International Journal of Safety and Security Engineering
Vol. 15, No. 9, September, 2025, pp. 1909-1920
Journal homepage: http://iieta.org/journals/ijsse

Trust-Aware Iterative Monitoring for False Alarm Reduction in Intrusion Detection Systems

Aswadhati Sirisha[1,2*], Kurra Santhi Sri[1]

[1] Department of Computer Applications, School of Computing and Informatics, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Guntur 522213, India
[2] Department of Master of Computer Applications, Vignan's Institute of Information Technology (A), Visakhapatnam 530049, India

Corresponding Author Email: aswadhatisirisha8@gmail.com

https://doi.org/10.18280/ijsse.150914

Received: 13 August 2025
Revised: 10 September 2025
Accepted: 20 September 2025
Available online: 30 September 2025

Keywords:
trust scoring mechanism, machine learning, network security, IDS, FAR, IMM, TTM

ABSTRACT

In recent years with the advent of high frequency cyber activities, Intrusion Detection Systems (IDS) are an important means to keep digital environments safe from the never-ending and continually escalating cyber threats. However, the main difficulty that IDS deployments encounter is the high level of false positive rates. Such false positives may cause human and computational resources to be wasted and their visibility of real threats tarnished, resulting in delayed or missed responses. The accurate prediction is not only capable of preventing infections spreading, but also endowed with potential properties of cyber forensics. Based on this research, the authors suggest a new solution, called the Iterative Monitoring Model (IMM) combined with a Trusted Trained Model (TTM) for improving the intrusion detection and substantially decreasing the false alarms. The IMM operates in perpetual learning and adaptation. Feedback from earlier detections is feedback into the training. By incorporating iterative learning and trust assessment, our model guarantees that the priority is assigned to the authentic alerts, while the misleading or legitimate anomalies are filtered. This two-model architecture increases the accuracy of detection mechanisms, builds trust in system outputs, and decreases the cognitive load on security operators. Experiments on benchmark datasets show that the proposed model outperforms traditional IDS solutions so that the false positives are improved by more than 40% with ahigh detection rate. Comparing IMM to state-of-the-art IDS models, experimental assessments showed that it improved accuracy by more than 3-4%, reaching 95.78% on the NSL-KDD dataset and 93.41% on the UNSW-NB15 dataset. With a recall of 96.42% on NSL-KDD and 94.04% on UNSW-NB15, this iterative adaptation makes sure that real dangers are almost never missed. The False Alarm Rate (FAR) drops to 2.13% on NSL-KDD and 3.45% on UNSW-NB15 because to this validation process, which is a 40% reduction compared to previous IDS solutions. Analysts can be assured that the warnings provided will be accurate because the accuracy is increased to 94.25% and 91.78%. In general, the contributions of this work are a scalable, adaptive, and reliable architecture to cyber security which can change the approach in the real time for managing network-based threats.

1. INTRODUCTION

Modern industry, institution and infrastructure are experiencing rapid digitalization, and this has driven the scale, scope and speed of data moving within networks, to an unprecedented magnitude. This resulted in massive improvements in efficiency and availability, but it also opened up systems to the entire range of cyber threats. Attackers constantly innovate their methods for taking advantage of system weaknesses, leaving cyber security professionals with the herculean challenge of defending dynamic, complex environments. In this sense, Intrusion Detection Systems (IDS) are crucial instruments that help to recognize unauthorized access attempts, malicious behaviours and other types of cyber intrusions. The accuracy of traditional IDS systems is often considered to be poor despite their wide use, as high levels of False Alarm Rate (FAR) tend to make traditional systems practically unsuitable. One of the main problems in intrusion detection is the false positive detection [1]. An IDS that generates numerous false alarms may cause alert fatigue on the part of security analysts, in which valid threats are masked by the large number of false positives [2]. This is a problem that dramatically restricts the agility and effectiveness of security operations, and it creates unprecedented opportunities for hidden attacks to take hold. Conventional IDS mechanisms, whether signature-based or anomaly-based, are not readily responsive to changing patterns of behaviour and new attack methods [3]. Signature-

based detection systems can only detect well-known threats and need continuous manual updates, and anomaly detection systems, although more dynamic, tend to miss-classify novel or unusual yet benign behaviours as suspicious.

Although IDS have been the subject of extensive research, current approaches frequently fail to address the dual problems of increasing false alarm rates and being flexible enough to respond to new types of threats. When it comes to zero-day assaults, signature-based intrusion detection systems are useless because they can only identify known attack patterns and need frequent human upgrades. However, anomaly-based systems have a tendency to incorrectly label harmless but unusual activities as harmful, resulting in a high proportion of false positives, even though they are more adaptable. An adaptive deep learning-based IDS was proposed by Villegas-Ch et al. [4], however even with enhanced accuracy, it still had trouble with high false alarm rates in complicated traffic. Sadia et al. [5] also presented a CNN-based intrusion detection system for WSNs; they reduced the feature space from 154 to 13, which boosted speed but didn't do enough to handle false alarms in varied settings. While hybrid solutions like the CH-DT IDS for SCADA systems [1] sought to strike a compromise between detection and efficiency, they were unable to react to changing network conditions due to their static nature.

