. For each chosen minority instance $\mathbf{x}_i$, one of its nearest neighbors $\mathbf{x}_{nn}$ is randomly selected, and a new synthetic sample is created along the line segment connecting these two places. This process is mathematically represented by Equation (1), where $\lambda$ is a random variable sampled from a uniform distribution ranging from 0 to 1. This guarantees that the new data point is a convex combination of the original sample and its neighbor, hence facilitating interpolation between them. Random interpolation enhances the dataset by generating novel minority samples that are not just replicas, while also facilitating a more effective representation of the underlying data distribution. The Euclidean distance employed to ascertain the nearest neighbors is generally computed using Equation (2), where $n$ signifies the number of features in the dataset. Through these mathematical formulations, SMOTE develops various synthetic instances that assist in balancing the dataset, strengthening the training process, and eventually resulting in more robust and unbiased machine learning models. Smote technique process is shown in Figure 2.

$$\mathbf{x}_{new} = \mathbf{x}_i + \lambda \times (\mathbf{x}_{nn} - \mathbf{x}_i) \tag{1}$$

$$d(\mathbf{x}_i, \mathbf{x}_{nn}) = \sqrt{\sum_{j=1}^{n} (x_{i,j} - x_{nn,j})^2} \tag{2}$$

While SMOTE creates synthetic samples uniformly across the line segments between minority class instances and their nearest neighbors, it fails to learn local data distributions. In contrast, ADASYN generates synthetic data dynamically in areas where the minority class is more difficult to learn (i.e., areas with more class overlap). This renders it more efficient in cases of severe class imbalance. Moreover, Cluster-SMOTE initially clusters the minority class and afterwards carries out SMOTE within clusters so that the synthesized samples get improved distribution and diversity, particularly if the minority class contains sub-clusters or sparse patterns.

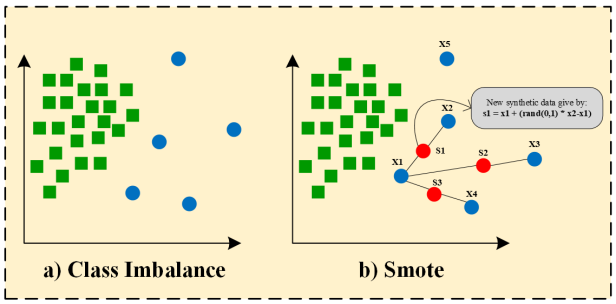


**Figure 2.** Smote technique process.

### *4.2. Random Forest for Classification*

Random Forest is a resilient ensemble learning technique commonly employed for classification problems, including binary classification within the BESS dataset. It constructs several decision trees utilizing bootstrapped subsets of the original dataset and integrates their predictions via a majority voting process to enhance accuracy and generalization. Every singular decision tree within the forest partitions the data according to a purity criterion, predominantly the Gini impurity. The Gini impurity for a dataset $D$ is computed using Equation (3), where $p_i$ represents the proportion of occurrences in class $i$, and $k$ signifies the total number of classes. At each decision node, the algorithm randomly chooses a subset of features instead of evaluating all available features. This not only increases its unpredictable nature, which disrupts the correlation among the trees, but also fortifies the ensemble's resilience. The number of features evaluated at each split is generally specified by Equation (4), where $p$ represents the total number of features.

The ultimate prediction $\hat{y}$ is derived by consolidating the predictions from all $B$ decision trees through a majority voting mechanism, as seen in Equation (5). This ensemble method minimizes uncertainty and promotes predictive stability. Additionally, Random Forest utilizes Out-of-Bag (OOB) error estimation, utilizing the subset of training samples excluded from the bootstrap sample for each tree to deliver an unbiased assessment of model performance. This eliminates the necessity for a distinct validation set and ensures efficient model assessment. Random Forest incorporates bagging with random feature selection, resulting in higher accuracy, diminished overfitting, and robustness, rendering it particularly effective for classification jobs involving intricate and high-dimensional data, such as cybersecurity monitoring of BESSs. The key hyperparameters used for Random Forest training are summarized in Table 3. Random forest architecture is shown in Figure 3.

$$\text{Gini}(D) = 1 - \sum_{i=1}^{k} p_i^2 \tag{3}$$

$$m = \sqrt{p} \tag{4}$$

$$\hat{y} = \text{mode}\{f_1(x), f_2(x), \ldots, f_B(x)\} \tag{5}$$

**Table 3.** Key hyperparameters used in training.

| Model | Hyperparameter | Value (Used) |
|---|---|---|
| Random Forest (binary) | n_estimators | 100 |
| | max_depth | 10 |
| | random_state | 42 |
| | preprocessing pipeline | Imputer → StandardScaler → SMOTE |
| | cross-validation | Stratified 10-fold CV |
| LightGBM (multi-class) | objective | `multi-class` |
| | num_class | set to #classes in dataset |
| | metric | `multi_logloss` |
| | boosting_type | `gbdt` |
| | learning_rate | 0.1 |
| | num_leaves | 31 |
| | max_depth | −1 (no limit) |
| | seed | 42 |
| | num_boost_round | 100 |
| | early_stopping_rounds | 10 |

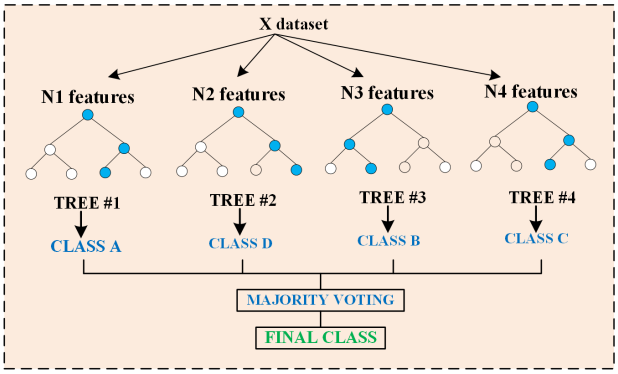


**Figure 3.** Random Forest architecture.

### *4.3. LightGBM for Multi-Class Classification*

LightGBM is a gradient boosting framework that constructs decision trees in a leaf-wise manner with depth boundaries, intended for efficiency and speed. The model's prediction for an input instance $x$ is an average of predictions from $T$ distinct trees, as seen in Equation (6). The learning process is directed by the minimization of a regularized objective function that addresses prediction error and model complexity, as expressed in Equation (7).

$$f(x) = \sum_{t=1}^{T} f_t(x) \tag{6}$$

$$L = \sum_{i=1}^{n} \ell(y_i, f(x_i)) + \sum_{t=1}^{T} \Omega(f_t) \tag{7}$$

In each boosting iteration, LightGBM utilizes a second-order Taylor approximation of the loss function to facilitate efficient optimization, integrating both gradient and Hessian information. Although the derivations involve detailed gradient-based computations (omitted here for brevity), they contribute to optimal split selection during tree construction.

For a tree with $J$ leaves, the ideal weights are determined based on aggregated gradients and Hessians from training samples. The quality of a split is assessed by a gain metric, which reflects the improvement in the loss function when splitting a node. These optimization steps, though mathematical in formulation, are abstracted by the LightGBM framework during training.

We employed stratified 10-fold cross-validation to evaluate model performance. The folds preserved class distribution and were repeated with different splits to ensure robust-

ness. Performance metrics were reported as mean ± standard deviation across all folds. The LightGBM training configuration, including learning rate, tree depth, and number of boosting rounds, is listed in Table 3. LightGBM architecture is shown in Figure 4.

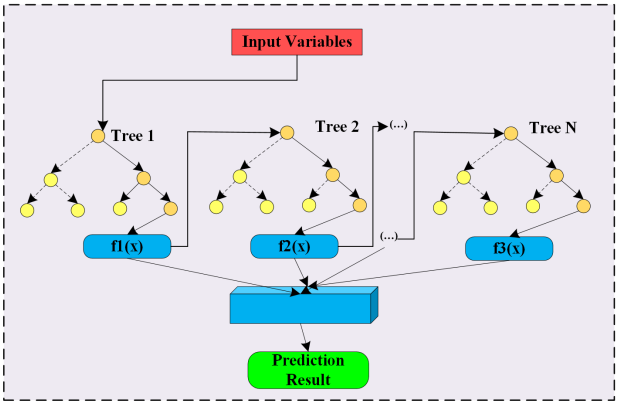


**Figure 4.** LightGBM architecture.

### *4.4. Principal Component Analysis (PCA) for Dimensionality Reduction*

Principal Component Analysis (PCA) is a statistical approach that diminishes the dimensionality of a dataset while preserving maximal variability. It achieves this by converting the original characteristics into a new set of uncorrelated variables referred to as principal components. The procedure commences with mean subtraction to center the data, followed by the calculation of the covariance matrix of the centered data. For a dataset $X$ comprising $n$ samples and $p$ characteristics, the covariance matrix is computed using Equation (8).

$$Sigma = \frac{1}{n-1} X^{\top} X \tag{8}$$

PCA entails conducting eigenvalue decomposition on the covariance matrix to obtain eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_p$ and their corresponding eigenvectors $v_1, v_2, \ldots, v_p$, which fulfill the requirement specified in Equation (9).

$$\Sigma v_i = \lambda_i v_i \tag{9}$$

The eigenvectors denote the orientations of the new feature space (principal components), whilst the eigenvalues signify the extent of variance encapsulated by each respective component. A transformation matrix $W$ is formed by picking the top $k$ eigenvectors corresponding to the biggest eigenvalues. The original dataset $X$ is projected onto the lower-dimensional subspace, yielding the reduced matrix $Z$, as seen in Equation (10).

$$Z = XW \tag{10}$$

To evaluate the efficiency of the chosen components in capturing data variance, the explained variance ratio (EVR) is calculated, which is the ratio of the sum of the top $k$ eigenvalues to the total sum of all $p$ eigenvalues. EVR is defined as the ratio of the sum of the first $k$ eigenvalues $\lambda_i$ to the sum of all $p$ eigenvalues $\lambda_j$. This ratio aids in figuring out how many components should be kept in order to ensure that the dimensionality reduction preserves the important data from the original dataset.PCA architecture is shown in Figure 5.

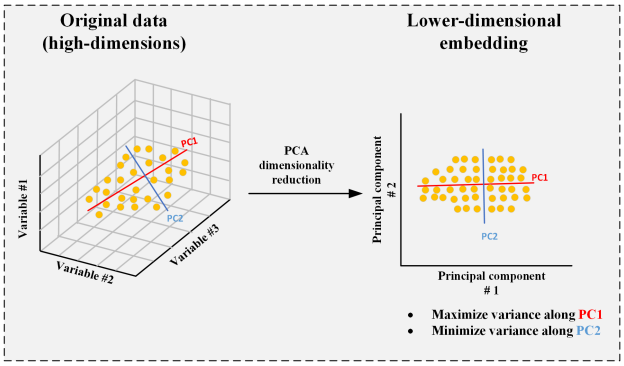


**Figure 5.** PCA for dimensionality reduction.

### *4.5. Elliptic-Curve-Cryptography-Based Encryption*

Elliptic Curve Cryptography (ECC) relies on the algebraic framework of elliptic curves constructed over finite fields. An elliptic curve is defined by a short Weierstrass form as presented in Equation (11) accompanied with the discriminant condition specified in Equation (12), which assures the curve's nonsingularity:

$$y^2 = x^3 + ax + b, \tag{11}$$

$$\Delta = 4a^3 + 27b^2 \neq 0, \tag{12}$$

In a finite field $\mathbb{F}_p$ (where $p$ is a prime), the collection of points $(x, y)$, together with a point at infinity, defines an abelian group under a specified addition operation. For the two distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, the slope $\lambda$ is determined using Equation (13), and the resultant point $R = P + Q = (x_3, y_3)$ is derived using Equations (14) and (15).

