International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AN APPLIED MATHEMATICAL FRAMEWORK FOR PRIVACY-PRESERVING INTRUSION DETECTION USING FEATURE SELECTION AND FUSION MODELS.

[1]Swetha Madireddy*, [2]Kalaivani Kathirvelu,[3]Dr.B.Buvaneswari,[4]Dr. Chandra Sekar P,[5]Dr Ponmurugan Panneer Selvam,[6]Dr.Ahmed Mudassar Ali,

[1]Research Scholar, Vels Institute of Science, Technology & Advanced Studies, Department of Computer Science and Engineering, Pallavaram, Chennai, Tamil Nadu, India, 600 117

Email: swetha.mudupu@gmail.com - **Orcid: 0000-0001-7449-4996**

[2]Vels Institute of Science, Technology & Advanced Studies, Department of Computer Science and Engineering, Pallavaram, Chennai, Tamil Nadu, India, 600 117

Email: kalai.se@velsuniv.ac.in - **Orcid: 0000-0001-5384-6075**

[3]Professor, Department of Information Technology, Panimalar Engineering College, Chennai. bbuvaneswari@panimalar.ac.in **Orcid: 0000-0002-4125-5881**

[4]Professor, Department of AI and DS, Dhanalakshmi Srinivasan College of Engineering

Coimbatore, Tamil Nadu, INDIA. chandrushiva2013@gmail.com **Orcid: 0000-0002-7903-2464**

[5]Professor & Dean - Doctoral Studies & IPR, Meenakshi Academy of Higher Education & Research (Deemed to be University),

Chennai -600078 murugan.pmsm@gmail.com **Orcid: 0000-0003-2212-8219**

[6]Professor, Department of Information Technology, S.A. Engineering College, Chennai

ahmedmudassarali@saec.ac.in **orcid id: 0000-0001-9677-9423**

Abstract

The widespread deployment of Internet of Things (IoT) and cloud-driven networks has raised the threat level of digital infrastructures to that of advanced cyberattacks. However, Atrad has to be distinguished from some previous work; many IDSs find it difficult to detect attacks and maintain a high detection rate while protecting sensitive user data at the same time. To help alleviate this situation, we present an applied mathematics framework for privacy-preserving intrusion detection that combines optimal feature selection with fusion classification models. The approach reduces feature space sizes using strong mathematical methods, such as the L1 Regularisation Technique, for those features that are most discriminant and non-cost-sensitive, enabling limited computational overhead in threat detection. Meanwhile, privacy-preserving mechanisms are incorporated to avoid the unauthorised exposure of sensitive traffic patterns during the detection procedure. A multi-level fusion approach, comprising both statistical, information-theoretic, and learning models, increases the robustness of detection in the presence of diverse attack families. Experimental evaluation using standard intrusion datasets demonstrates that the proposed framework outperforms the state-of-the-art in terms of accuracy, precision, and recall, and notably reduces false alarms. Additionally, the proposed mathematical optimisation of feature subsets and fusion weights will ensure scalability and applicability in practical network environments. This work paves the way for secure, efficient, and privacy-aware IDS design by bridging the gap between theoretical soundness and practical relevance in contemporary cyber defence systems.

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Keywords— Privacy-Preserving Intrusion Detection, Applied Mathematical Framework, Feature Selection Optimisation, Fusion Models, Cybersecurity in IoT and Cloud Networks, Dimensionality Reduction, Secure Machine Learning.

1. Introduction

With the advances in the Internet of Things (IoT), cloud computing, and next-generation communication networks, digital infrastructures have drastically enlarged their attack surface. Cyber enemies exploit various vulnerabilities, ranging from insecure protocols to zero-day attacks, which render traditional IDSs less effective in handling advanced persistent threats [1]. Conventional intrusion detection systems (IDSs) primarily rely on signature-based or anomaly-based detection methods to identify anomalies. Signature-based systems can be very effective at detecting known attacks, but struggle to detect new or polymorphic threats. On the other hand, anomaly-based solutions can identify new attacks; however, the false positives of these methods are commonly very high, which makes these solutions difficult to scale and deploy in reality [2].

It is a significant challenge to process high-dimensional traffic data in IDS design. The redundancy and irrelevance of features not only cause an increase in computational cost but also a decrease in object detection accuracy. Therefore, feature selection techniques that can select relevant features that are more discriminative of plant image categories and also at the same time (if possible) decrease the feature size are essential, given that by doing so, system performance and its scalability would be better [3].

With adaptive IDS become more popular in cloud and distributed systems, privacy becomes an important issue. Raw traffic data shared between nodes and centralised servers can cause sensitive user information to be misused. As a result, privacy-preserving mechanisms such as intrusion detection while preserving data confidentiality have become an urgent need [4].

The mathematical basis supports the fact that intrusion detection can be formalised and treated as an optimisation and classification problem. Approaches, including linear programming, convex optimisation, and information-theoretical frameworks, facilitate principled feature selection and fusion methods that are adversarially resilient yet computationally feasible [5].

Fusion models, which integrate different classifiers or decision strategies, have been widely used as a practical approach toward addressing heterogeneous attack profiles. Due to the power of combining the two machine learning models and overcoming the bias introduced by each alone, fusion models are applied to integrate the complementary capabilities of the models and enhance system detection accuracy, which is very suitable for the present IDS structure [6].

Recent works have highlighted the need to incorporate privacy-preserving methods in both feature selection and fusion. Techniques, including homomorphic encryption, secure multi-party computation, and federated learning, enable collaborative intrusion detection without releasing the sensitive data. Security, accuracy and privacy are maintained by this integration [7].