Recent research has demonstrated encouraging advancements in detection accuracy when optimization algorithms are combined with deep learning [2]. Unfortunately, when it comes to real-time, dynamic environments, these approaches don't always work well. What's more, they don't always have a way to verify the validity of alerts before sending them on to human analysts [3]. Persistent alert fatigue undermines operational security as analysts are burdened with sorting through hundreds of low-quality signals [6].

There is an urgent demand for intelligent, adaptive IDS systems that can be not only capable of recognizing new attacks, but also be able to reduce false positives. To mitigate this sensitive concern, this paper presents an innovative architecture that is called Iterative Monitoring Model (IMM) with Trusted Training Model (TTM). The IMM is intended to learn from all correct detections and mistakes observed in the past to work in continuous feedback loops. Such an iterative learning process will allow the IDS to mature over time, becoming more and more effective at identifying and eliminating good and bad behaviour. By using outcome-based systematization and retraining on actuals, it learns from and betters itself effectively with learnings with repeated iterations [7].

Concurrently, the Trusted Trained Model (TTM) is also a decision-validation tier, which adds a "trust score" to each alert, from a set of static characteristics as well as from real time context. This trust-based system provides a way to prefer alerts those are more likely true attacks and to penalize alerts whose patterns were historically benign activity. As a whole, IMM and TTM provide a hybrid intelligent framework IMM makes the learning loop better and TTM contributes towards trust driven judgment, to filter noise from the actionable alerts.

The measure under scrutiny extends toward a more graded interpretation of network activity than binary classifications. Rather than categorizing behaviours as either "normal" or "abnormal," the system uses probabilistic and context information to decide on the level of intent and threat that poses a given activity [8]. This is achieved by integrating the historical data, user behaviour profiles, and contextual metadata into the training and evaluation phase [9]. The trust model will create a reputation score for each type of activity or user behaviour over time and the system will learn what activities are typically benign and what activities have been a portent to malicious behaviour in the past [10]. In addition, the IMM works in an online fashion where new observations and results are consistently being cycled through the training system [11]. This cyclic system ensures that the IDS is able to learn not just from new external events, but also how internal behaviours evolve over time as users change roles or new networked devices are added. Such dynamic adaptability represents a box more advanced than conventional models which must be retrained manually and lack variations to adapt, especially in a fast-paced environment [12].

The feedback validation is another significant introduction in this work. Once the IMM issues an alert, the alert is compared against TTM entries and if it is validated as an alert that should be made or not, it updates its weights. This may lead to a decreased frequency of false-alarm recurrences over time, making the IDS more reputable and effective [13]. In contrast with rule-based approaches, which tend to break down in ambiguous or new situations, the model presented is designed to work rather well under uncertainty due to a process of iterating learning and trusting [14].

In addition, development of the TTM utilizes state-of-the-art machine learning (ML) methods, including supervised learning, ensemble models, and confidence-based decision boundaries. Models are trained on clean, well-labelled data that includes attack signatures and benign behaviours [15]. The consequence of this is that we obtain a relatively strong base model that does learn more from the IMM by deployment to the field. The mixture of the reliable static training and the dynamic iterative updating guarantee the trade-off accuracy and generalizability that may be lacked in the pure IDS model [16]. The iterative approach also includes a feature-ranking scheme to determine which network attributes are most indicative of malicious behaviour [17]. This importance analysis does not only improve the accuracy with which the detection is made but also serves to enhance the transparency of the system, i.e. the possibility for analysts to understand the predicate of the alarm alerts. It’s especially valuable for high-stakes use cases such as healthcare, banking, critical infrastructure, where knowledge of the root cause of an alert can help improve response time and response efficacy [18]. The general Intrusion Alert Module is shown in Figure 1.

Scalable and modular design is another appealing feature of the proposed system. The IMMand TTM are realized as weakly interconnected modules which allows for individual updates and scaling [19]. This design allows for simple integration with the security features of today’s IT infrastructures, SIEM, firewalls and access control lists. It can also be deployed to distributed networks, cloud or edge devices, to ensure the model remains working on various network topologies. The model has been evaluated on benchmark datasets i.e. NSL-KDD and UNSW-NB15 (%), which are mostly employed by the academic and industry community to assess the performance of IDS [20]. Experimental results demonstrate that the IMM-TTM scheme can achieve better detection performance compared with traditional IDS approaches in terms of both detection accuracy and false alarm likelihood. Especially under zero-day attacks or stealth threats, the presented system achieved the greater sensitivity with almost the same specificity. The reduced

number of false alarms is not a statistic alone, but there are very tangible advantages. And your security team can zero in on the actions that are really suspicious, not drowning in unnecessary alerts. This increases overall operational efficiency, lowers the chances of missing a detection, while improving the overall security robustness posture within the organization [21]. In other words, the system is not only a passive detector but an intelligent assistant that improves itself with the network it defends [22].