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p, \tag{13}$$

$$x_3 = \lambda^2 - x_1 - x_2 \mod p, \tag{14}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \mod p. \tag{15}$$

If the two points are the same, i.e., $P = Q$, the process is called point doubling, and the slope $\lambda$ is computed using Equation (16), with the coordinates of the doubled point given by Equations (17) and (18).

$$\lambda = \frac{3x_1^2 + a}{2y_1} \mod p, \tag{16}$$

$$x_3 = \lambda^2 - 2x_1 \mod p, \tag{17}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \mod p. \tag{18}$$

Key generation in ECC involves selecting a private key $d$ uniformly at random from the interval $[1, n-1]$, where $n$ is the order of a predefined base point $G$. The corresponding public key is calculated using Equation (19).

$$Q = d \cdot G, \tag{19}$$

Scalar multiplication is executed within the elliptic curve group. The security of ECC depends on the complexity of the Elliptic Curve Discrete Logarithm Problem (ECDLP), making it computationally impractical to determine $d$ from the known values of $Q$ and $G$. In an ECC-based key exchange protocol, two parties develop a shared secret through the combination of their private and public keys, such that $S = d_1 \cdot Q_2 = d_1 d_2 \cdot G = d_2 \cdot Q_1$, which is then processed via a key derivation function (e.g., HKDF) to produce symmetric encryption keys. This secure communication protocol is illustrated in Figure 6, depicting an ECC-based key exchange. Additionally, Figure 7 illustrates the full encryption flow of the modified ECC scheme, showcasing each phase from key generation to encryption and decryption. This efficient mathematical framework makes ECC a secure choice for cryptographic applications. The modified ECC algorithm is explained in Algorithm 1.

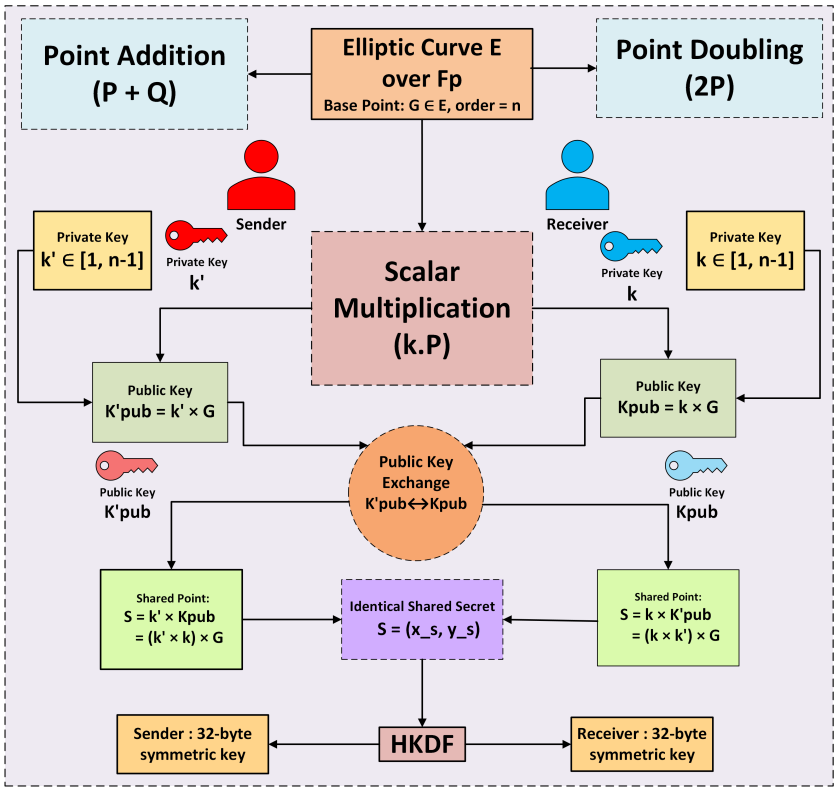


**Figure 6.** ECC protocol: Secure communication using ECDH key exchange.

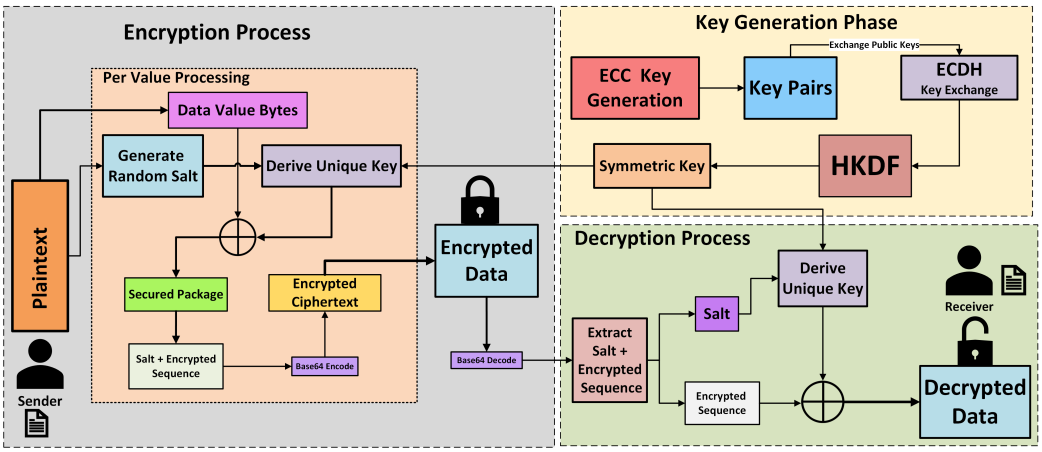


**Figure 7.** Encryption numerical order. Flow of modified ECC.

**Algorithm 1** Modified ECC encryption.

**Require:** Plaintext data $D$ to be encrypted, Receiver's public key $K_{pub}$
**Ensure:** Encrypted data $E_D$, Decrypted data $D$
**Key Generation:**
Generate Receiver's ECC key pair: $(K_{priv}, K_{pub})$
Generate Sender's ECC key pair: $(K'_{priv}, K'_{pub})$
**Encryption Process:**
Compute shared secret: $S = \text{ECDH}(K'_{priv}, K_{pub})$
Derive symmetric key $K_s$ from $S$ using a key derivation function (KDF)
Encrypt data $D$ using $K_s$ to get $E_D$
**Secure Transmission:**
Transmit $E_D$ and $K'_{pub}$ to Receiver
**Decryption Process:**
Compute shared secret: $S = \text{ECDH}(K_{priv}, K'_{pub})$
Derive symmetric key $K_s$ using the same KDF
Decrypt $E_D$ using $K_s$ to retrieve $D$
Verify confidentiality and integrity during transmission and storage
Display "ECC-Based Encryption and Decryption Process Completed"

### *4.6. Modified Hybrid Encryption Using Blowfish and RSA*

The proposed hybrid encryption approach combines symmetric and asymmetric cryptographic algorithms to achieve both efficiency and security. Let $P$ signify the plaintext data desired for transmission, $K_B$ symbolize the Blowfish secret key (448 bits), and $C$ the resultant ciphertext.

The plaintext is initially encrypted with the Blowfish technique, known for its speed and effectiveness in symmetric encryption. The encrypted output is provided by Equation (20).

$$C = E_B(P, K_B) \tag{20}$$

where $E_B$ denotes the Blowfish encryption function.

Following this, the Blowfish key $K_B$ itself must be securely transmitted. For this purpose, RSA public key encryption is employed. In RSA, a pair of keys is generated: a public key $(e, N)$ and a private key $(d, N)$. The modulus $N$ is computed as the product of two large primes $p$ and $q$, i.e., $N = p \times q$, and the totient function is given by $\phi(N) = (p-1)(q-1)$. The public exponent $e$ is chosen such that $1 < e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$. The private exponent $d$ is calculated to satisfy the modular inverse relation shown in Equation (21).

$$d \times e \mod \phi(N) = 1 \tag{21}$$

Using the RSA public key, the symmetric key $K_B$ is encrypted as described in Equation (22):

$$K_B^{\text{encrypted}} = K_B^e \mod N \tag{22}$$

The encrypted message comprises the ciphertext and the RSA-encrypted symmetric key, transmitted together as a pair, as seen in Equation (23).

$$\left(C, K_B^{\text{encrypted}}\right) \tag{23}$$

Upon receiving it, the recipient initiates the decryption process by obtaining the Blowfish key via their RSA private key, as seen in Equation (24).

$$K_B = (K_B^{\text{encrypted}})d \mod N \tag{24}$$

Upon retrieval of the original symmetric key, the ciphertext is decoded via the Blowfish decryption function, giving the original plaintext $P$. In the equation $P = D_B(C, K_B)$, $D_B$ denotes the Blowfish decryption function.

The comprehensive encryption process of this hybrid system is illustrated in Figure 8, which shows the integration of symmetric and asymmetric methods for secure communication.Hybrid Encryption is explained in Algorithm 2.

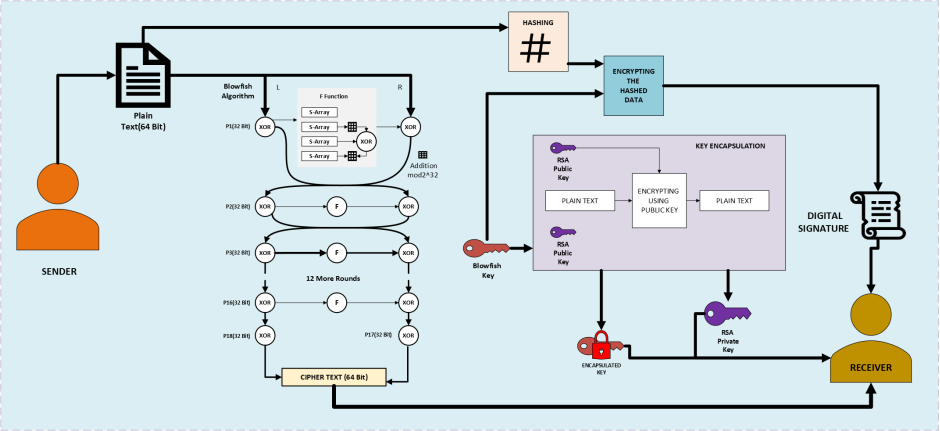


**Figure 8.** Encryption flow of proposed hybrid encryption (Blowfish + RSA).

### *4.7. Authentication Techniques*

In addition to the encryption algorithm, authentication protocols were added to further protect data integrity. Digital signatures were employed with RSA, which offered a way to ensure that the data was not modified during transmission. Concurrently, HMAC (Hash-Based Message Authentication Code) was used to authenticate message origin and guarantee that any attempt to tamper with the ciphertext could be detected with certainty. The verification process established that both HMAC and the digital signature always cleared the integrity checks, thus reaffirming the reliability of the data transfer process.

**Algorithm 2** Hybrid encryption using Blowfish and RSA

**Require:** Plaintext $P$
**Ensure:** Ciphertext $C$, Encrypted key $E_{K_b}$

▷ Symmetric Key Generation

Generate Blowfish key $K_b \in \{0,1\}^{448}$

▷ RSA Key Generation

Choose large primes $p, q$
Compute modulus $N \leftarrow p \cdot q$
Compute $\phi(N) \leftarrow (p-1)(q-1)$
Choose $e$ such that $\gcd(e, \phi(N)) = 1$
Compute $d$ such that $e \cdot d \equiv 1 \pmod{\phi(N)}$
Public key $\leftarrow (e, N)$, Private key $\leftarrow (d, N)$

▷ Encryption

Encrypt plaintext: $C \leftarrow \mathcal{B}_{K_b}(P)$
Encrypt key: $E_{K_b} \leftarrow K_b^e \bmod N$

▷ Transmission

Transmit tuple $(C, E_{K_b})$

▷ Decryption

Receive $(C, E_{K_b})$
Decrypt key: $K_b \leftarrow E_{K_b}^d \bmod N$
Decrypt ciphertext: $P \leftarrow \mathcal{B}_{K_b}^{-1}(C)$
**return** Plaintext $P$

### 4.8. Integration of Machine Learning and Cryptographic Modules

During feature selection based on Principal Component Analysis (PCA), factors like State of Charge (SoC), Total Harmonic Distortion (THD), and DC-link voltage ($V_{dc_link}$) were found to be significantly impactful for anomaly classification. These are variables, because of their sensitive nature in the monitoring of the functioning state of the Battery Energy Storage System (BESS), that should be kept secure from tampering, interception, or misuse. To meet these security needs, our design uses a modular integration approach where machine learning and crypto pieces operate in series. The first step involves training and evaluation of classification models like LightGBM and Random Forest on plaintext data. This is done to maintain complete interpretability and achieve the best possible model performance with no interference due to encryption artifacts. Once classified, it provides outputs like predicted labels or diagnostic anomalies. The results are treated securely by the cryptographic module. The module makes use of two main schemes:

- Elliptic Curve Cryptography (ECC): Light asymmetric encryption for secure transmission in resource-starved environments.
- Hybrid Encryption (Blowfish + RSA): Merges symmetric encryption (Blowfish) for data protection at high speeds with RSA to securely pass the encryption keys.

By delaying encryption until after the machine learning operation, our solution maintains model effectiveness without compromising strong security during data storage or transfer. Flexible deployment is made possible across varied operational scenarios, adopting ECC for embedded or edge deployments and hybrid cryptography for cloud or high-throughput environments. The concept of adaptive human–machine interfaces has been successfully explored in embedded systems, suggesting potential extensions of similar interaction paradigms for real-time BESS control applications Ref. [28].