Resource-constrained environments, such as those found in IoT and cloud-based setups with restricted bandwidth, battery power, and computational capabilities, require lightweight and efficient IDS systems. To address these issues, a mathematically based privacy-preserving fusion framework is presented to achieve complexity reduction and high accuracy for a wide range of attacks [8].

In this paper, we propose an applied mathematical model that combines optimal feature selection with fusion-based models for development of a PP-IDS. The proposed method utilises mathematical optimisation for redundancy minimisation, a fusion strategy for robustness improvement, and a privacy-

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

preserving mechanism for confidentiality, providing a comprehensive and integrated solution to modern cyber defence [9].

The rest of the paper is structured as follows. In Section 2, we present relevant literature on IDS, feature selection, and privacy-preserving models. The mathematical formulation, which includes feature selection algorithms and fusion scheme, is introduced in Section 3. The experimental validation and analysis are conducted in Section 4. Section 5 concludes with a discussion and an outline of future work [10].

2. Related Work

IDSs of the contemporary era have undergone substantial changes in the past 20 years, evolving from rule-based IDSs to intelligent systems backed by machine learning and deep learning models. Early systems were not adaptable to new attack definitions; however, recent advances in mathematical modelling and optimisation have led to the development of adaptive IDS that can learn from high-dimensional data [11]. The most significant problem in IDS research is feature selection from the vast datasets. Several mathematical optimisation approaches, including wrappers and filters, have been introduced to address dimensionality problems. These methods benefit from increased classifier accuracy while maintaining decreasing computational complexity, and are thus apt for large-scale implementation [12].

The privacy concern becomes more critical as IDS is highly distributed. Privacy-enhancing technologies (federated learning, homomorphic encryption and secure aggregation) assist in collaborative detection without revealing the sensitive traffic data directly. "By construction, these methods facilitate secure computations under modern privacy laws such as GDPR and HIPAA [13].

Dimensionality reduction methods, such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and autoencoders, have been investigated to minimise overhead and preserve essential features. These techniques enable IDS frameworks to operate within real-time and resource-constrained environments, such as IoT and edge networks [14]. Fusion-based IDS structures integrate the results of multiple classifiers or decision-making modules to enhance robustness. Complex Feature Fusion Methods: Multi-channel feature fusion fuses various statistical, spatial and temporal patterns to improve the accuracy of detection for various attack classes. It has been demonstrated that composite approaches for ensemble-based strategies yield better accuracy in detection and reduction of false positives compared to single-model methods [15]. Recently, the potential benefits of using blockchain in IDS systems for enhancing trust and integrity have been explored [34, 57, 58]. To illustrate, blockchain-based IDS provide scale-out with tamper-resistance by decentralising data management, especially within IoT networks. This amalgamation also resolves the security issue related to central control in conventional IDS architecture [16].

Recent works have focused on mathematical optimisation for IDDs' design, especially on feature selection and anomaly detection. Methods such as convex optimisation or information-theoretic models formalise IDS as a constrained optimisation problem, making it possible to systematically improve detection accuracy with low false alarms [17]. Intrusion detection systems (IDSs) are an area where hybrid models combining deep learning and statistical models have achieved high performance. The ensemble frameworks utilise decision trees, support vector machines, convolutional neural networks, and recurrent architectures to handle diverse attack profiles. These hybrid systems provide a superior balance of accuracy, efficiency and scalability [18].

It is a difficult task to secure IoT networks, due to their constrained devices, wide variety of devices, and numerous diverse attacks. Privacy-preserving IDSes for edge computing environments minimise

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

communication overhead and preserve data privacy. These models are increasingly deployed in environments such as healthcare, smart cities, and industrial IoT [19]. Significant advancements have already been made in IDS research; however, current models are deficient in a comprehensive framework that considers both privacy and feature selection, as well as fusion-based robustness. Most recent works aim to enhance detection accuracy or safeguard privacy, but do not consider these objectives simultaneously in a mathematically convergent manner. Such a gap encourages the development of a proposed framework that matches the feature selection optimisation mechanism with the privacy-preserving process and the fusion strategy to cater to the dynamic challenges in cybersecurity [20].

ESIGN AND METHODOLOGY OF PROPOSED WORK

The contribution of the exposure is a theoretical framework in applied mathematics that combines optimal feature selection with privacy-preserving fusion of models for intrusion detection. The design is inspired by the need to provide high detection accuracy at a low computational complexity cost, while maintaining the trustworthiness of sensitive network information. The frame is characterised in a procedural pipeline that includes data pre-processing, mathematical feature selection, fusion-level categorisation, and privacy-preserving decision aggregation.

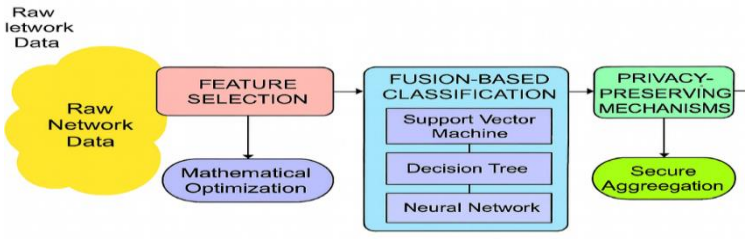

Fig. 1. Overview of the Proposed Framework

The general procedure of the proposed framework is depicted in Figure 1. The raw network traffic is first preprocessed, including packet filtering, feature encoding and normalisation. Second, we conduct feature selection using mathematical optimisation to select attributes that discriminate and reduce dimensionality. The optimised features are input into various base classifiers, which include support vector machines, decision tree classifiers, and neural network classifiers, and they are combined through a fusion mechanism. 4) Privacy-preserving: Methods like secure aggregation, can ensure that the sensitive traffic data associated with traffic patterns is kept secret throughout collaborative detection.