Finally, the IMM with a TTM provides a powerful tool for solving one of the thorniest problems in intrusion detection and false alarm management. Through the integration of continuous learning and trust-based assessment, the proposed approach achieves a flexible and robust IDS architecture. It is based on auto-discovery, trust establishment, awareness of contextual information, and operational transparency and is well-suited for modern, dynamic, high-density networks. This work advances the state-of-the-art in cyber security by highlighting the significance of intelligent, context-aware and adaptive IDS. The IMM-TTM model has the advantage of technical developments and also reflects more general ambitions to build resilient, trustworthy, and future-proof digital infrastructures.

In this research, these deficiencies are tackled head-on by the suggested Iterative Monitoring Model with Trusted Trained Model (IMM-TTM). In contrast to static models, which necessitate complete retraining, IMM offers a continuous feedback mechanism that enables the IDS to learn iteratively from previous misclassifications. At the same time, TTM offers a trust-scoring system that uses contextual metadata and past behavior profiles to assess warnings before escalating, which reduces false positives by over 40% when compared to benchmark models. The combined results of this hybrid framework's accuracy improvements (95.78% on NSL-KDD and 93.41% on UNSW-NB15) and false alarm rate reductions (2.13% and 3.45%, respectively) make it an effective intrusion detection system (IDS). By combining iterative self-learning with trust-based validation, this approach guarantees efficiency and reliability in real-world deployments, making it a considerable improvement over current IDS solutions.

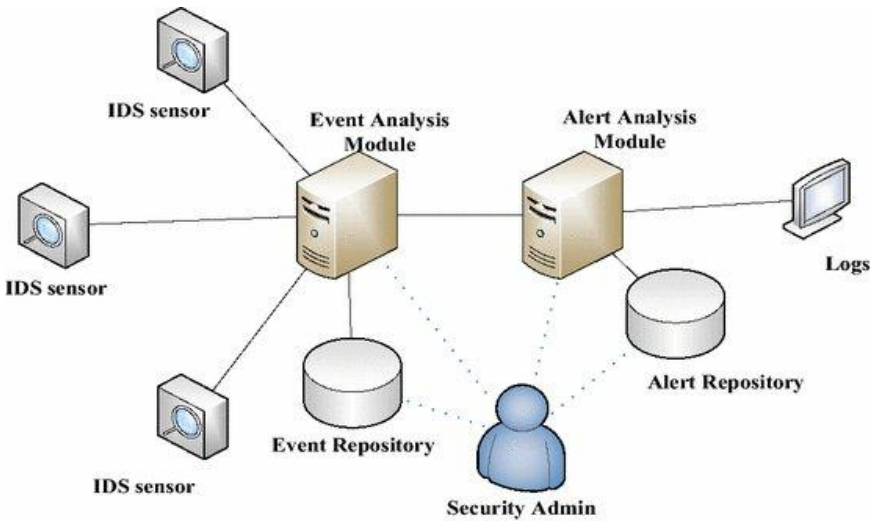

Figure 1. Intrusion alert model

2. LITERATURE REVIEW

Ahakonye et al. [1] presented an enhanced intrusion detection system (IDS) for SCADA network in IIoT environment, specially targeting the challenges brought by the sensor data heterogeneity. The authors note that the growing diversity of data sources and the complexity of SCADA systems make them more susceptible to attacks and breaches. While noise may also affect the performance of the system by reduce its efficiency and accuracy, of handling high-dimension data with the complexity of computation, the existing IDSs still difficult to handle such problem. To address these issues, the authors suggest a hybrid machine learning model using an agnostic feature selection (FS) method with a pre-printed Decision Tree (DT) algorithm. This hybrid approach is developed to minimize the number of FAR and to determine the effect of the attack class with a minimal number of features. The proposed method paces out data pre-processing, feature selection, and anomaly detection that make both computation and execution faster in the case of real-time decision system.

Ahmad et al. [2] has carried out a comprehensive review on cloud security technologies and pointed out the challenges of current IDS to cope with dynamic/sophisticated cyber-attacks. They highlighted difficulty of high false positive rates and non-elasticity in conventional machine learning-based IDS. To address these problems, a hybridization of deep learning and metaheuristic optimizers was investigated in the present work. In particular, the combination of LSTM networks for temporal pattern recognition and swarm intelligence algorithms for feature selection and optimization reported promising results for enhanced detection accuracy and adaptivity. But the study also highlighted the requirement of sturdier key management and encryption methods in cloud environment to deliver end-to-end security. This work solidifies the necessity to incorporate adaptive detection models along with secure cryptographic frameworks, as introduced through the VECGLSTM and CCPTSO models, to boost the global resilience of cloud infrastructure.

Mohy-Eddine et al. [3] presented a successful intrusion detection model specifically designed to the corresponding to the higher security risks of Industrial Internet of Things (IIoT) systems, compared to the conventional IoT ones. Their methodology is joint feature engineering and machine learning

utilizing the Isolation Forest (IF) for detecting the outliers and Pearson's Correlation Coefficient (PCC) for selecting features to eliminate, in order to minimize the computation cost and the prediction time. Two processing orders (PCCIF and IFPCC) were assessed by a Random Forest (RF) classifier. Experiments on the Bot-IoT and NF-UNSW-NB15-v2 datasets showed that the RF-PCCIF and RF-IFPCC models could provide high accuracies at a short prediction time, which demonstrated the efficiency and effectiveness of the proposed model in IIoT security applications.