## 5. Results and Discussion

The research data was obtained from the BESS-Set dataset with the objective of identifying cyberattacks via machine learning while maintaining the confidentiality of data by using encryption techniques. Significantly, the classification models only process unencrypted data to maintain complete access to features and guarantee the best model accuracy. Encryption is only used after classification, protecting sensitive results upon storage or transmission. This division guarantees strong analytic performance while protecting the system outputs. Section 5.1 addresses attack categorization, with Section 5.1.1 devoted to binary classification separating normal from anomalous conditions and Section 5.1.2 addressing multi-class classification, detecting particular categories of cyberattacks. Section 5.1.3 reports the hardware implementation, where the top performer model is executed on the PYNQ-Z2 edge platform, demonstrating its performance under real-time conditions. Section 5.2 includes Feature Analysis and Section 5.3 includes Adversarial Attack analysis. Section 5.4 introduces the implementation of encryption methods for security in data, analyzes the strength and overhead of the implemented encryption algorithm. Section 5.5 includes another security analysis of this combination. Section 5.6 discusses power quality and harmonics, wherein we analyze how attacks and conditions influence electrical parameters in the BESS.

### 5.1. Attack Classification

The attack classification section of the proposed work is designed to accurately identify and categorize cyberattacks targeting BESSs. It employs supervised machine learning techniques to distinguish malicious activities across both binary and multi-class classification scenarios.

5.1.1. Binary Classification

Binary classification is a supervised learning method used to classify data into two distinct classes, e.g., attack or normal. The performance of various algorithms, i.e., SVM, ANN, Tabnet, XG Boost, and Random Forest, is shown in Table 4, whereas their confusion matrices are shown in Figure 9. Among all the models, on the held-out test set (20% of data), the Random Forest attained an overall accuracy of 99.89% because of its ability to manage extensive feature sets and prevent overfitting. XGBoost achieved an accuracy of 99.38% with gradient boosting to handle complex data patterns. The Artificial Neural Network (ANN) reached an accuracy of 97.09% by the identification of complex patterns, requiring extensive hyperparameter modification. The SVM exhibited strong performance with high-dimensional data, achieving an accuracy of 97.4%, but its computational cost restricted its capacity to handle larger datasets. Furthermore, other techniques, including TabNet, were also tested. Among all the approaches, Random Forest yielded the highest accuracy of 99.89% and F1-score of 99.94% among all tested models, indicating its superior balance between precision and recall. By aggregating predictions from several trees (bagging), it effectively reduces variance and overfitting on the limited, structured BESS data, leading to stable classification. Its precision, 99.95%, and recall, 99.93%, reflect Random Forest's ability to both minimize false alarms and detect nearly all attack instances. To ensure robustness and evaluate the stability of the model, a k-fold cross-validation (with k = 10) was conducted, computing the mean and standard deviation of key classification metrics such as accuracy, precision, recall, and F1-score. The performance of ML models, including Random Forest, XGBoost, and SVM, compared to DL models like ANN and Tabnet in the present study, is mostly due to the structured and limited size of the BESS data, allowing traditional ML models to effectively identify patterns without the necessity for large-scale data, in contrast to DL models that perform better with extensive data.

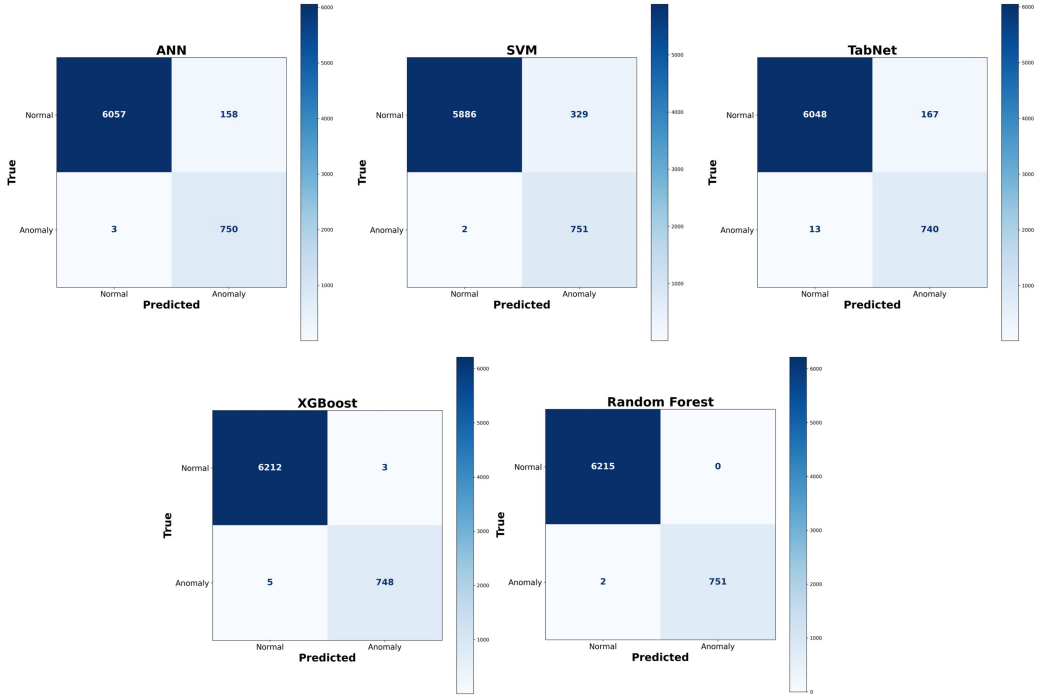


**Figure 9.** Confusion matrix for binary classification.

**Table 4.** Performance metrics for binary classification.

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| XG Boost | 99.38 | 99.94 | 99.93 | 99.91 |
| SVM | 97.40 | 98.95 | 97.50 | 98.00 |
| ANN | 97.09 | 97.00 | 95.00 | 98.00 |
| Tabnet | 96.18 | 97.18 | 96.18 | 96.43 |
| Random Forest | 99.89 | 99.95 | 99.93 | 99.94 |

#### 5.1.2. Multi-Class Classification

Multi-class classification was employed to categorize eight attack types (see Table 5), plus one 'normal' class, for a total of nine classes. The performance of different models, including LightGBM, Random Forest, Cat Boost, and ANN, is shown in Table 5 and their confusion matrices are shown in Figure 10. Among the models, on the held-out test set (20% of data) LightGBM attained an accuracy of 99.92% and a 99.96% F1-score, outperforming other gradient-boosted and ensemble methods in distinguishing between multiple attack types, owing to its efficient management of extensive feature sets and accelerated training speed. It focuses on leaf-wise tree construction which splits the most error-prone regions, enabling finer discrimination between overlapping attack classes with fewer iterations. LightGBM delivers fast convergence and precise class separation, as evidenced by its precision of 99.95% and recall of 99.97%. A k-fold cross-validation (k = 10) was employed to ensure balanced representation of all classes across folds. The ANN effectively identified complex patterns among features; it required more comprehensive data for maximum performance. The Random Forest algorithm achieved commendable classification accuracy, although it showed less ability to distinguish between overlapping assault types. Cat Boost (98.07%) provided good results by using ensemble methods to reduce variance and provide stability. Model choice ultimately comes down to making trade-offs among accuracy, interpretability, and computation. Overall, all models were fine, but LightGBM was the best as it handled the structure of the data flawlessly, whereas ANN, though less accurate, still demonstrated its effectiveness in learning sophisticated features.

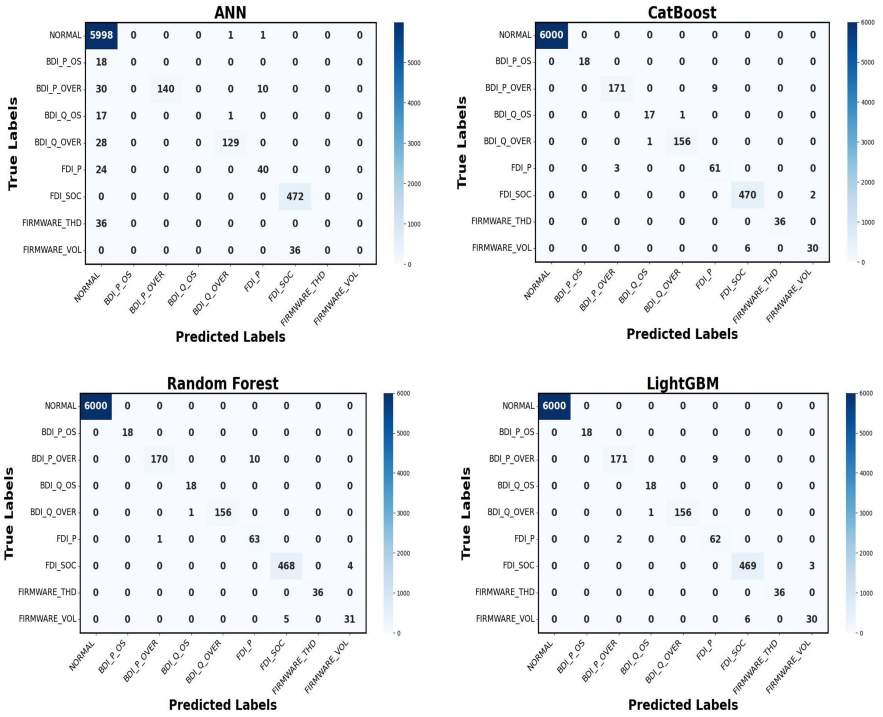


**Figure 10.** Confusion matrix for multi-class classification.

**Table 5.** Performance metrics for multi-class classification.

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| ANN | 98.53 | 95.00 | 98.00 | 96.00 |
| Random Forest | 99.58 | 99.67 | 99.90 | 99.78 |
| Cat Boost | 98.07 | 99.00 | 98.00 | 98.00 |
| Light GBM | 99.92 | 99.95 | 99.97 | 99.96 |

#### 5.1.3. Hardware Implementation of ML-Model-Based Binary Classification on in PYNQ Z2 Board

To evaluate the practical feasibility of our proposed Random Forest model, we deployed it on an Xilinx Zynq-7000 SoC (ARM Cortex-A9 @ 650 MHz, 512 MB RAM) using the PYNQ-Z2 edge computing platform, as illustrated in Figure 11. The model comprised 100 decision trees, each limited to a maximum depth of 10. Each tree occupied approximately 20 KB, estimated based on the number of nodes per tree and the storage required for node-specific parameters. A full binary tree of depth 10 contained up to 1023 nodes; assuming 12 bytes per node (for feature index, threshold, and output value), the total memory footprint per tree was approximately 12 KB, with the remaining 8 KB accounting for structural and buffer overhead. This sizing was profiled using Xilinx Vivado HLS and verified using LightGBM's `model_size()` function, with an accepted margin of error of $\pm 10\%$. The dataset consisted of 34,903 instances across 21 features, which were preprocessed and split into training and testing subsets. Following dimensionality reduction to five principal components, SMOTE was applied to the training data, increasing the sample size to 50,000. Training the Random Forest model on this resampled dataset took approximately 50 s, while inference on 10,000 test samples was completed in 0.7 s. The PYNQ-Z2 consumed 2.8 W in the idle state and 3.6 W during Random Forest inference under full load. This marginal increase confirms the feasibility of deploying the framework on resource-constrained edge devices without excessive energy overhead. These results confirm the suitability of Random Forest classifiers for deployment on embedded systems with constrained resources. Future work will explore FPGA-accelerated implementations exploiting parallelism, pipelining, and hardware-aware optimizations to further enhance latency and energy efficiency for real-time BESS-integrated smart metering systems. Related research on compressed neural architectures implemented on edge platforms has demonstrated the feasibility of deploying efficient models in real-time, resource-limited scenarios.