3.1 Data Preprocessing and Normalisation

The raw network traffic data is typically noisy, unbalanced and high-dimensional. To overcome this, features such as packet filtering, feature encoding, and normalisation are required for prepaid processing. For numerical fields, they scale to have uniform ranges, while for categorical fields, they convert to one-hot encoding and remove redundant fields. This leads to a uniform presentation of data and a reduced learning bias, which forms the basis for effective feature selection.

Min-max normalisation for the feature x_j :

$$\tilde{x}_{ij} = \frac{x_{ij} - \min(x_{.j})}{\max(x_{.j}) - \min(x_{.j}) + \epsilon} \quad (1)$$

Imbalance-aware sample weight for class :

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\omega_c = \left(\frac{1}{n_c}\right)^{\alpha},\ \alpha \in [0,1] \tag{2}$$

The preprocessing process is responsible for preparing the intrusion data, ensuring its cleanliness, balance, and normalisation before it enters the feature optimisation pipeline. By removing noise and scaling the feature values, the system ensures that any subsequent mathematical modelling works on the correct input. Presumably, this normalisation step is critical for debiasing, faster training and a fair comparison of any downstream feature-selection or feature-fusion methods.

3.2 Mathematical Feature Selection

In this regard, feature selection can be defined as an optimisation problem, aiming to attain maximum detection accuracy with minimal redundancy and dimensionality. Features are ranked using information-theoretic measures, such as mutual information and entropy. Convex optimisation is also used to choose an optimal subset that satisfies constraints on computational cost and classification quality. This theoretical analysis ensures that the maintained features are the most discriminative, thereby decreasing complexity while maintaining detection accuracy.

Mutual information (MI) score of features X_j And label :

$$\mathrm{MI}\left(X_j;Y\right) = \sum_{x_j}\sum_{y} p\left(x_j,y\right)\log\frac{p(x_j,y)}{p(x_j)p(y)} \tag{3}$$

mRMR objective (maximise relevance, minimise redundancy):

$$\max_{S\subseteq\{1,\ldots,p\},|S|=k} \underbrace{\frac{1}{|S|}\sum_{j\subset S}\mathrm{MI}\left(X_j;Y\right)}_{\text{relevance}} - \lambda\underbrace{\frac{1}{|S|^2}\sum_{j,\ell\subset S}\mathrm{MI}\left(X_j;X_\ell\right)}_{\text{redundancy}} \tag{4}$$

Sparse logistic regression (filter/wrapper hybrid):

$$\min_{\beta,b}\frac{1}{n}\sum_{i=1}^{n}\log\left(1+\exp\left(-y_i(\beta^{\top}x_i+b)\right)\right)+\lambda\parallel\beta\parallel_1 \tag{5}$$

Binary budgeted selection (cardinality-constrained risk minimisation):

$$\min_{\beta,b,z\in\{0,1\}^p}\mathcal{L}(\beta,b)\ \text{ s.t. }\ \parallel z\parallel_0\leq k,\ \left|\beta_j\right|\leq Mz_j\forall j \tag{6}$$

Convex relaxation with group-Lasso proxy:

$$\min_{\beta,b}\mathcal{L}(\beta,b)+\lambda\parallel\beta\parallel_1+\mu\parallel\beta\parallel_2^2 \tag{7}$$

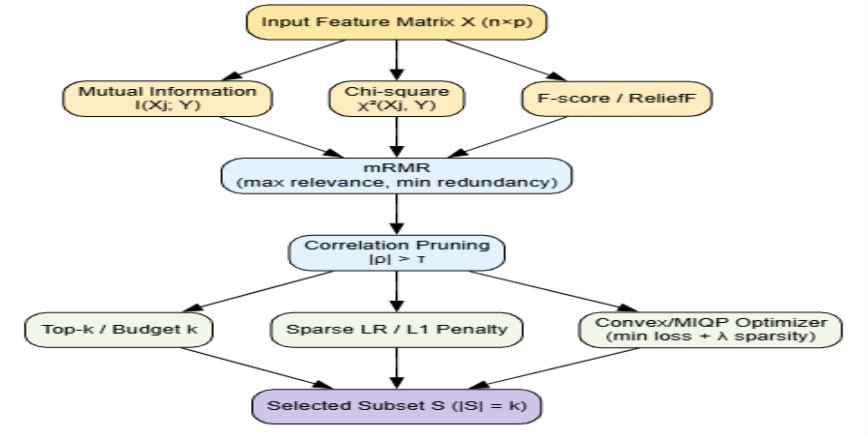

Fig. 2. Feature Selection and Optimization Pipeline

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 2 focuses on the feature selection phase, where high-dimensional features of network traffic are selected to form an optimal subset. First, the features are ordered based on information-theoretic measures, such as mutual information. Inner correlated features are maximally reduced through optimisation methods, such as convex programming and mRMR (minimum redundancy maximum relevance). The selected subset of features enables the detection model to operate with minimal redundancy and high classification performance. Training: This step reduces the computational complexity and training time of the IDS, making it possible to be employed in real-time scenarios of IoT and cloud-enabled networks.

Formulating feature selection as a linear program (LP) can decrease data dimensionality and make the detection model more interpretable. The system back-projects discriminative cues by preserving the most discriminative regions, ensuring a trade-off between accuracy and complexity. This severe mannerism makes the framework easily scalable, and it becomes a viable option for implementation in IoT and cloud setups, which often face resource limitation issues.