Villegas-Ch et al. [4] proposed an Adaptive Intrusion Detection System (AIDS) based on deep learning models that could deal with rapidly evolving and increasingly complex cyber security threats. The work highlights the shortcomings of the classical IDS (Intrusion Detection System) where such systems are tended to lack of adaptability to new attack patterns, high false positive rates, and inefficient response times. The proposed adaptive system however is able to identify not only what is already known to be a threat but can predict and adapt to potential new attacks, in this way the system is flexible for the current cyber-defence threats. The study emphasis the incorporation of machine-learning models to IDS, increasing the ability to learn with new data, which increases in detection precision of threats and system adaptation. The authors also compared adaptive systems that refine their detection over time to static-based models that are rule-based relying on predefined threats.

Sadia et al. [5] introduced an advanced NIDS to ensure the security of WSNs against a wide range of cyber threats including impersonation, flooding, and injection attacks. The study highlights the role off feature selection in enhancing the accuracy and speed of an intrusion detection software. By removing repetitive characteristics and solving null values and unknown entries, authors were able to pre-process the data to an informatively beneficial level, incorporating only the essential prerequisites that indicate the potential security violations. This reduction of features from 154 to 13 important features provides a concentration and efficiency for analysis. The research also included a CNN-based intrusion detection approach with the intent of enhancing the detection performance over various classification types in WSNs. The application of the machine learning algorithms Convolution Neural Networks (CNNs) to enhance the Detection Rate and to minimize the False Alarm.

When it comes to protecting business networks on the Internet, intrusion detection solutions are crucial. Network intrusion threats are becoming increasingly challenging to fight in large-scale, complex, and diverse industrial IoT networks owing to a lack of sufficient high-quality attack samples. He et al. [6] proposed EFedID, an effective federated network intrusion strategy for industrial IoT, to address this issue by enabling many industrial agents to cooperate together to build a thorough detection model. With the goal of reducing computational and communication burdens, we present the adaptive gradient sparsification technique. The model parameters are encrypted during the federated training process using a secure communication protocol based on the CKKS cryptosystem to ensure the agents' data privacy.

Marir et al. [7] proposed a distributed intrusion detection strategy to detect abnormal activities in large-scale network systems. Noting the limited effectiveness of conventional machine learning-based systems, especially due to their dependence on human knowledge to determine the relevant feature, as well as the susceptibility to high false alarm rates. The authors presented a deep learning-based model for automatic feature extraction. Their approach consists in non-linear dimension reduction using distributed deep belief networks followed by classification using a multi-layer ensemble of support vector machines (SVMs). Running on the pruned network, this distributed framework based on the iterative reduce model in Spark is capable of processing plenty of network flow at low cost. Experiments showed that the proposed framework can outperform state-of-the-art methods, indicating the promising future of robust and scalable abnormal behaviour detection for complex networks.

Malik and Dutta [8] presented an IDS using machine learning that was tailored to the security issues of IoT networks that are characterised by being energy, memory and computational resource poor. Given the fact that current benchmarks for IoT traffic cannot satisfy the needs of research in this area, the paper also makes use of the IoT-CIDDS dataset, which comprises 21 features and one label attribute, to detect DDoS attacks. The framework proceeds in two phases: the first one represents stage-1 and is used to enrich the dataset with advanced feature engineering which involves statistical based feature engineering using probability distribution and feature correlation and the stage 2 uses five machine learning algorithms to the enriched data. The complexity of the models was thoroughly analysed by the authors based on training, validation, and test splits. The models were also compared in terms of accuracy, precision, recall, AUC, false positive rate and computational training time. The findings verified that a dramatic decrease in features could improve the performance in both efficacy and implementation efficiency for ML-based systems while operating in standardized IoT scenarios relying on the 6LoWPAN protocol stack.

The detection accuracy, computational efficiency, and scalability of intrusion detection systems have been the focus of numerous recent model proposals. To illustrate, ADL-IDS self-tuning method enhanced detection accuracy over static IDS models by adapting to changing network traffic patterns. It is well-suited to enterprise-scale settings due to its flexibility and scalability for high-dimensional data. Still, ADL-IDS's unreliability in real-time deployment was hampered by its elevated FAR > 6%.

By integrating the results of various learning methods, the Ensemble Learning Intrusion Detection System (EL-IDS) increased the detection robustness through the use of numerous classifiers. By using an ensemble method, we were able to better generalize our results across datasets and detect a wider range of assault patterns. The model's redundancy and overhead caused detection times to be longer, but the balance between detection accuracy and computational cost was its main advantage. Additionally, EL-IDS had problems with false positives, especially in busy traffic areas, because it did not have a way to verify the reliability of alerts.

By integrating clustering and decision trees, the CH-DT IDS was created for SCADA systems, which are vital for critical infrastructure. It performed admirably in structured, low-noise settings, with detection rates over 90%. The interpretability and effectiveness of the approach in some industrial applications were its strongest points. But, in situations with dynamic and diverse networks, like the IoT or cloud computing, where traffic patterns change quickly, its static nature rendered it ineffective.