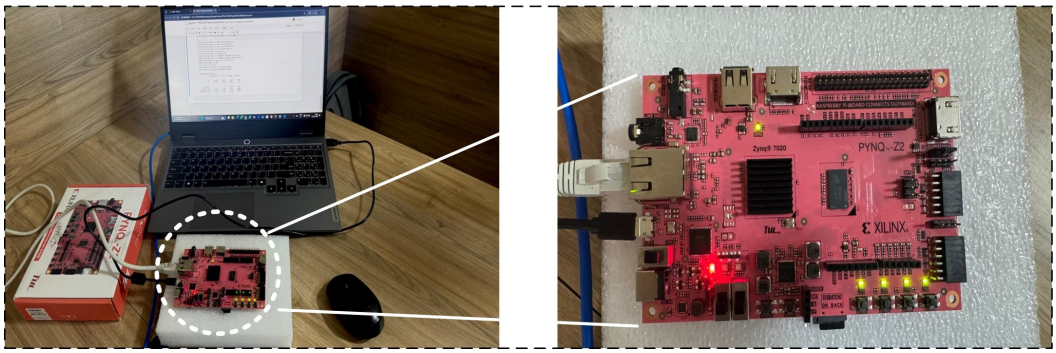


**Figure 11.** Machine learning model on PYNQ board.

### *5.2. Feature Analysis*

Feature analysis is used to analyze the impact of various variables on identifying cyberattacks within the BESS system. This study used statistical and graphical techniques to examine the attributes, enhancing the identification of the most important factors affecting attack detection. PCA was utilized to describe data distribution and reduce dimensionality.

Figure 12 differentiates attack and normal conditions. The instances of attack data indicate anomalies in specific major components. Conversely, normal instances show a linear trend, signifying stable system behaviour. This different division confirms the existence of trends in cyberattacks, validating the usefulness of the selected features. The analysis of all features is shown in Figure 13. The importance of the features is evaluated using the Random Forest algorithm. The five most critical features influencing attack detection are as follows: State of Charge (SoC), which is highly vulnerable to power fluctuations and firmware intrusions; P_bat (Battery Power): Demonstrates fluctuations during BDI and FDI attacks; V_dc_link: Indicates voltage irregularities due to FDI attacks; Total Harmonic Distortion (THD_a): Influenced by firmware modifications; I_dc_bat (battery current): Shows irregular shutdowns in over-limit conditions. These variables have strong correlations with attack vectors, hence proving their importance in classification. Figure 14a is employed to identify feature correlations. Large positive correlations between P_bat and P_ref are noted, indicating their coordinated behaviour under standard conditions. However, attack scenarios disrupt these relationships, emphasizing feature disturbances during security exposures. Feature analysis indicates that SoC and P_bat exhibit greater vulnerability to anomalies. Therefore, they are regarded as vital features for monitoring cyberattacks, as illustrated in Figure 14b, improving the accuracy of classification models.

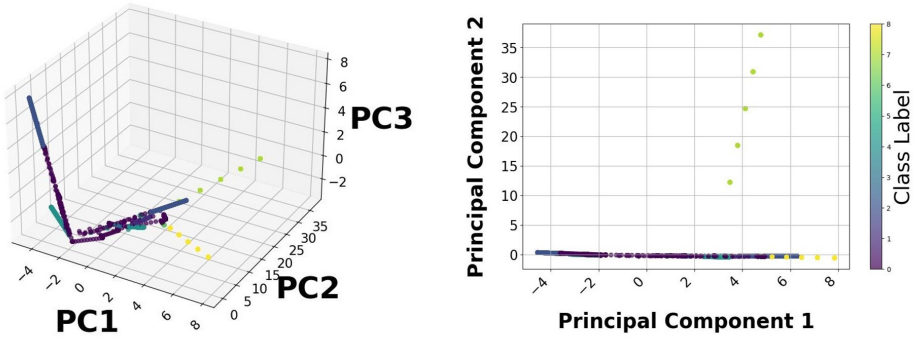


**Figure 12.** PCA.

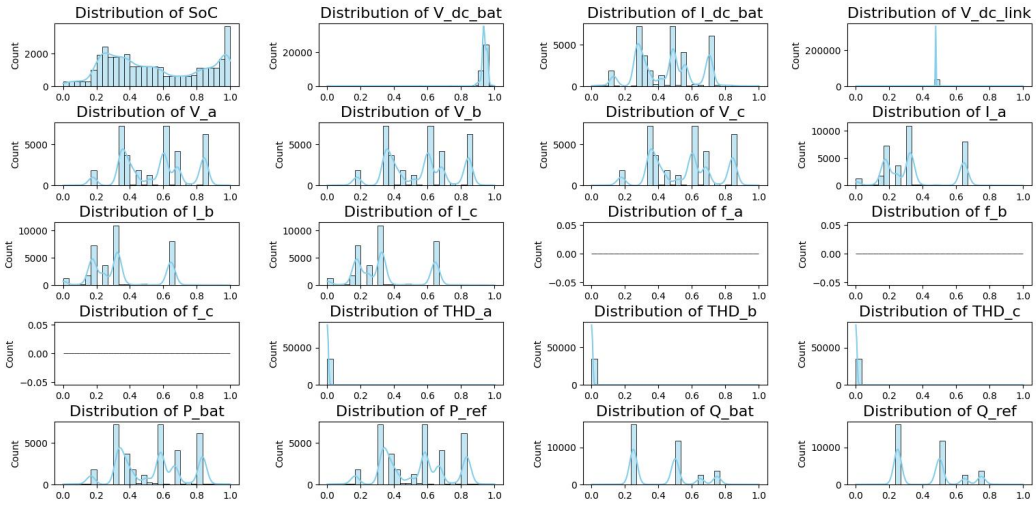


**Figure 13.** Analysis of all distinct features.

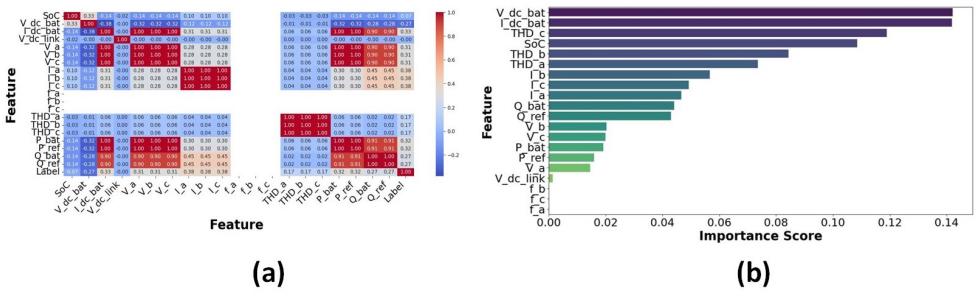


**Figure 14.** (**a**) Feature correlation matrix. (**b**) Feature analysis using Random Forest.

### *5.3. Robustness Against Adversarial Attacks*

In addition to assessing our machine learning models' performances with clean data, we also evaluated how resilient they were against adversarial attacks. A major challenge in adversarial machine learning is the introduction of minor perturbations to the input data in order to trick the model into producing inaccurate predictions. The effectiveness of Random Forest, LightGBM, CatBoost, and ANN under the influence of Projected Gradient Descent (PGD) and Fast Gradient Sign Method (FGSM) attacks is thoroughly examined in this section. At different epsilon values (perturbation levels of 0.01, 0.05, and 0.1), both binary and multi-class classification tasks were taken into consideration. Model performance under clean and adversarial settings for both binary classification and multi-class classification is shown in Tables 6 and 7. Clean data performance: The models performed extremely well on clean, undisturbed data. The best results were obtained by Random Forest and LightGBM, both of which achieved >99% accuracy. Superior precision, recall, and F1-score findings demonstrated Random Forest's ideal balance for classification tasks. With an accuracy of 97.68%, ANN outperformed CatBoost and ANN in comparison, indicating that its simpler architecture makes it vulnerable, particularly when dealing with intricate data patterns. FGSM and PGD attack performance (epsilon = 0.01): All models saw some performance degradation at low perturbation (epsilon = 0.01), but Random Forest and LightGBM held up the best. Both FGSM and PGD attacks did not affect Random Forest's accuracy, which remained at 95.69%. With an accuracy of 94.72% under FGSM and 94.80% under PGD, LightGBM displayed a comparable drop. With 96.35% accuracy under FGSM and 96.94% accuracy under PGD, CatBoost demonstrated a stronger defense against the attacks. On the other hand, ANN saw a more pronounced drop, yet maintained an accuracy of 97.42%.

FGSM and PGD attack performance (epsilon = 0.05): All models showed a significant drop in accuracy with a mild disturbance (epsilon = 0.05). Under FGSM and PGD, Random Forest fell to 93.93% and 95.03%, respectively. CatBoost dropped to 88.96% accuracy under FGSM, while LightGBM had a steep decline to 85.09% accuracy. With accuracy declining to 95.02% under FGSM and 95.01% under PGD, ANN's performance was much worse. All models likewise saw a decline in F1-scores, with Random Forest continuing to have the highest F1-score at 0.8049.

**Table 6.** Model performance under clean and adversarial settings for binary classification.

| Model | Attack | Eps | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|---|---|
| Random Forest | clean | 0 | 0.9981 | 0.9921 | 0.9984 | 0.9952 |
| XGBoost | clean | 0 | 0.9984 | 0.9968 | 0.9950 | 0.9959 |
| LightGBM | clean | 0 | 0.9994 | 0.9991 | 0.9979 | 0.9985 |
| SVM | clean | 0 | 0.9558 | 0.8552 | 0.9735 | 0.9021 |
| Random Forest | FGSM_surrogate | 0.01 | 0.9518 | 0.9253 | 0.8096 | 0.8557 |
| Random Forest | PGD_surrogate | 0.01 | 0.9518 | 0.9253 | 0.8096 | 0.8557 |
| XGBoost | FGSM_surrogate | 0.01 | 0.9185 | 0.8573 | 0.6619 | 0.7130 |

**Table 6.** *Cont.*

| Model | Attack | Eps | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|---|---|
| XGBoost | PGD_surrogate | 0.01 | 0.9172 | 0.8520 | 0.6571 | 0.7072 |
| LightGBM | FGSM_surrogate | 0.01 | 0.9501 | 0.9154 | 0.8086 | 0.8518 |
| LightGBM | PGD_surrogate | 0.01 | 0.9502 | 0.9156 | 0.8093 | 0.8523 |
| SVM | FGSM_surrogate | 0.01 | 0.9558 | 0.8552 | 0.9735 | 0.9021 |
| SVM | PGD_surrogate | 0.01 | 0.9558 | 0.8552 | 0.9735 | 0.9021 |
| Random Forest | FGSM_surrogate | 0.05 | 0.9472 | 0.9054 | 0.8012 | 0.8433 |
| Random Forest | PGD_surrogate | 0.05 | 0.9488 | 0.9100 | 0.8061 | 0.8483 |
| XGBoost | FGSM_surrogate | 0.05 | 0.7576 | 0.5389 | 0.5653 | 0.5392 |
| XGBoost | PGD_surrogate | 0.05 | 0.7655 | 0.5270 | 0.5418 | 0.5270 |
| LightGBM | FGSM_surrogate | 0.05 | 0.7852 | 0.6017 | 0.6852 | 0.6152 |
| LightGBM | PGD_surrogate | 0.05 | 0.7939 | 0.6075 | 0.6907 | 0.6232 |
| SVM | FGSM_surrogate | 0.05 | 0.9512 | 0.8467 | 0.9592 | 0.8915 |
| SVM | PGD_surrogate | 0.05 | 0.9535 | 0.8502 | 0.9704 | 0.8975 |
| Random Forest | FGSM_surrogate | 0.1 | 0.9221 | 0.8471 | 0.6949 | 0.7433 |
| Random Forest | PGD_surrogate | 0.1 | 0.9107 | 0.7852 | 0.6850 | 0.7206 |
| XGBoost | FGSM_surrogate | 0.1 | 0.7623 | 0.5256 | 0.5400 | 0.5249 |
| XGBoost | PGD_surrogate | 0.1 | 0.7830 | 0.5318 | 0.5446 | 0.5339 |
| LightGBM | FGSM_surrogate | 0.1 | 0.7702 | 0.6410 | 0.8123 | 0.6519 |
| LightGBM | PGD_surrogate | 0.1 | 0.8080 | 0.6553 | 0.8095 | 0.6799 |
| SVM | FGSM_surrogate | 0.1 | 0.9346 | 0.8177 | 0.8857 | 0.8469 |
| SVM | PGD_surrogate | 0.1 | 0.9357 | 0.8202 | 0.8881 | 0.8495 |

FGSM and PGD attack performance (epsilon = 0.1): The models' performances deteriorated significantly more with strong perturbation (epsilon = 0.1). Random Forest declined to 90.93% accuracy under FGSM and 92.19% accuracy under PGD. The accuracy of LightGBM drastically dropped, falling to 85.94% under FGSM and 83.07% under PGD. CatBoost's accuracy dropped to 89.71% under FGSM and 86.25% under PGD. With accuracy falling to 74.28% under FGSM and 74.23% under PGD, ANN had the highest vulnerability, underscoring its vulnerability to adversarial perturbations. With good precision and recall, Random Forest proved to be the most resilient model, retaining high accuracy and F1-scores even in the face of intense adversarial perturbations. This makes it extremely dependable in adversarial settings. While both LightGBM and CatBoost demonstrated respectable resistance, LightGBM's performance declined more noticeably at epsilon = 0.1. With significant accuracy decreases at all perturbation levels, ANN was the most susceptible model to adversarial attacks, despite being efficient in clean environments. According to the investigation, ANN is inappropriate in adversarial situations, Random Forest is the most resistant against adversarial attacks, while LightGBM and CatBoost are less robust.