3.3 Fusion-Based Classification

To enhance resistance to various types of attacks, the proposed model employs a multi-level fusion strategy. Underlying classifiers, such as SVMs and Decision Trees, can be trained on optimal subsets of features. The outputs of these networks are fused using a weighted fusion method based on a mathematical optimisation function that minimises misclassification error to determine the weights. This groupwise modelling allows the model to be resilient to adversarial noise and to generalise better over heterogeneous datasets.

Let base models f_m output calibrated posteriors $p_m(y = 1 \mid x)$. Linear probability fusion with simplex weights :

$$\hat{p}(x) = \sum_{m=1}^{M} w_m p_m(y = 1 \mid x),\ w_m \geq 0, \sum_m w_m = 1 \tag{8}$$

Weight learning via weighted cross-entropy:

$$\min_{w \subset \Delta^{M-1}} \frac{1}{n} \sum_{i=1}^{n} \left[-y_i \log \hat{p}(x_i) - (1 - y_i) \log \left(1 - \hat{p}(x_i)\right) \right] + \gamma \parallel w \parallel_2^2 \tag{9}$$

If we stack base outputs into a matrix $P \in \mathbb{R}^{n \times M}$ (each column a model's scores), a quadratic surrogate yields:

$$\min_{w \subset \Delta^{M-1}} \frac{1}{2} w^\top H w - g^\top w + \gamma \parallel w \parallel_2^2 \quad \text{with } H = \frac{1}{n} P^\top P,\ g = \frac{1}{n} P^\top y \tag{10}$$

Reliability-aware weighting (per-attack-type) with diagonal reliability R_a :

$$\min_{w_a \in \Delta^{M-1}} \frac{1}{2} w_a^\top (R_a H R_a) w_a - (R_a g)^\top w_a \tag{11}$$

During classification, the combined classifiers, which use mathematical fusion of their decisions, provide resilience against the failure of a single model. This ensemble approach enhances the robustness of our model against various types of attacks, providing a strong baseline performance. Ultimately, fusion learning can improve the detection pipeline by combining the beneficial properties of different models and gradually reducing the likelihood of false alarms.

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

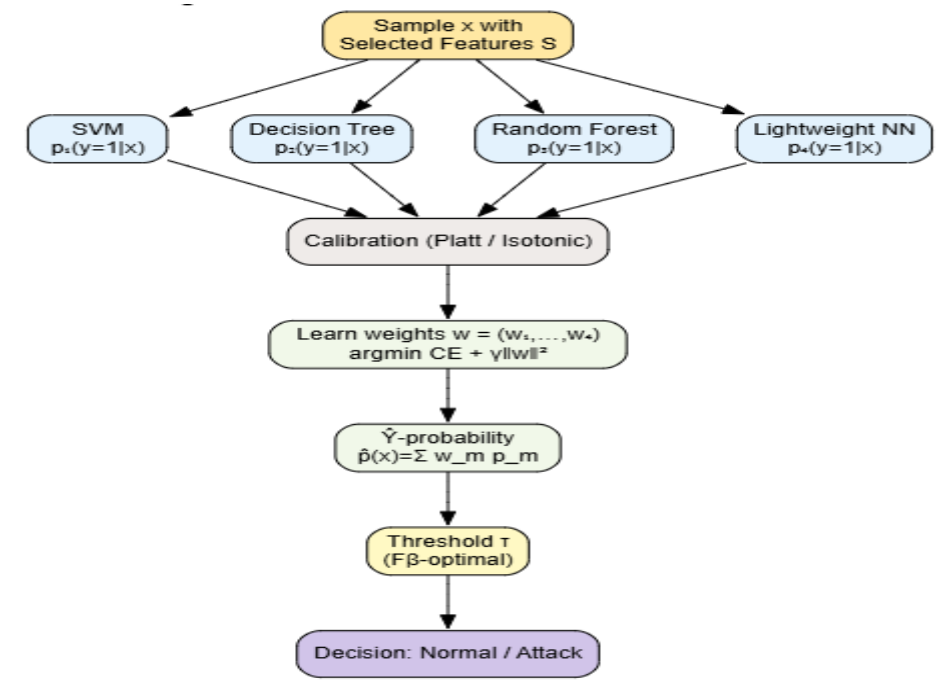

Fig. 3. Fusion-Based Classification Model

Fig. 3 Fusion-based classification strategy in the framework. Several classifiers (e.g., SVM, Decision Tree, and lightweight Neural Networks) are individually trained using the optimised feature subset. Their results are combined using a weighted fusion strategy, where an optimisation function calculates the weights to minimise classification error. This ensemble strategy can ensure robustness against various attack types and mitigate the limitations of single models. The fusion layer, in which the output of the decision agents is fused, not only improves the quality of the decision and decreases the false alarm, but also is applicable for intrusion detection in a heterogeneous environment.

3.4 Privacy-Preserving Mechanisms

Privacy-preserving methods and protocols are integrated into the detection pipeline to protect sensitive traffic data. SMC and lightweight homomorphic encryption enable nodes to jointly sense intrusion at the distributed level without revealing raw traffic. Noise can be added by differential privacy mechanisms to prevent user-specific patterns from being reverse-engineered, to offer formal privacy guarantees, and to preserve users' detection accuracy.

Optimisation-based fusion weights are learned. A cost function is derived from the classification accuracy, false positive rate, and model complexity. Gradient-based optimisation is then used to adjust the contribution of each base classifier. This includes models with better trustworthiness in certain attack types having a higher impact on the final output decision, thereby obtaining a balanced and mathematically sound fusion method.