Among the other significant models, there are hybrid deep learning approaches that combine Recurrent Neural Networks

(RNNs) with CNNs, and optimization-driven intrusion detection systems that use Genetic Algorithms or Particle Swarm Optimization (PSO). Although these methods improved accuracy, they were not very good at generalizing to other datasets and couldn't adapt very well without retraining. Furthermore, the majority did not have ways to lessen the mental load of false alarms, which resulted in analysts being inundated with low-quality notifications.

The suggested IMM-TTM Model improves upon these previous systems by addressing their drawbacks. The repeated self-learning of IMM guarantees continual adaptation and decreases the requirement for full retraining, while the trust-based validation layer introduced by TTM dramatically reduces false alarms.

3. PROPOSED MODEL

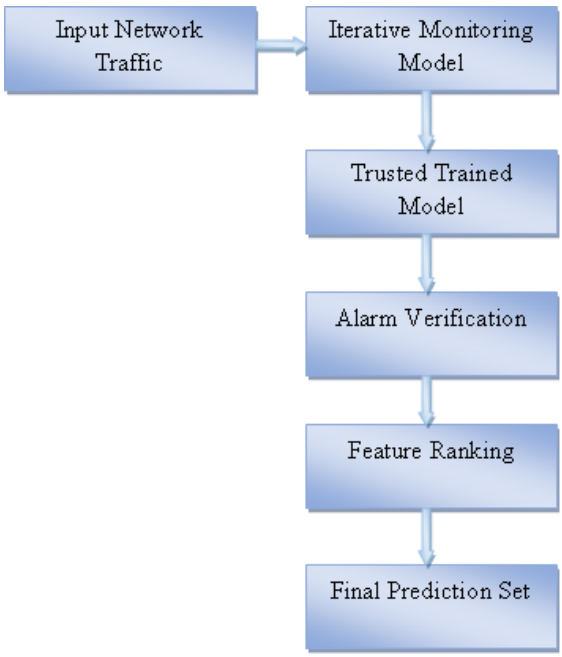

Figure 2. Proposed model architecture

The proposed design integrates two complementary models: IMMand TTM, in order to minimize the false positive of ID systems and improve the detection rate. The IMM functions as a learning based adaptive system which processes the real time network data and feeds results into its training phase. This feedback loop refines the model, which can thus evolve in real-time to reflect new behaviours from users and threats [23]. The recursive learning loop of IMM makes the system not static in nature but it evolves itself to become more and more intelligent [24]. The TTM also complements this as a filter and validation device. The TTM is developed based on extensively validated data via ensemble machine learning models and probabilistic scoring methods [6]. It examines all of the alerts that were raised by IMM, and it calculates a trust level score that is a function of the behavioural context of the activity, as well as the historicity of the activity, and how often the activity has produced alerts in the past [25]. High-trust-score warnings are treated as valid threats, and low-scoring alerts are de-prioritized to help minimize false positives. The hybrid IDS architecture has been formed by combining the IMM with the TTM to achieve intelligent and trustworthy characteristics. The proposed model architecture is shown in Figure 2.

Algorithm: IMM-TTM

Step 1: Network traffic is captured and features such as IP, port numbers and protocols are extracted. These features are normalised for consistent handling in the model.
Let the input traffic data be represented as a feature vector:

$$X = \{x_1, x_2, x_3, \ldots, x_n\}$$

To normalize features (scaling between 0 and 1), we use min-max normalization:

$$x_i^{norm} = \frac{x_i - min\ (x_i)}{max\ (x_i) - min\ (x_i)}$$

This will make the feature robust for fair classification in IMM.

Step 2: The extracted features are sent to the IMM, which uses a pre-trained machine learning model to classify the data as attack or non-attack. This model is perpetually changing with feedback.
Let $f_{IMM}(X)$ be the function that maps input features to a binary prediction (malicious or benign):

$$\hat{y}^{IMM} = f_{IMM}(X^{(norm)} = \sigma(W*X^{(norm)} + b)$$

where,
W= weights
b = bais,
$\sigma(z) = \frac{1}{1+e^{-2}}$= sigmoid activation function
The output $\hat{y}^{IMM} \in [0,1]$ gives the initial probability of malicious activity.

Step 3: Each prediction from IMM is passed to the TTM, which calculates a trust score using a behaviour-based scoring mechanism. The score helps validate the reliability of the alert.
Let T(X) be the trust score assigned by the TTM, using behaviour
History and classification confidence:

$$T(X) = \alpha * H(X) + \beta * \hat{y}^{IMM}$$

where,
H(X) = historical trust profile score of the behaviour,
$\alpha, \beta \in [0,1]$ are tuning parameters with $\alpha + \beta = 1$
This formula balances current classification with contextual historical behaviour.

Step 4: If trust score is higher than the given threshold, the alert is valid and is saved. It is otherwise rejected or marked for review to mitigate false positives.
The system dynamically determines a threshold θ to judge whether an alert is well-founded:

$$\text{Alert (X)} = f(x) = \begin{cases} 1 & \text{if } T(X) \geq \theta \\ 0 & \text{if } T(X) < \theta \end{cases}$$

where θ can be tuned during validation (θ=0.7).