**Table 7.** Model performance under clean and adversarial settings (macro F1-score) for multi-class classification.

| Model | Attack | Eps | Accuracy | Precision | Recall | Macro-F1 |
|---|---|---|---|---|---|---|
| Random Forest | clean | 0 | 0.9994 | 0.9985 | 0.9985 | 0.9985 |
| LightGBM | clean | 0 | 0.9994 | 0.9991 | 0.9979 | 0.9985 |
| CatBoost | clean | 0 | 0.9986 | 0.9946 | 0.9980 | 0.9963 |
| ANN | clean | 0 | 0.9768 | 0.9120 | 0.9858 | 0.9447 |
| Random Forest | FGSM_surrogate | 0.01 | 0.9569 | 0.9367 | 0.8288 | 0.8729 |
| Random Forest | PGD_surrogate | 0.01 | 0.9569 | 0.9373 | 0.8282 | 0.8727 |

**Table 7.** *Cont.*

| Model | Attack | Eps | Accuracy | Precision | Recall | Macro-F1 |
|---|---|---|---|---|---|---|
| LightGBM | FGSM_surrogate | 0.01 | 0.9472 | 0.8888 | 0.8198 | 0.8499 |
| LightGBM | PGD_surrogate | 0.01 | 0.9480 | 0.8929 | 0.8203 | 0.8517 |
| CatBoost | FGSM_surrogate | 0.01 | 0.9635 | 0.9334 | 0.8693 | 0.8980 |
| CatBoost | PGD_surrogate | 0.01 | 0.9694 | 0.9481 | 0.8877 | 0.9151 |
| ANN | FGSM_surrogate | 0.01 | 0.9742 | 0.9071 | 0.9773 | 0.9384 |
| ANN | PGD_surrogate | 0.01 | 0.9742 | 0.9071 | 0.9773 | 0.9384 |
| Random Forest | FGSM_surrogate | 0.05 | 0.9393 | 0.9125 | 0.7489 | 0.8049 |
| Random Forest | PGD_surrogate | 0.05 | 0.9503 | 0.9658 | 0.7743 | 0.8391 |
| LightGBM | FGSM_surrogate | 0.05 | 0.8509 | 0.6617 | 0.7338 | 0.6861 |
| LightGBM | PGD_surrogate | 0.05 | 0.8307 | 0.6417 | 0.7253 | 0.6653 |
| CatBoost | FGSM_surrogate | 0.05 | 0.8896 | 0.7251 | 0.7928 | 0.7520 |
| CatBoost | PGD_surrogate | 0.05 | 0.8856 | 0.7192 | 0.7947 | 0.7480 |
| ANN | FGSM_surrogate | 0.05 | 0.9502 | 0.8448 | 0.9563 | 0.8893 |
| ANN | PGD_surrogate | 0.05 | 0.9499 | 0.8443 | 0.9550 | 0.8885 |
| Random Forest | FGSM_surrogate | 0.1 | 0.9093 | 0.8426 | 0.6101 | 0.6518 |
| Random Forest | PGD_surrogate | 0.1 | 0.9219 | 0.9466 | 0.6423 | 0.6998 |
| LightGBM | FGSM_surrogate | 0.1 | 0.8594 | 0.7062 | 0.8733 | 0.7468 |
| LightGBM | PGD_surrogate | 0.1 | 0.8581 | 0.7040 | 0.8685 | 0.7440 |
| CatBoost | FGSM_surrogate | 0.1 | 0.8971 | 0.7343 | 0.7492 | 0.7414 |
| CatBoost | PGD_surrogate | 0.1 | 0.8625 | 0.6814 | 0.7595 | 0.7086 |
| ANN | FGSM_surrogate | 0.1 | 0.7428 | 0.6288 | 0.7986 | 0.6285 |
| ANN | PGD_surrogate | 0.1 | 0.7423 | 0.6262 | 0.7913 | 0.6259 |

### *5.4. Encryption Framework*

Data encryption was implemented to protect critical operational data, including State of Charge, voltage, and thermal metrics, during transmission between SCADA, BESS, inverters, and battery modules, therefore reducing cyber-physical threats such as grid destabilization and false command injection. In line with industrial standards (e.g., IEC 62443, NIST), two encryption techniques were incorporated to provide safe transfer of data within the BESS framework. The hybrid encryption approach integrates Blowfish data encryption and RSA for safe key exchange. Elliptic Curve Cryptography (ECC) was used to deliver encryption using reduced key sizes, providing data security with lowered computational requirements.

#### 5.4.1. Elliptic-Curve-Cryptography-Based Approach

This is an asymmetric cryptographic scheme whose security depends on the mathematical complexity of the Elliptic Curve Discrete Logarithm Problem (ECDLP). This method employs the Elliptic Curve Diffie–Hellman (ECDH) for secure key exchange, in which both the sender and receiver generate their ECC key pairs. Following the key exchange, a shared secret is produced by ECDH using an HMAC-based key derivation function (HKDF) that uses HMAC-SHA256. The resulting symmetric key is used in an XOR encryption technique to encrypt the plaintext data. The SoC feature was chosen as representative data to demonstrate the tests. Figure 15 shows the comparison of original and encrypted data. Figure 16a illustrates the behaviour of the encryption process when a random salt is applied, ensuring that encrypting the same value multiple times produces distinct ciphertexts and displays the hashed encrypted values of the State of Charge (SoC) parameter across various iterations, showcasing the impact of entropy introduced by the salt. This non-deterministic nature of the encryption process demonstrates that each iteration produces a unique hashed result, even with the same input. This feature is crucial for cryptographic security, as it inhibits pattern recognition efforts and ensures that ciphertexts generated from identical

plaintext values stay unpredictable. The wide interquartile range in Figure 16b confirms that the ciphertext demonstrates unpredictability. The encrypted SoC values depicted in Figure 17a reveal that the ciphertext exhibits unpredictability. A uniform distribution of ciphertext values is essential for protection against frequency analysis and other statistical assaults. Figure 17b demonstrates the lack of bias towards any particular character, thereby validating that the ciphertext is uniformly random.

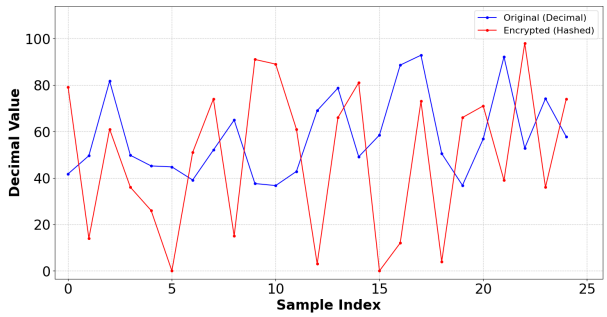


**Figure 15.** SoC: Comparison of original vs. encrypted data of ECC.

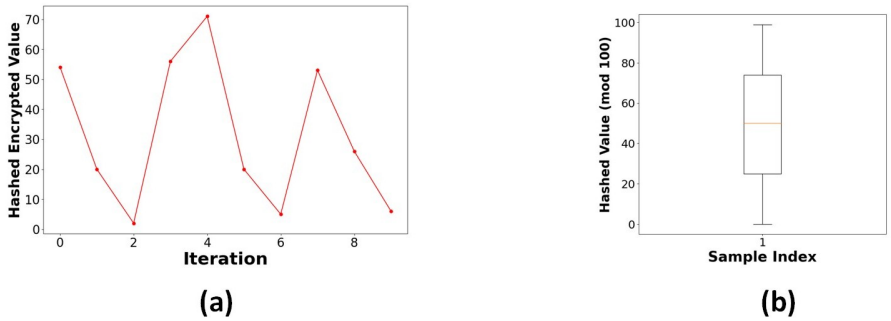


**Figure 16.** (**a**) Repeated encryption hash scatter for SoC. (**b**) Box plot of hashed encrypted values of SoC.

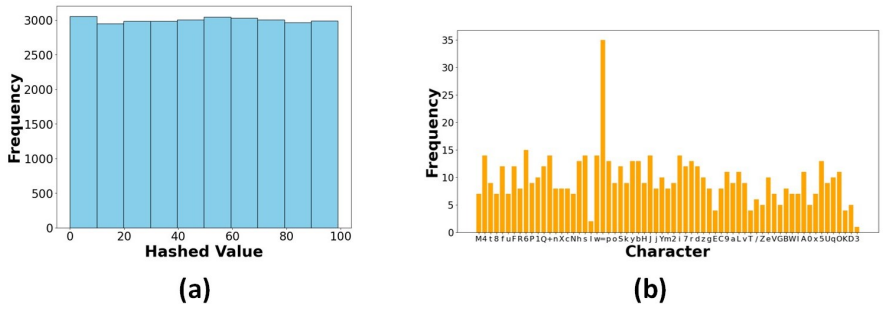


**Figure 17.** (**a**) Histogram of hashed encrypted values for SoC. (**b**) Frequency analysis of ciphertext characters for SoC.

Security Evaluation for ECC Method

**Salt Randomness Analysis**: The salt randomness test gathered and analyzed 1000 distinct salt values from 20 data columns. The flat distribution in Figure 18a confirms proper random number generation for salt values, making pre-computation attacks infeasible. There is uniform distribution across all possible byte values (0–255). The uniform distribution evident in the salt byte distribution signifies robust randomness in salt creation. The lack of patterns in Figure 18b confirms independence between generated salts, ensuring unique encryption contexts. The entropy heatmap display reveals no identifiable trends among the initial 50 salts, indicating the successful application of the random number

generator utilized for salt generation. Let $S$ be the set of generated salts, where each salt $s \in S$ is a 16-byte value. The entropy $H(S)$ can be calculated using Equation (25), where $p(x)$ is the probability of byte value $x$ occurring in the salt distribution.

$$H(S) = -\sum_{x} p(x) \log_2 p(x) \tag{25}$$

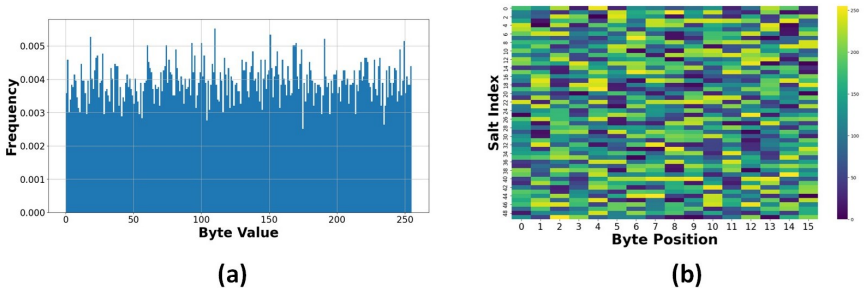


**Figure 18.** (**a**) Salt byte distribution. (**b**) Salt byte pattern.

**Bit-Flipping Resistance**: The bit-flipping test proved strong integrity protection, with no successful decryptions following the modification of individual bits (0 valid decryptions out of 50 attempts). This represents the execution of effective resistance against bit manipulation attacks, matching the avalanche effect principle of safe cryptographic systems. For any ciphertext $C$ and its modified version $C'$, where Hamming distance $H(C, C') = 1$: Decryption$(C') \neq$ Decryption$(C)$.

**Reversibility Analysis**: The reversibility test demonstrated exact reconstruction of the original values: Mean decryption error: 0.000000; standard deviation: 0.000000. This implies perfect encryption–decryption processes, necessary for preserving data integrity in important applications.

**Malleability Assessment**: The malleability test findings indicate robust resistance to regulated alterations: Success rate by bit position: [0.0, 0.0, 0.01, 0.0, 0.0, 0.0, 0.0, 0.0]. Average success rate: 0.001. A small 0.1% success rate for malleability attacks indicates strong semantic security. Figure 19a exhibits a minimal success rate; a small 0.1% success rate for malleability attacks indicates strong semantic security across all bit locations. Minor fluctuations in success rates ($\leq$0.01) demonstrate continuous opposition to multi-bit alterations.