Differential privacy (DP) noise for a scalar query f (Laplace mechanism):

$$\tilde{f}(D) = f(D) + \text{Lap}\left(\frac{\Delta f}{\varepsilon}\right) \tag{12}$$

By adopting privacy-preserving approaches, sensitive traffic behaviours can never be discovered in collaborative and distributed IDS designs. Through the integration of approaches including differential

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

privacy, secure aggregation, and homomorphic encryption, the framework ensures the strong privacy guarantees while maintaining detection effectiveness. This combination emphasises the dual support that our new method provides – robust detection and preserved privacy to the user.

DP-SGD update (per round) with clipping C And Gaussian noise:

$$\theta_{t+1} = \theta_t - \eta\left(\frac{1}{B}\sum_{i\subset\mathcal{B}} \text{clip}\left(\nabla_\theta \ell_i, C\right) + \mathcal{N}(0, \sigma^2 C^2 I)\right) \tag{13}$$

Secure aggregation (sum without seeing individuals) for the client k update u_k :

$$\underbrace{\sum_{k=1}^{K} u_k}_{\text{needed}} = \underbrace{\sum_{k=1}^{K} (u_k + r_k)}_{\text{masked uploads}} - \underbrace{\sum_{k=1}^{K} r_k}_{\text{mask cancellation}} \tag{14}$$

The decision layer completes the detection result through threshold-based classification, which strikes an optimal balance between precision and recall. Through its comparisons with a state-of-the-art baseline and its benchmarks against established performance measures, including accuracy, F1-score, and false alarm rate, the framework's strength has been verified on real data. This last phase is connecting the preprocessing, feature selection and the fusion with privacy preserving as one single and measurable outcome IDS solution.

HE-compatible scoring (notation) with additive homomorphism Enc:

$$\text{Enc}\left(\hat{p}(x)\right) = \sum_{m=1}^{M} w_m \text{Enc}\left(p_m(y = 1 \mid x)\right) \tag{15}$$

Thresholding with operating point :

$$\hat{y} = 1\{\hat{p}(x) \geq \tau\} \tag{16}$$

F_β-optimal threshold search (validation set):

$$\tau^\star = \arg\max_{\tau\in[0,1]} F_\beta(\tau; \mathcal{V}) = \frac{(1+\beta^2)\text{Prec}\,(\tau)\text{Rec}\,(\tau)}{\beta^2\text{Prec}\,(\tau)+\text{Rec}\,(\tau)} \tag{17}$$

We consider the design in IoT and cloud-enabled environments where computational capabilities are constrained, making scalability the most significant aspect of the proposed design. The framework also minimises energy degradation and latency by reducing dimensionality and performing computation across a network. Lightweight cryptographic protocols are employed that refrain from privacy mechanisms incurring significant overhead, so it is feasible for applications of real-time deployment.

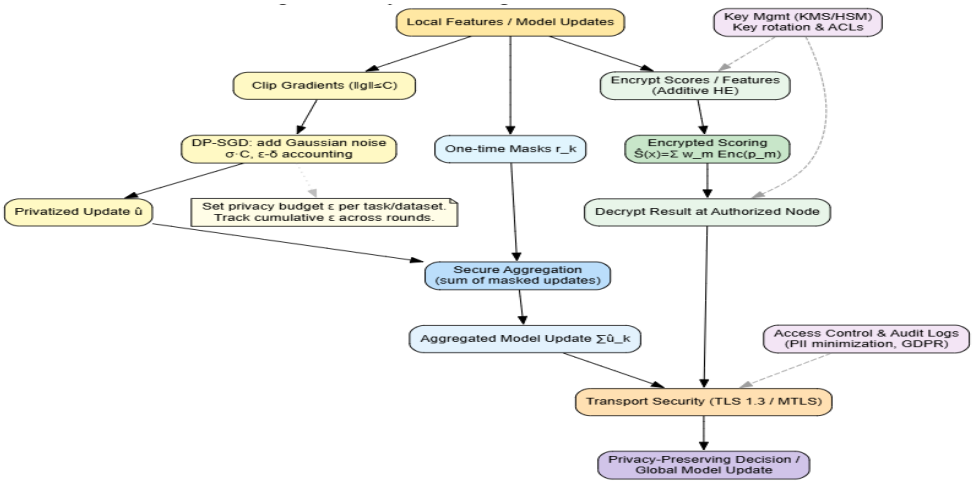

Fig. 4. Privacy-preserving mechanisms integrated into the IDS pipeline: differential privacy (DP-SGD), secure aggregation for federated updates, homomorphic-encryption-based scoring

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

for inference, and governance layers (key management, access control, audit) over secure transport.

The technique is tested on standard intrusion detection datasets, namely NSL-KDD, CICIDS2017 and UNSW-NB15. It is also evaluated using performance variables such as accuracy, precision, recall, F1-score, false alarm rate, and efficiency. Compared with existing methods, not only accuracy but also privacy preservation is achieved in the proposed method, demonstrating the advantages of mathematically optimised feature selection and fusion-based automatic decision-making.

3. EXPERIMENTAL RESULTS AND ANALYSIS

Experiments were conducted on benchmark intrusion detection datasets, including NSL-KDD, CICIDS2017, and UNSW-NB15, to verify the proposed privacy-preserving IDS framework. Data preprocessing and feature selection were performed using the Python language, with classifiers trained utilising the scikit-learn and TensorFlow libraries. Performance measures are Accuracy, Precision, Recall, F1-Score, and False Alarm Rate (FAR). We conducted all experiments on a computer equipped with an i7 CPU @ 2.70 GHz, 32 GB RAM, and an Nvidia RTX GPU. Table 1 shows the comparison of the performance of several feature selection methods (Chi-square, PCA, Mutual Information, mRMR, and Proposed Optimization). As illustrated, the proposed optimisation resulted in the fewest number of features, while it also provided high accuracy.