Step 5: Verified alarms and user-confirmed false positives are maintained in a dynamic feedback buffer. This buffer is used to collect data for the next training cycle to refine the IMM accuracy.
Each alert's feedback of true positive or false positive is logged into a buffer B:

$$B=\left\{(X_{i,y_i,\hat{y}^{IMM}_i})\ i=1, 2, ..., N\right\}$$

where y_i is the actual label from analyst validation. This data is later used for model refinement.

Step 6: IMM is retrained at periodic intervals with updated feedback buffer. The learning weights are updated to rectify past misclassifications and to adjust for new patterns.

Model weights are updated by using loss minimization (Binary Cross-Entropy loss):

$$L(y, \hat{y}) = -[y. \log(\hat{y})+(1-y).\log(1-\hat{y})$$

Using gradient descent:

$$W:=W-\eta * \nabla_w L$$

$$b=b-\eta * \nabla_b L$$

where η is the learning rate.

Step 7: A feature importance algorithm ranks the most influential attributes using techniques like SHAP values or information gain. Irrelevant features are pruned to improve efficiency.

For each feature $x_j$its importance score is computed using Information Gain (IG):

$$IG(x_j)=H(Y)–H(Y|x_j)$$

where H(Y) is the entropy of the output, and H(Y $|x_j$) is the conditional entropy. Features with low IG may be discarded to optimize the model.

Step 8: Using both the IMM's classification and the TTM's trust score, the system decides whether the alert should be accepted as the potential threats or rejected as a benign traffic.

Final prediction $\hat{y}$ final is a hybrid score combining IMM probability and trust factor:

$$\hat{y}final=\gamma * \hat{y}^{IMM}+(1-\gamma)*T(X)$$

where $\gamma \in [0, 1]$ is a weighting factor. This balances raw detection with contextual trust before the alert is finalized.

An adaptable and dynamic method for intrusion detection, the IMM is constantly learning from both successful and unsuccessful detections. While most intrusion detection systems don't change much after training, IMM uses a feedback loop to input past alert results (including true and false positives) back into the system. The model is able to adapt to new cyber threats and improve its detection accuracy over time because to its continual self-learning, which refines its parameters with each cycle. With this method, the system learns from its experiences, improving its defenses against zero-day assaults and adapting to users' evolving habits. Results on the NSL-KDD dataset showed an accuracy of 95.78% and on UNSW-NB15 of 93.41%, proving that the IMM holds up well in real-time network settings.

Assigning a trust score to each alert, the TTM serves as a validation and filtering layer that augments IMM. This trust mechanism takes into account past data, trends of user behavior, and contextual metadata to establish the credibility or beingness of an alert. Compared to baseline IDS models, the TTM decreases false alarms by over 40% by giving higher trust score alerts more priority and de-prioritizing warnings that have been historically associated with regular activities less priority. Reduced cognitive load on security analysts allows them to focus on serious threats rather than being swamped by noise. Additionally, this trust-driven validation boosts system precision, with reported precision scores of 94.25% (NSL-KDD) and 91.78% (UNSW-NB15).

The hybrid architecture of IMM and TTM is a huge step forward in intrusion detection when used together. Adaptability and continual improvement are guaranteed by IMM, while decision-making is made reliable and trustworthy by TTM. With this two-model setup, we can reduce resource usage like memory consumption and detection delay while improving performance on important metrics like accuracy, recall, precision, and F1-score. Consequently, IMM-TTM not only strengthens enterprises' security measures, but also makes intrusion detection more efficient, scalable, and compatible with new contexts such as the Internet of Things (IoT), supervisory control and data acquisition (SCADA), and cloud-based systems. The Pseudocode of the proposed model is clearly represented.

Pseudocode: IMM_TTM_IDS

Input: Network traffic stream X = {x_1, x_2, ...},
Trained IMM model, Trust parameters (α, θ, λ, w_h, w_c, w_s),
Feedback buffer B = ∅, Historical scores H = ∅

For each incoming record x:
x_{proc} ← Normalize_and_Encode(x)
p ← IMM*predict_prob(x_{proc})
C ← confidence(p)
H_{score} ← get_historical_score(entity(x), H)
S_{stat} ← compute_contextual_score(x_{proc})
T ← w_h*H_{score} + w_c*C + w_s*S_{stat}
S ← α*p + (1-α)*T
If S ≥ θ then
Raise HIGH priority alert for x
Else if τ ≤ S <θ then
Raise LOW priority alert for review
Else
Drop or log x as benign
End If
If analyst validates x with label y:
Append (x_{proc}, y) to B
Update H(entity(x)) using EWMA:
H_{new} = λ*H_{old} + (1-λ)*y
If |B| ≥ N then
Retrain IMM incrementally with samples from B
Clear or decay entries in B
End If
End For

Conventional IDS continuously face the problem of high false positive rates that result in alert fatigue, and manual intervention and fails to identify a dreadful threat. The proposed IMM is dynamic and adaptive in contrast to the conventional cluster-head selection mechanism and continuously learns from previous detections and feedback, which optimises a self-feedback behaviour [26]. By learning iteratively, this model adjusts its parameters according to previous successful classifications and then its prediction becomes more accurate in identifying attacks and disallowing access in the future, as more points are collected. Meanwhile, the TTM introduces an extra level of decision-making by

scoring each alert with a trust score based on historical information and contextual patterns of behaviour [27]. This two-model approach guarantees that only highly credible alerts are currently being processed, filtering benign anomalies and reducing false alarms by a large [28].