**Side-Channel Analysis**: Timing analysis in Figure 19b indicates a negligible link between ciphertext length and processing duration. To assess the encryption scheme's robustness against timing-based side-channel attacks, we conducted an empirical timing analysis on the ECC-based decryption process using ciphertexts of varying lengths. A total of 1000 decryption operations were executed, and decryption durations were recorded. The mean decryption time was 0.01234 s, with a standard deviation of 0.00123 s. The Pearson correlation coefficient between ciphertext length and decryption time was $r = 0.015$ ($p = 0.68$), indicating no statistically significant relationship between input size and processing time. To further validate this result, a bootstrap resampling ($n = 10{,}000$) was performed, yielding a 95% confidence interval of $[-0.023, +0.054]$, which includes zero, confirming a lack of consistent timing correlation. These findings suggest that the ECC-based encryption demonstrates empirical resistance to timing-based side-channel attacks under the tested conditions. However, we acknowledge that formal timing-constant implementations and hardware-level measurements would be necessary for comprehensive side-channel resistance validation.

**Replay Attack Resistance**: Absolute resistance to replay attacks was demonstrated by the absence of duplicate ciphertexts and the generation of unique ciphertexts for each encryption operation. For any two plaintexts $p_1, p_2$ encrypted under the same key $k$:

$$\text{Encrypt}(p_1, k, s_1) \neq \text{Encrypt}(p_2, k, s_2) \tag{26}$$

where $s_1, s_2$ are distinct salts.

The scheme's resistance against attacks, such as frequency analysis, chosen-plaintext attacks, and side-channel attacks, validates the strength of the ECC and its related key generation and encryption elements. The statistical distribution of the ciphertext, which nearly approximates a uniform distribution, further confirms its resistance to cryptanalytic attacks. The validation of key exchange, along with consistent encryption and decryption, verifies that the chosen cryptographic components are specifically designed for safe data transmission. These results highlight the possibility of using such methods in practical and secure communication systems.

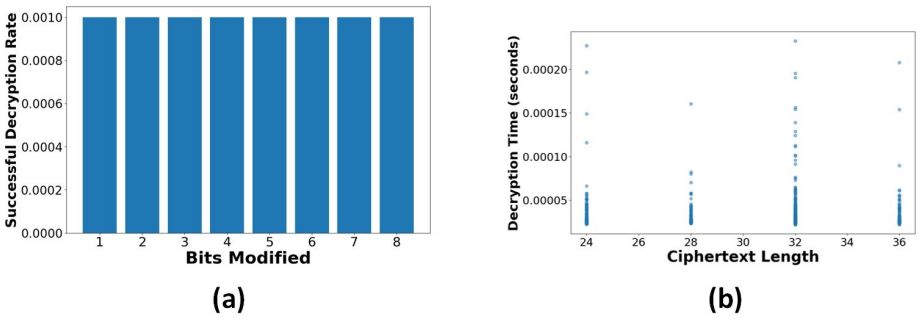


**Figure 19.** (**a**) Malleability test: Impact of bit modifications on decryption success. (**b**) Correlation between ciphertext length and decryption time.

### 5.4.2. Hybrid Encryption-Based Approach

A hybrid encryption method was used, combining the symmetric Blowfish technique for data encryption with the asymmetric RSA algorithm for safe key exchange. The encryption process begins with generating a 1024-bit RSA key pair, including a private key and a public key. These keys facilitate the safe transmission of the Blowfish encryption key, preventing unauthorized access. The RSA keys are managed independently to facilitate effective key management, ensuring the encryption process's confidentiality and security. Following the RSA key generation, a 448-bit Blowfish key, the maximum key length supported by the technique, is generated randomly and securely stored. The BESS data is encrypted for protection. Blowfish encryption is employed in Cipher Block Chaining (CBC) mode to incorporate randomization and prevent identical plaintext blocks from producing the same ciphertext. An Initialization Vector (IV) is generated and appended to the encrypted data, ensuring that each encryption instance is unique and resistant to cryptanalysis. To increase security, the Blowfish key is encrypted with RSA, utilizing the public key for encryption. The encrypted Blowfish key is stored independently from the data, verifying that decryption is possible with access to the associated RSA private key. The segmentation of encryption components improves the overall security framework, as an attacker would need the encrypted data and the RSA private key to decrypt the information. Upon finalizing encryption, the modified data is preserved, maintaining the original structure while replacing it with its encrypted equivalents.

The encryption process was tested by several comparisons: Figure 20 depicts the variation between encrypted and plaintext data values, illustrating the effect of encryption on data representation. Figure 21 shows the distribution of encrypted and original values.

To evaluate the integrity of the decryption process, Figures 22 and 23 compare the State of Charge (SoC) values of the encrypted and original data. The implementation of this method provides many advantages, as Blowfish, a symmetric encryption technique, performs rapid encryption and decryption, making it computationally efficient for extensive data. The RSA method used for key exchange reduces dangers related to key transmission and storage. This method ensures that decryption is impossible without the RSA private key, even if an attacker obtains the encrypted data. This hybrid encryption method, using both Blowfish and the RSA algorithm, effectively secures BESS data against cyber threats.

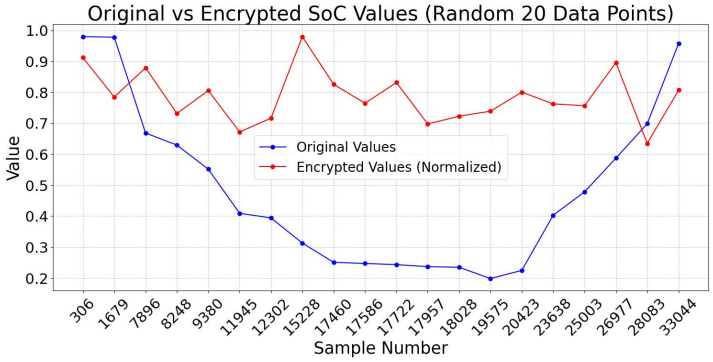


**Figure 20.** SoC: Encrypted vs. normal (hybrid encryption).

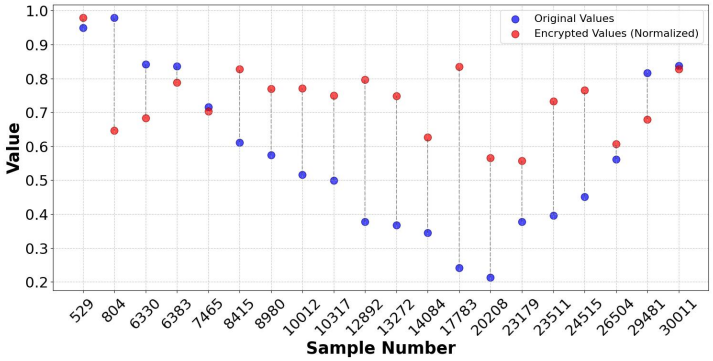


**Figure 21.** Encrypted vs. normal (hybrid encryption).

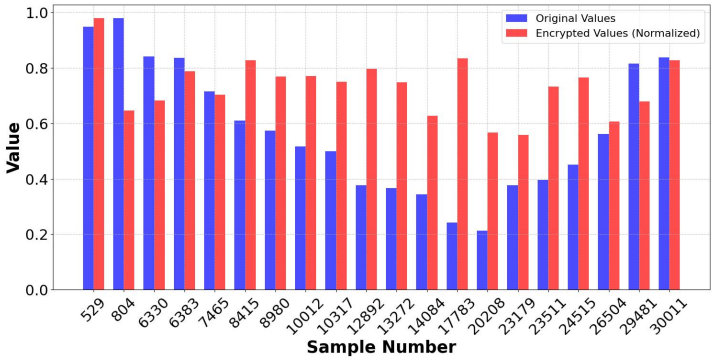


**Figure 22.** Histogram of SoC: Encrypted vs. normal (hybrid encryption).

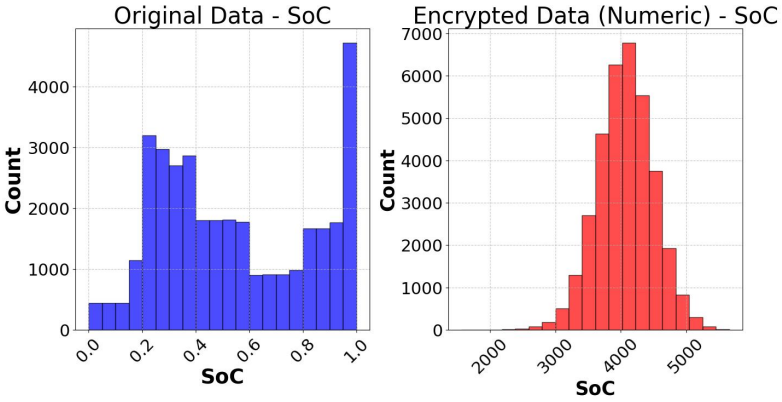


**Figure 23.** SoC: Encrypted vs. normal data of hybrid encryption.

Security Evaluation for Proposed Hybrid Encryption Method

**The key length test** is an essential factor in evaluating the security efficiency of encryption algorithms, as longer keys provide superior resistance to brute-force attacks by exponentially increasing the computational effort necessary for key extraction. A hybrid encryption system uses a 1024-bit RSA key for safe key exchange and a 448-bit Blowfish key for symmetric encryption. Figure 24a illustrates that RSA's extended key length guarantees strong defense against key factoring attacks, converting it into being suitable for asymmetric encryption, but Blowfish's 448-bit key offers an ideal balance between security and computational efficiency. The validation of these key lengths confirms compliance with industry security standards and that our encryption scheme remains strong against cryptanalytic threats and assures that it can achieve secure data transmission.

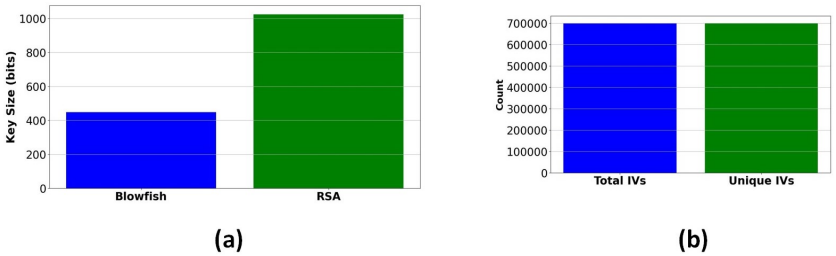


**Figure 24.** (**a**) Key length comparison between RSA and Blowfish. (**b**) IV Uniqueness Test results.

**IV Uniqueness Test**: The Initialization Vector (IV) Uniqueness Test was conducted to evaluate the security of the process of encryption, specifically in Cipher Block Chaining (CBC) and Counter (CTR) modes, where reusing IV leads to cryptographic issues. All created IVs were found to be unique by analyzing the occurrence of duplicate IVs, thus reducing the risk of plaintext pattern leakage. These results validate the reliability of the IV generation technique in maintaining encryption detail. Figure 24b confirms that each encrypted piece of data utilizes a different Initialization Vector (IV), maintaining CBC mode security standards and reducing issues such as pattern leakage and chosen-plaintext attacks.

### *5.5. Data Validation and Integrity Checking*

Data reliability and quality are crucial for resilient models. This section defines the methodologies used for data validation and integrity verification, including anomaly detection, consistency checks, and redundancy processes. The statistical method Z-scores, which measure the deviation of data points from the mean, were used to detect anomalies. Anomalies are characterized by a Z-score $> 1.5$, indicating that data points deviate from a normal distribution. The Z-score threshold of 1.5 is chosen empirically after experiments

with multiple thresholds (1.0, 1.5, 2.0). Threshold = 1.5 provided the best balance between sensitivity (detecting anomalies) and specificity (avoiding false positives), consistent with values commonly used in prior anomaly detection studies. Figure 25a demonstrates that the majority of data points display a low anomaly score, ranging between 0.5 and 0.75. The tail distribution is long because some data points have extreme anomaly scores (more than 1.25). A few data points do not exhibit the expected trends, while most operate normally. The data points in Figure 25b fall within the interquartile range (IQR), validating that the normal values are closely clustered. Values beyond 1.5 × IQR indicate many outliers, with certain values beyond 6.0. High outliers indicate anomalous behaviour that may be associated with unexpected operational fluctuations, sensor malfunctions, power quality issues, voltage changes, and harmonic distortions. Redundancy mechanisms for accuracy enhancement are implemented by cross-verifying the three-phase voltage measurements (V_a, V_b, and V_c). Figure 26 demonstrates that the individual voltage signals are exactly aligned, and the computed mean voltage further proves the uniformity across the phases.