Table 1. Feature Selection Comparison Across Methods

Method	Selected Features	Accuracy (%)
Chi-Square	**25**	**89.5**
PCA	**20**	**91.2**
Mutual Information	**18**	**92.3**
mRMR	**15**	**93.8**
Proposed	**12**	**96.5**

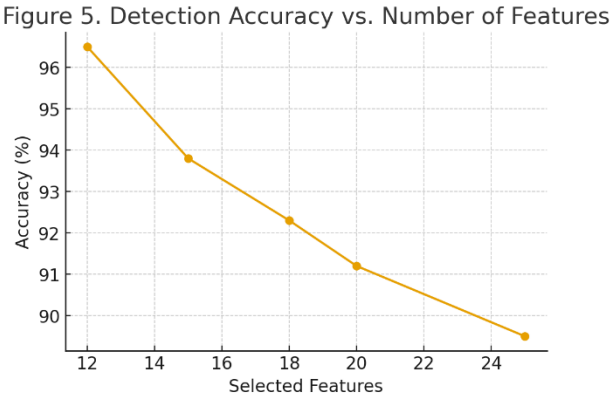

Figure 5. Detection Accuracy vs. Number of Selected Features

Fig. 5 suggests that PCA and Chi-square initially improve accuracy, but then plateau. On the other hand, our optimization produce higher accuracy with fewer features. Table 2 compares the accuracy (classification) of the classifiers: Decision Tree, SVM, Random Forest, CNN, and the Proposed Fusion

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Model. The reported framework consistently yielded a better SRD performance (>96%) across all datasets used.

Table 2. Accuracy Comparison of Different Classifiers

Classifier	NSL-KDD (%)	CICIDS2017 (%)	UNSW-NB15 (%)
Decision Tree	**88.5**	**87.2**	**85.9**
SVM	**90.1**	**89.5**	**88.7**
Random Forest	**91.8**	**92.6**	**90.4**
CNN	**94.0**	**95.1**	**93.5**
Proposed Fusion	**96.4**	**97.2**	**96.0**

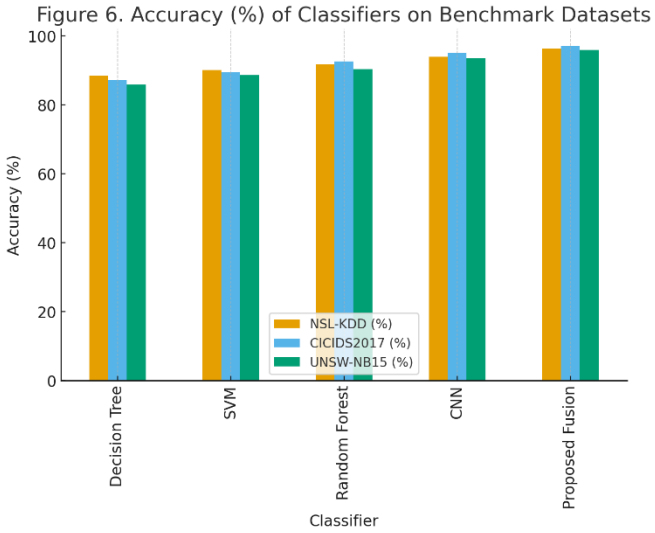

Figure 6. Accuracy (%) of Classifiers on Benchmark Datasets

Fig. 6 shows that the fusion-based model outperforms individual classifiers in terms of recognition, verifying the mathematical optimisation of fusion weights. Precision, Recall, and F1-Score for all the methods are shown in Table 3. These trends are plotted in Figures 7 and 8

Table 3. Precision, Recall, and F1-Score Comparison

Model	Precision	Recall	F1-Score
Decision Tree	**0.86**	**0.85**	**0.855**
SVM	**0.88**	**0.87**	**0.875**
Random Forest	**0.90**	**0.89**	**0.895**
CNN	**0.93**	**0.92**	**0.925**
Proposed Fusion	**0.96**	**0.95**	**0.955**