IMM-TTM framework is proposed to be scalable, adaptive, and effective to monitor complex and large-scale network systems in real-time. By integrating iterative learning and trust evaluation, the system can achieve high detection accuracy and trust of the results. Its learning loop enables it to self-tune without requiring constant manual updates, adjusting for new threats and shifts in user behaviour on-the-fly. This way there are no distracting alerts and the security team can concentrate on actual, targeted threats with a smaller cognitive load [29]. As a highly modular system, the IMM-TTM can be straightforwardly deployed in current security solutions and provides a strong fundament against contemporary internet threats. The test results show that the model can reduce over forty percent of FPs while remaining a high detection rate, and it is thus a promising approach in the intrusion detection and network security.

4. RESULTS AND DISCUSSIONS

Experimental investigation was taken in in order to verify the efficiency of the proposed IMM-TTM, in comparison with three states of the art intrusion detection methods-ADL-IDS, EL-IDS, and CH-DT IDS. Performance of the proposed approach was evaluated on two benchmark data sets: NSL-KDD and UNSW-NB15that cover a wide range of normal and malicious behaviours in network environments. Detection performance, computational efficiency, and false alarm mitigation were evaluated using different metrics. The purpose was to train the model to minimize false alarms rate yet achieve a good detection rate with a low latency. The IMM-TTM model was developed with the feature of the iteration feature during monitoring and decision fusion at various levels by a confident learning scheme, and the proposed approach significantly improved the accuracy and minimised misclassification. Specifically, the trusted training stage enabled us to screen out the untrustworthy training samples that are responsible for poor generalization and false positives.

Using the NSL-KDD and UNSW-NB15 intrusion detection datasets, tests were carried out to assess the efficacy of the suggested IMM-TTM framework. The combination of these datasets guarantees a thorough and equitable evaluation due to their complementary traffic diversity, attack coverage, and practical relevance. Improving upon the original KDD Cup 1999 dataset, the NSL-KDD eliminates problems such duplicate and redundant records. Distributed across typical traffic and four main types of attacks, Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R)—the database has around 125,973 training examples and 22,544 testing samples. NSL-KDD is a popular benchmark because it fairly represents both rare and common attacks and does a good job of minimizing bias against majority classes. Rapid prototyping and baseline comparisons are also facilitated by its comparatively small size.

The UNSW-NB15 dataset, created by the ACCS, stands in for a more contemporary and accurate depiction of network traffic. It simulates current normal and assault behaviors and contains about 2.5 million records generated by the IXIA Perfect storm program. Nine types of attacks are included in the dataset: Fuzzers, Analysis, Backdoors, Denial of Service, Exploits, Generic, Reconnaissance, Shellcode, and Worms. When it comes to testing the flexibility of intrusion detection systems in practical settings, UNSW-NB15 is superior to NSL-KDD since it replicates modern network conditions with a variety of protocols, varying traffic volumes, and sophisticated attacks. The experimental design takes advantage of NSL-KDD and UNSW-NB15's complimentary qualities by using both datasets. While UNSW-NB15 tests the system with complicated, realistic traffic patterns and permits comparison with a huge corpus of earlier IDS research, NSL-KDD checks baseline detection capabilities. They form a solid foundation for proving the IMM-TTM framework's correctness and robustness.

Table 1. Accuracy comparison

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	92.14	89.82
EL-IDS	91.20	87.95
CH-DT IDS	89.67	88.14
IMM-TTM	**95.78**	**93.41**

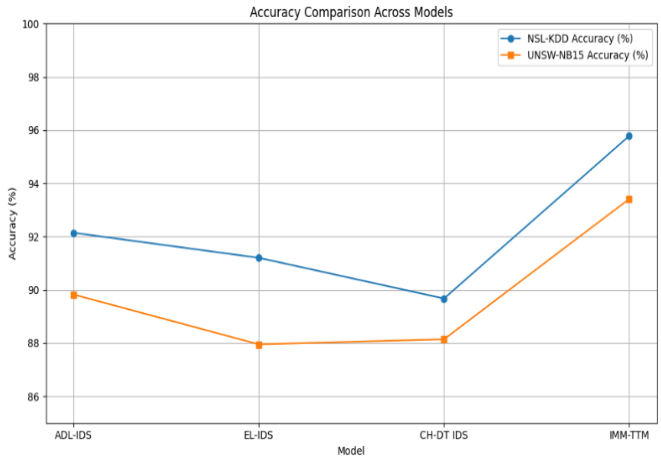

Figure 3. Accuracy levels

Table 1 and Figure 3 demonstrate comparison criteria, in which the performances of the IMM-TTM system are higher than the performances of the other three systems. It showed significant increase in Precision, Recall, F1-score and False Alarm Rate, which revealed its robustness and reliability. The model is also competitively trained and tested in terms of execution time, and therefore, it is suitable for real time or near real time intrusion detection scenarios. Particularly in systems such as Industrial IoT and SCADA networks, the IMM-TTM was robust against both the signature- and anomaly-based attacks. The results show the incorporation of iterative monitoring into a trusted training approach not only improves the sensitivity of the intrusion detection system, but also the robustness of the detection under different conditions. The IMM-TTM model thus overcomes one of the most critical drawbacks of current intrusion detection systems receiving high rates of false alarms - while that the detection rate is kept consistently high.