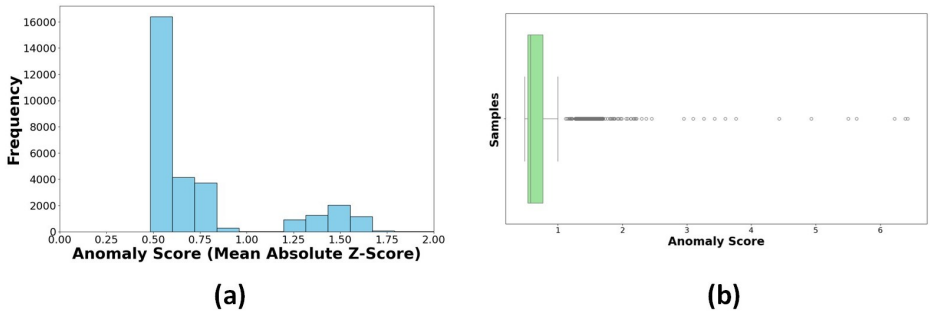


**Figure 25.** (**a**) Anomaly scores (mean of Z-scores). (**b**) Box plot for outlier detection (anomaly scores).

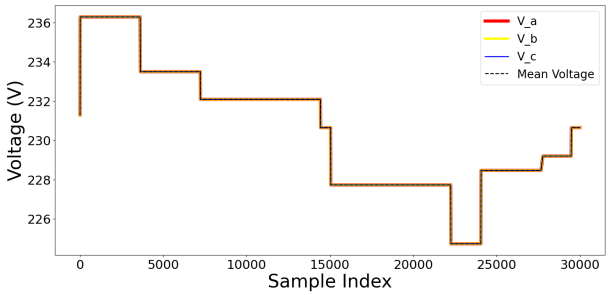


**Figure 26.** Phase voltages over samples.

### *5.6. Power Quality Control and Harmonics*

This section outlines the results of power quality control measures, including adaptive filtering, dynamic recalibration, and threshold alarms. The findings indicate that the integrated approach decreases harmonic distortions and improves operational stability while complying with IEEE 519-2022 standards. Adaptive filtering for harmonic auppression is implemented using a low-pass Butterworth filter on the V_a signal, which is essential to minimize the impact of harmonic injection. The filtered signal maintains the overall trend of the original measurement, as shown in Figure 27, while effectively reducing high-frequency noise. This filtering method is essential for verifying harmonic analysis, as it improves the interpretation of the fundamental voltage waveform. The system can initiate a dynamic Inverter Control Parameter recalibration process when the anomaly score surpasses a predetermined threshold. However, a majority of values remain within normal parameters, as illustrated in Figure 28a,b. The framework is established to modify control parameters. This ensures that the system can maintain optimal performance despite minor variations. A correlation heatmap, Figure 29, of selected parameters, phase voltages, load

currents, power, and THD percentages highlights strong interdependencies among these variables. Threshold alarms have been established to monitor Total Harmonic Distortion (THD) values. The IEEE 519-2022 guidelines indicate that Total Harmonic Distortion (THD) values exceeding 5% are frequently harmful. The results show that the THD values for phases A, B, and C constantly stay beneath the threshold, showing that the system runs within acceptable harmonic distortion limitations and ensuring good power quality, as seen in Figure 28.

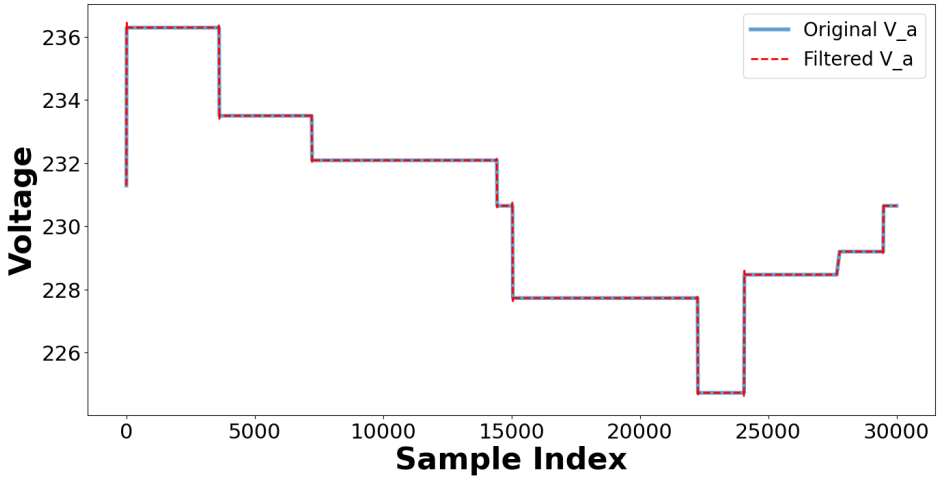


**Figure 27.** Adaptive filtering on V_a signal (original vs. filtered signal).

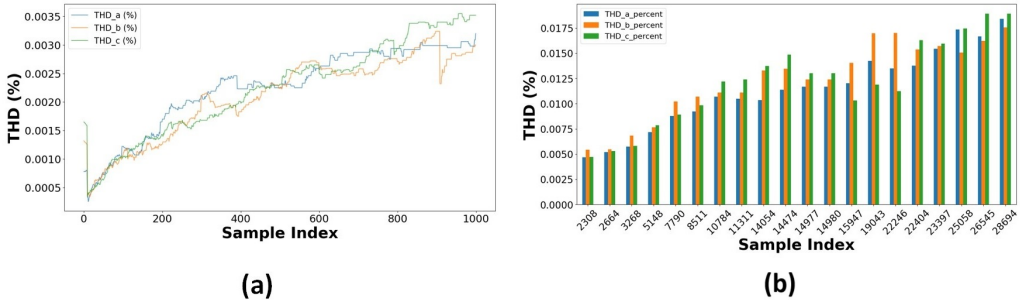


**Figure 28.** (**a**) Time series of THD percentages (first 1000 samples). (**b**) THD percentages for random samples of each phase.

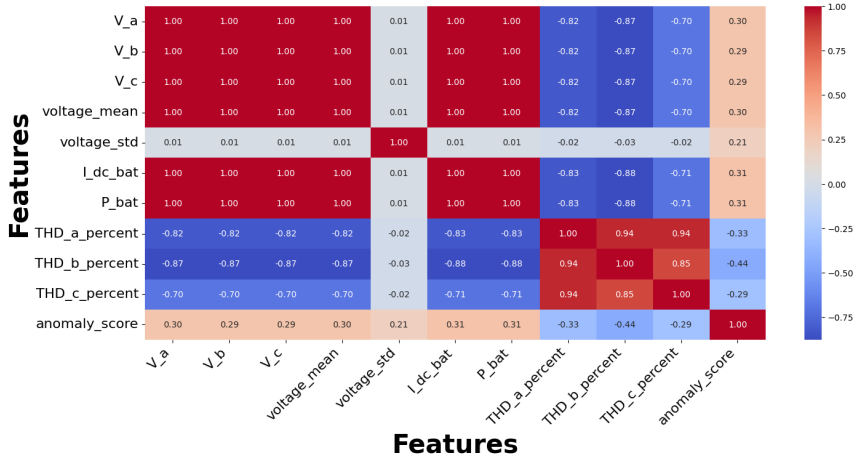


**Figure 29.** Correlation heatmap of selected features.

Verifying compliance with the IEEE 519 standard for Total Harmonic Distortion (THD) for all three phases provided information about power quality throughout system operation. This was carried out by measuring THD levels against the stated threshold of 5% for voltage harmonics at the point of common coupling (PCC). The maximum Total Harmonic Distortion (THD) values recorded across all phases were consistently 1.00%. The statistical analysis revealed mean Total Harmonic Distortion (THD) values of 0.0035% for Phase A and 0.0036% for Phases B and C. All phases demonstrated a standard deviation of approximately 0.046%, indicating consistent harmonic performance. Furthermore, the distribution characteristics showed that the 75th percentile values were below 0.001%, while the maximum values remained far below the IEEE 519 criteria of 5%. All three phases exhibited high compliance with IEEE 519 requirements, with median THD values (50th percentile) consistently below 0.001% and maximum THD values only reaching 20% of the acceptable limit, indicating successful harmonic mitigation and balanced operation. These findings demonstrate that the BESS data upholds superior power quality during standard operating settings, remaining far below regulatory thresholds, indicative of efficient harmonic control measures.

### *5.7. Multi-Layered Security Analysis of BESS*

The analysis of attack data assessed the influence of assaults on 20 critical BESS parameters. The mean absolute differences between normal and attack data are illustrated in Figure 30a, describing the variable effects across various features. Significant variations in power-related metrics (P_bat, P_ref) and voltage measurements (V_dc_bat, V_dc_link) were identified in this study, indicating that the attack prioritized power flow manipulation. A voltage-based protection system was established using the V_dc_bat parameter, with thresholds set at the standard operational data's 5th and 95th percentiles. As illustrated in Figure 30b, the protection system accomplished detection of trip percentage: 59.49% abnormal samples and clear discrimination between normal and attacked voltage profiles established protection boundaries with lower threshold = 663.7 V and upper threshold = 675.78 V.

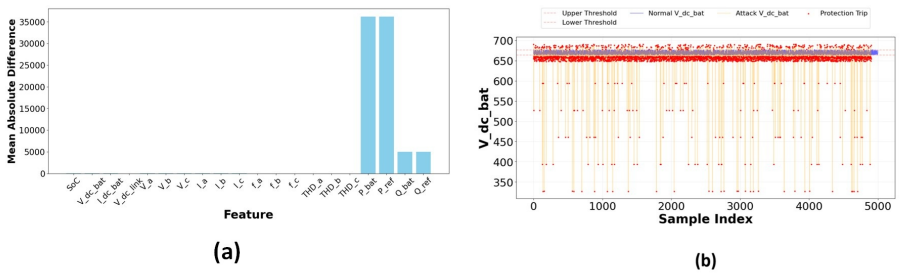


**Figure 30.** (**a**) Mean absolute difference for features. (**b**) Electrical protection mechanism on V_dc_bat.

High-frequency analysis of I_dc_bat showed unique features, including more noise and distortion during attacks, as shown in Figure 31a. During normal operation, sinusoidal waveforms were reliably detected with a noise level of 2%. The waveforms that were attacked exhibited distortion patterns and an increase in noise of 10%. A higher harmonic content was found by frequency domain analysis under attack conditions. The Data Integrity Assessment's power consistency tests in Figure 31b show variations between the calculated and measured power values. To verify consistency, the computed power $(V\_dc\_bat \times I\_dc\_bat)$ was compared to the measured battery power $P\_bat$. A statistical threshold of $\mu + 3\sigma$ was defined for anomaly identification, which discovered that 78 instances had integrity violations above the threshold, indicating a temporal correlation with attack intervals. These results show data modification during attack occurrences.

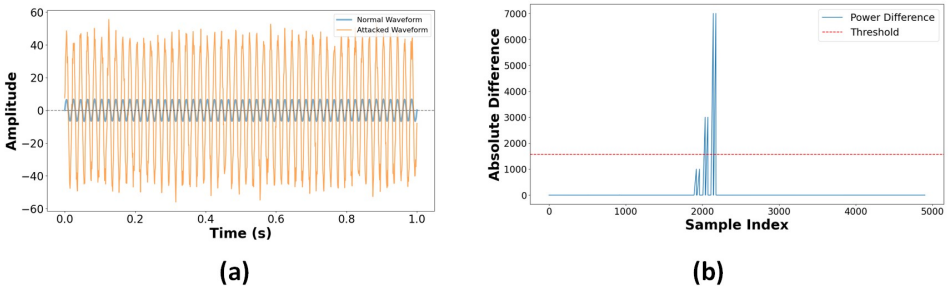


**Figure 31.** (**a**) Waveform data analysis for I_dc_bat. (**b**) Data integrity issues in power calculation.

## 6. Conclusions

This work introduces an end-to-end architecture that integrates machine-learning–based cyberattack detection with cryptographic protection for Battery Energy Storage Systems (BESSs). Random Forest and LightGBM emerged as effective classification models for the BESS-Set dataset, achieving high accuracy while remaining computationally efficient for embedded deployment. For secure communication, the system employs Elliptic Curve Cryptography (ECC) and a hybrid Blowfish–RSA scheme to protect classified outputs. Deployment of the ML models on the PYNQ-Z2 board demonstrated real-time feasibility in resource-constrained environments. The RAM usage, inference latency, and power draw during execution were reported, providing a clearer picture of the hardware performance for edge deployment scenarios.