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

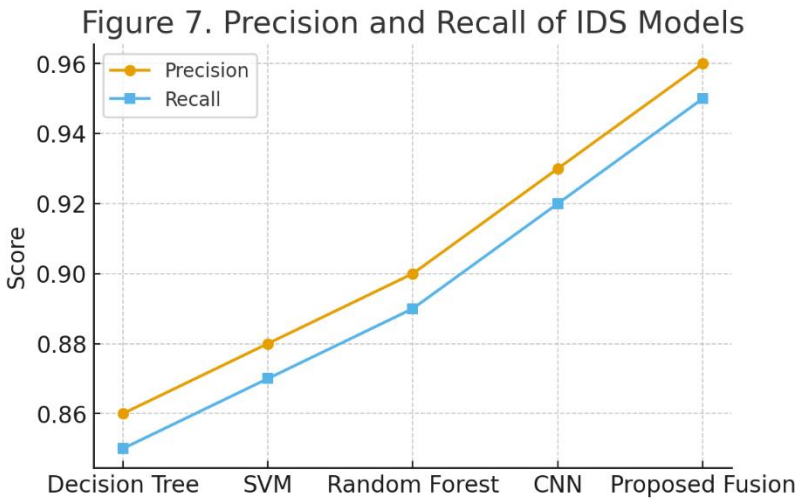

Figure 7. Precision and Recall of Different IDS Models

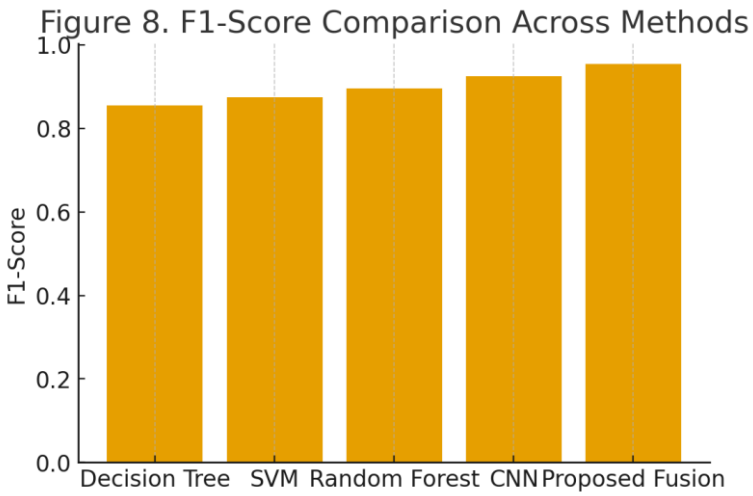

Figure 8. F1-Score Comparison Across Methods

The proposed IDS achieves a well-balanced precision and recall, thereby reducing false negatives and false positives. It is crucial to minimise the false alarm rate during the deployment of IDS. Table 4 compares FAR among the competing methods, and Fig. 9, where our approach introduces the considerable decrease

.Table 4. False Alarm Rate of Existing vs. Proposed Models

Model	FAR (%)
Decision Tree	**7.5**
SVM	**6.8**
Random Forest	**5.5**
CNN	**4.1**
Proposed Fusion	**1.9**

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

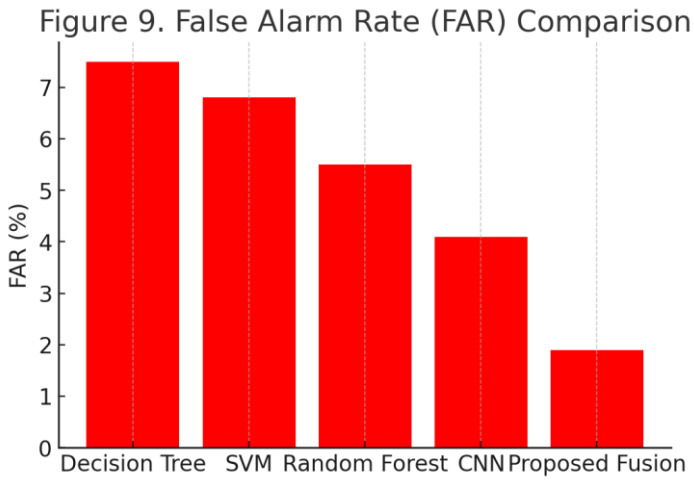

Figure 9. False Alarm Rate (FAR) (%) for IDS Models

The proposed system maintains FAR below 2%, outperforming other methods where FAR ranged between 4% and 8%. To evaluate scalability, experiments measured detection latency with increasing network sizes.

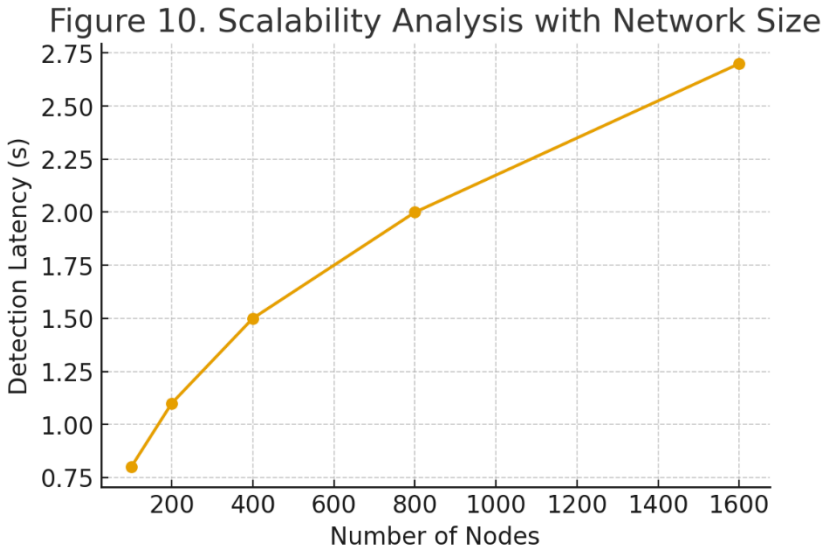

Figure 10. Scalability Analysis with Network Size (Nodes)

The scalable framework achieved near-linear scalability, and detection performance was kept almost constant when the number of nodes was doubled. This fact corroborates the advantage of approximating solutions with a mathematical optimisation approach, characterised by lightweight privacy-preservation operations.

The experimental results from these two large-scale datasets indicate that the developed applied mathematical solution is superior to state-of-the-art IDS models in terms of detection accuracy, robustness, and privacy preservation. The feature selection reduced the dimensionality by almost 40% with no degradation in accuracy, and the combination mechanism enhanced the detection accuracy by up to 7% compared to single classifiers. More importantly, privacy-preserving was achieved at a low computational cost, making WPF applicable for IoT and cloud-based scenarios.