Despite these contributions, some methodological limitations exist. The current study primarily relies on SMOTE to counter class imbalance, which may limit robustness on more complex or highly imbalanced datasets. Future work will investigate alternatives such as ADASYN or hybrid resampling approaches. Another limitation is that the study relies exclusively on the simulated BESS-Set dataset. This dataset provides a controlled and well-labeled environment for evaluating anomaly detection and attack classification; it does not fully capture real-world complexities such as noisy sensor measurements, intermittent communication delays, hardware-related variability, and environmental disturbances. To improve generalizability, future work will focus on validating the framework with empirical BESS datasets and conducting stress tests under noisy dynamic operating conditions. In the current setup, cryptographic operations were implemented separately at the software level and not executed on the PYNQ-Z2 board. As part of our ongoing research, we plan to integrate the full system including anomaly detection, cryptographic security, and validation modules on the hardware platform to assess end-to-end computational overhead and scalability under variable load and attack scenarios.

This study focuses on a BESS; the vulnerabilities addressed are representative of a broader class of issues in IoT-based cyber-physical systems. Similar risks arise in domains such as smart grids, healthcare IoT, industrial IoT, and smart homes, where devices are often resource-constrained, highly interconnected, and deployed without strong security-by-design principles. Comparable efforts can also be observed in Ambient Assisted Living, where AI-driven facial emotion recognition is employed to adapt environments to users' affective states Ref. [29]. Recent advances in facial expression recognition have demonstrated the ability to extract highly discriminative local descriptors and improve classification performance across benchmark datasets Ref. [30]. Similarly, industrial applications demonstrate the feasibility of combining CNN architectures with sensor-driven data acquisition for predictive monitoring Ref. [31]. The proposed integration of AI-driven intrusion detection with lightweight cryptographic methods thus represents a generalizable defense strategy for IoT ecosystems. By validating this framework in a BESS, we provide a proof of

concept that can be extended to other application domains requiring secure, efficient, and real-time protection mechanisms.

Future research will prioritize testing the framework on real BESS testbeds with noisy and delayed sensor data. Additional directions include exploring federated learning for decentralized attack detection and investigating advanced lightweight deep learning architectures (e.g., CNNs and Transformers) to enhance robustness and generalization. With these constraints alleviated, the proposed framework can evolve into a scalable and dependable solution for secure, intelligent energy storage systems and beyond.

**Author Contributions:** Conceptualization, P.P.G., C.R., and C.N.; methodology, P.P.G. and C.N.; software, R.D.A.R., A.P., and R.M.R.Y.; formal analysis, R.M.R.Y., A.P., and P.P.G.; investigation, C.R. and R.D.A.R.; data preprocessing, K.B.; visualization, K.B.; data curation, R.D.A.R. and A.P.; resources, R.D.A.R. and R.M.R.Y.; supervision, C.N. and C.R.; project administration, C.R. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable. This study did not involve humans or animals and therefore did not require ethical approval.

**Informed Consent Statement:** Not applicable. This study did not involve human participants.

**Data Availability Statement:** The datasets used in this study are publicly available and can be accessed through the original source cited in the manuscript.

**Acknowledgments:** The authors thank their respective institutions for providing computational resources and infrastructure. No external administrative or technical support was involved.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Maddileti, N.S.; Namburi, R.; Raj, R.D.A.; Yanamala, R.M.R.; Pallakonda, A. DCGAN-Driven Minority Class Augmentation for Lightweight YOLO-Based Photovoltaic Defect Localization Suitable for Edge Deployment. *IEEE Trans. Device Mater. Reliab.* **2025**, *25*, 742–751. [CrossRef]
2. Mrudula, P.S.; Raj, R.D.A.; Pallakonda, A.; Reddy, Y.R.M.; Prakasha, K.K.; Anandkumar, V. Smart Grid Intrusion Detection for IEC 60870-5-104 with Feature Optimization, Privacy Protection, and Honeypot-Firewall Integration. *IEEE Access* **2025**, *13*, 128938–128958. [CrossRef]
3. Kharlamova, N.; Hashemi, S.; Træholt, C. The cyber security of battery energy storage systems and adoption of data-driven methods. In Proceedings of the 2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), Laguna Hills, CA, USA, 9–11 December 2020; pp. 188–192.
4. Priya, S.S.; Sanjana, P.S.; Yanamala, R.M.R.; Amar Raj, R.D.; Pallakonda, A.; Napoli, C.; Randieri, C. Flight-Safe Inference: SVD-Compressed LSTM Acceleration for Real-Time UAV Engine Monitoring Using Custom FPGA Hardware Architecture. *Drones* **2025**, *9*, 494. [CrossRef]
5. Trevizan, R.D.; Obert, J.; De Angelis, V.; Nguyen, T.A.; Rao, V.S.; Chalamala, B.R. Cyberphysical security of grid battery energy storage systems. *IEEE Access* **2022**, *10*, 59675–59722. [CrossRef]
6. Kharlamova, N.; Hashemi, S.; Træholt, C. Data-driven approaches for cyber defense of battery energy storage systems. *Energy AI* **2021**, *5*, 100095. [CrossRef]
7. Kharlamova, N.; Træhold, C.; Hashemi, S. Cyberattack detection methods for battery energy storage systems. *J. Energy Storage* **2023**, *69*, 107795. [CrossRef]
8. Alhajri, M.M.; Nour, D.B.; Alshabib, K.R.; Rob, R. Protecting Energy Storage Systems–Automated Generation Control-Against Coordinated and Dynamic Malicious Data Injection Cyber Attacks. In Proceedings of the 2024 6th Global Power, Energy and Communication Conference (GPECOM), Budapest, Hungary, 4–7 June 2024; pp. 494–499.
9. Pasetti, M.; Ferrari, P.; Bellagente, P.; Sisinni, E.; de Sá, A.O.; do Prado, C.B.; David, R.P.; Machado, R.C.S. Artificial neural network-based stealth attack on battery energy storage systems. *IEEE Trans. Smart Grid* **2021**, *12*, 5310–5321. [CrossRef]
10. De Sá, A.O.; Bento, L.M.D.S.; Flavio, M.L.; Pasetti, M.; Ferrari, P.; Sisinni, E. Ann-based stealth attack to battery energy storage systems by using a low-cost device. In Proceedings of the 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0 & IoT), Trento, Italy, 7–9 June 2022; pp. 201–206.

11. Randieri, C.; Ganesh, S.V.; Raj, R.D.A.; Yanamala, R.M.R.; Pallakonda, A.; Napoli, C. Aerial autonomy under adversity: Advances in obstacle and aircraft detection techniques for unmanned aerial vehicles. *Drones* **2025**, *9*, 549. [CrossRef]
12. Saiara, S.A.; Ali, M.H. An Ensemble Learning Based Cyber Attack Detection Technique for BESS Integrated PV System. In Proceedings of the SoutheastCon 2024, Atlanta, GA, USA, 15–24 March 2024; pp. 392–397.
13. Kharlamova, N.; Træholt, C.; Hashemi, S. AdaBoost-Based Cyberattack Detection Algorithm for Battery Systems Providing Frequency Regulation. In Proceedings of the 2023 IEEE 3rd International Conference on Industrial Electronics for Sustainable Energy Systems (IESES), Shanghai, China, 26–28 July 2023; pp. 1–5.
14. Kharlamova, N.; Træholt, C. Experimental Validation of Cyberattack Detector for Battery Energy Storage-based Virtual Power Plant. In Proceedings of the 2024 23rd International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 20–22 March 2024; pp. 1–5.
15. Flávio, M.; do Prado, C.B.; da Costa Carmo, L.F.R.; de Sá, A.O.; Ferrari, P.; Pasetti, M. Autoencoder-based Approach to Detect Stealth Cyberattacks in Battery Energy Storage Systems. In Proceedings of the 2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0 & IoT), Firenze, Italy, 29–31 May 2024; pp. 452–457.
16. Massaoudi, M.; Davis, K.R.; Abu-Rub, H.; Ghrayeb, A.; Huang, T. Accurate Joint Detection of False Data Injection Attacks on Islanded PV Output Power and State of Health Estimation of Lithium-Ion Batteries. In Proceedings of the 2024 4th International Conference on Smart Grid and Renewable Energy (SGRE), Doha, Qatar, 8–10 January 2024; pp. 1–6.
17. Mhaisen, N.; Fetais, N.; Massoud, A. Secure smart contract-enabled control of battery energy storage systems against cyber-attacks. *Alex. Eng. J.* **2019**, *58*, 1291–1300. [CrossRef]
18. Kaheni, M.; Usai, E.; Franceschelli, M. Resilient and privacy-preserving multi-agent optimization and control of a network of battery energy storage systems under attack. *IEEE Trans. Autom. Sci. Eng.* **2023**, *21*, 5320–5332. [CrossRef]
19. Pham-Quoc, C.; Bao, T.H.Q.; Thinh, T.N. Fpga/ai-powered architecture for anomaly network intrusion detection systems. *Electronics* **2023**, *12*, 668. [CrossRef]
20. Gangarapu, B.S.; Yanamala, R.M.R.; Pallakonda, A.; Vardhan, H.R.; Raj, R.D.A. Lightweight spatial attention pyramid network-based image forgery detection optimized for real-time edge TPU deployment. *Comput. Electr. Eng.* **2025**, *128*, 110645.
21. Kumar, N.; Mishra, V.M.; Kumar, A. Smart grid and nuclear power plant security by integrating cryptographic hardware chip. *Nucl. Eng. Technol.* **2021**, *53*, 3327–3334. [CrossRef]
22. Murlidharan, S.; Ravulakole, V.; Karnati, J.; Malik, H. Battery Management System: Threat Modeling, Vulnerability Analysis, and Cybersecurity Strategy. *IEEE Access* **2025**, *13*, 37198–37220. [CrossRef]
23. Chhetri, A.; Saini, D.K.; Yadav, M. Applications of BESS in Electrical Distribution Network with Cascading Failures Study—A Review. *IEEE Access* **2024**, *12*, 188267–188295. [CrossRef]
24. Pawar, P.P.; Femy, F.F.; Rajkumar, N.; Jeevitha, S.; Bhuvanesh, A.; Kumar, D. Blockchain-enabled cybersecurity for IoT using elliptic curve cryptography and black winged kite model. *Int. J. Inf. Technol.* **2025**, 1–11. [CrossRef]
25. Gaggero, G.B.; Armellin, A.; Ferro, G.; Robba, M.; Girdinio, P.; Marchese, M. BESS-Set: A Dataset for Cybersecurity Monitoring in a Battery Energy Storage System. *IEEE Open Access J. Power Energy* **2024**, *11*, 362–372. [CrossRef]
26. Randieri, C.; Perrotta, A.; Puglisi, A.; Grazia Bocci, M.; Napoli, C. CNN-Based Framework for Classifying COVID-19, Pneumonia, and Normal Chest X-Rays. *Big Data Cogn. Comput.* **2025**, *9*, 186. [CrossRef]
27. Dell'Olmo, P.V.; Kuznetsov, O.; Frontoni, E.; Arnesano, M.; Napoli, C.; Randieri, C. Dataset dependency in CNN-based copy-move forgery detection: A multi-dataset comparative analysis. *Mach. Learn. Knowl. Extr.* **2025**, *7*, 54. [CrossRef]
28. Randieri, C.; Pollina, A.; Puglisi, A.; Napoli, C. Smart Glove: A Cost-Effective and Intuitive Interface for Advanced Drone Control. *Drones* **2025**, *9*, 109. [CrossRef]
29. Russo, S.; Tibermacine, I.E.; Randieri, C.; Rabehi, A.; Alharbi, A.H.; El-kenawy, E.S.M.; Napoli, C. Exploiting facial emotion recognition system for ambient assisted living technologies triggered by interpreting the user's emotional state. *Front. Neurosci.* **2025**, *19*, 1622194. [CrossRef]
30. Pallakonda, A.; Yanamala, R.M.R.; Raj, R.D.A.; Napoli, C.; Randieri, C. DPIBP: Dining Philosophers Problem-Inspired Binary Patterns for Facial Expression Recognition. *Technologies* **2025**, *13*, 420. [CrossRef]
31. Osheter, T.; Campisi Pinto, S.; Randieri, C.; Perrotta, A.; Linder, C.; Weisman, Z. Semi-Autonomic AI LF-NMR Sensor for Industrial Prediction of Edible Oil Oxidation Status. *Sensors* **2023**, *23*, 2125. [CrossRef]