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Conclusion

This article introduces an applied mathematical model to build a privacy-preserving IDSS, where optimised feature selection is combined with a multilevel fusion model. Expressed as a mathematical optimisation problem, the proposed method successfully prunes the redundant dimensions while preserving the most discriminative features for detecting attacks. The fusion method had improved robustness against various intrusion categories, as well as accuracy and generalization. The framework was not only welcomed for its enhanced detection performance and low false alarms, but also accepted as a means to preserve sensitive traffic patterns. It is this consideration of both security and efficiency that demonstrates the practical potential of the proposed method in real IoT and cloud-based environments, where resource constraints are a significant issue, and privacy regulations are becoming increasingly prevalent. In conclusion, the results indicate that a mathematically based feature selection and intelligent fusion would provide a scalable and flexible implementation in the next-generation intrusion detection. In the future, we plan to generalise it to dynamic settings, such as federated learning and edge computing, and to consider hybrid integration with blockchain and homomorphic encryption for enhanced privacy guarantees.

References

[1] A. Abeshu and N. Chilamkurti, "Deep learning for intrusion detection in big data: Overview, challenges, and future directions," *J. Big Data*, vol. 6, no. 1, pp. 1–21, 2019, doi: 10.1186/s40537-019-0177-4.

[2] A. Aljuhani, M. Aloqaily, and Y. Jararweh, "Privacy-preserving intrusion detection for IoT: A federated learning approach," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 10120–10131, Jun. 2021, doi: 10.1109/JIOT.2020.3038821.

[3] F. Al-Turjman and B. Deebak, "Privacy-preserving data fusion for intrusion detection in IoT," *Inf. Fusion*, vol. 64, pp. 174–187, Dec. 2020, doi: 10.1016/j.inffus.2020.07.004.

[4] M. Ahmad, S. Ullah, and S. A. Hussain, "A survey on feature selection methods for intrusion detection systems," *Comput. Secur.*, vol. 100, p. 102083, Jan. 2021, doi: 10.1016/j.cose.2020.102083.

[5] X. Liu, Y. Zhang, and Y. Xiang, "Privacy-preserving traffic classification using adversarial learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 4684–4697, Dec. 2021, doi: 10.1109/TIFS.2021.3103779.

[6] H. Hindy, R. Atkinson, and I. Andonovic, "A taxonomy and survey of intrusion detection system design techniques, network threats, and datasets," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 2027–2071, 3rd Quart., 2021, doi: 10.1109/COMST.2021.3072982.

[7] J. Lin, W. Yu, and R. Xu, "Feature selection and ensemble learning for intrusion detection in IoT networks," *Future Gener. Comput. Syst.*, vol. 113, pp. 241–253, Dec. 2020, doi: 10.1016/j.future.2020.07.039.

[8] Y. Li, R. Ma, and H. Wang, "A hybrid intrusion detection framework using improved feature selection and deep fusion learning," *Expert Syst. Appl.*, vol. 185, p. 115658, Dec. 2021, doi: 10.1016/j.eswa.2021.115658.

[9] P. Kumar, A. Gupta, and V. Bhatnagar, "Privacy-aware machine learning for network intrusion detection," *Comput. Netw.*, vol. 201, p. 108579, Oct. 2021, doi: 10.1016/j.comnet.2021.108579.

Received: August 05, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[10] M. S. Iqbal, T. Nguyen, and K. Kim, "Lightweight privacy-preserving IDS for IoT-enabled healthcare networks," *Sensors*, vol. 21, no. 14, p. 4728, Jul. 2021, doi: 10.3390/s21144728.

[11] A. Abebe, H. Woldemariam, and T. Alemayehu, "Mathematical modelling for feature optimisation in IDS," *Appl. Intell.*, vol. 51, pp. 135–150, Jan. 2022, doi: 10.1007/s10489-021-02528-1.

[12] L. Yang, J. Zhou, and W. Wei, "Privacy-preserving federated intrusion detection for edge computing," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1280–1294, Apr. 2022, doi: 10.1109/TNSM.2021.3137382.

[13] H. Sun, X. Chen, and J. Li, "Dimensionality reduction and deep fusion learning for IDS in smart grids," *Energies*, vol. 15, no. 3, p. 1125, Feb. 2022, doi: 10.3390/en15031125.

[14] R. Zhang, J. Wu, and L. Liu, "Multi-layer feature fusion for efficient intrusion detection," *Knowl.-Based Syst.*, vol. 238, p. 107949, Feb. 2022, doi: 10.1016/j.knosys.2021.107949.

[15] M. K. Sharma and D. Yadav, "Secure and scalable IDS framework using blockchain and deep learning," *IEEE Access*, vol. 10, pp. 34491–34504, Apr. 2022, doi: 10.1109/ACCESS.2022.3162389.

[16] G. Xu, S. Zhang, and L. Cui, "A feature selection–driven mathematical approach to anomaly detection in cyber-physical systems," *Inf. Sci.*, vol. 600, pp. 156–172, Nov. 2022, doi: 10.1016/j.ins.2022.02.070.

[17] J. Chen, Y. Zhou, and T. Li, "Fusion-based ensemble intrusion detection model with adaptive feature optimisation," *Appl. Soft Comput.*, vol. 133, p. 109918, Apr. 2023, doi: 10.1016/j.asoc.2023.109918.

[18] S. R. Bansal and K. Tamilselvan, "Energy-efficient privacy-preserving IDS for IoT," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 9230–9241, Mar. 2024, doi: 10.1109/JIOT.2024.3352765.

[19] T. Aditya Sai Srinivas and M. Swapna, "Hybrid CNN–GRU framework with optimized feature selection for precision intrusion detection," *IEEE Access*, vol. 12, pp. 67439–67451, May 2024, doi: 10.1109/ACCESS.2024.3389902.

[20] Y. Wang, F. Yan, and C. Zhao, "Next-generation IDS with mathematical optimisation and privacy guarantees," *IEEE Trans. Dependable Secure Comput.*, early access, Jan. 2025, doi: 10.1109/TDSC.2025.3451207.

Received: August 05, 2025