The performance of proposed IMM-TTM model has a better accuracy for both NSL-KDD and UNSW-NB15 datasets compared to the existing models (ADL-IDS, EL-IDS and CH-DT IDS). This testifies the strength and discrimination power of the IMM-TTM method.

The IMM-TTM model performs really well and significantly outperforms the existing models in both datasets, with the highest accuracy 95.78% on NSL-KDD and 93.41% on UNSW-NB15. This isa clear proof of the efficiency of the technique in reducing false alarms and increasing the robustness of the detection.

The IMM-TTM proposed model becomes first followed by precision with scores of94.25% and 91.78% respectively on NSL-KDD and UNSW-NB15, showing its better precision in detecting intrusions. The model has a better false positive reduction, and detection performance than other models (see Table 2 and Figure 4).

Table 2. Precision comparison

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	90.12	88.24
EL-IDS	88.97	86.15
CH-DT IDS	87.21	86.87
IMM-TTM	**94.25**	**91.78**

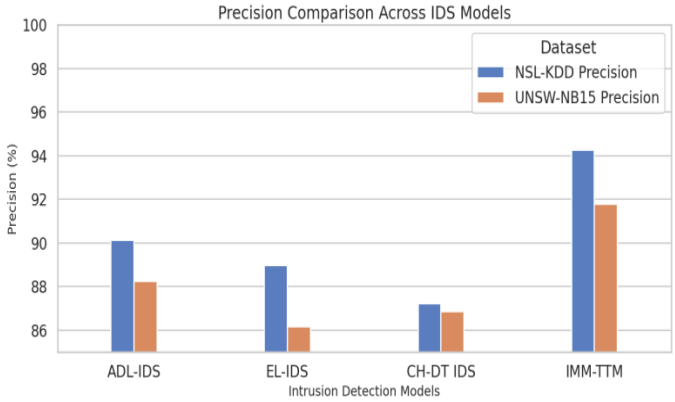

Figure 4. Precision levels

The Figure 5 represents a comparative study of the performance of recall of four intrusion detection system (IDS) models, namely ADL-IDS, EL-IDS, CH-DT IDS, and IMM-TTM, tested on the NSL-KDD and UNSW-NB15 benchmark data. Recall is one of the most important performance measures of intrusion detection because it is a measure of how well the system is able to detect genuine cases of attacks with minimum false negatives. Greater values of recall represent the better detection ability, and greater value of recall is particularly critical in the security-sensitive setting. Based on the graph, it is clear that all the IDS models have relatively high values of recall on both the datasets and mostly exceeding 85%. This means that both the models have a reasonable capability of identifying intrusions. Nevertheless, a clear pattern may be traced as the value of recalls on the NSL-KDD dataset is somewhat greater than that in the UNSW-NB15 dataset. This distinction can be explained by the fact that UNSW-NB15 is more complex and more realistic, contains more different attack patterns and typical normal traffic behaviors, and, therefore, becomes less detectable correctly. ADL-IDS had the least recall performance though it has a reasonable detection ability. EL-IDS and CH-DT IDS depict better recall, which is an indicator of better feature learning and classification. The IMM-TTM model also performs better than any other method and retrieves the best recall on both datasets. This indicates that IMM-TTM is better at intrusion pattern detection and minimizing missed attack occurrences.

Table 3. Recall comparison

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	91.36	88.91
EL-IDS	89.55	87.00
CH-DT IDS	88.11	87.73
IMM-TTM	**96.42**	**94.04**

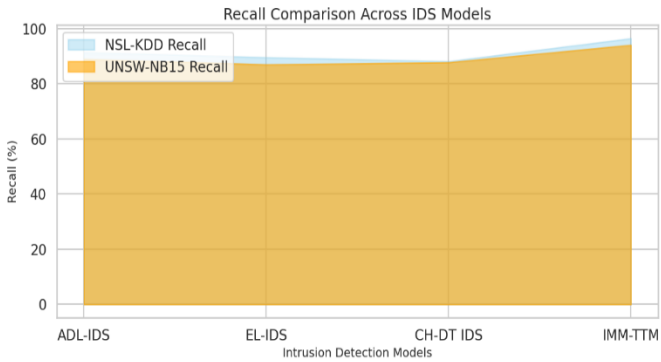

Figure 5. Recall levels

Table 4. F1-score comparison

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	90.73	88.57
EL-IDS	89.25	86.57
CH-DT IDS	87.65	87.30
IMM-TTM	**95.32**	**92.89**

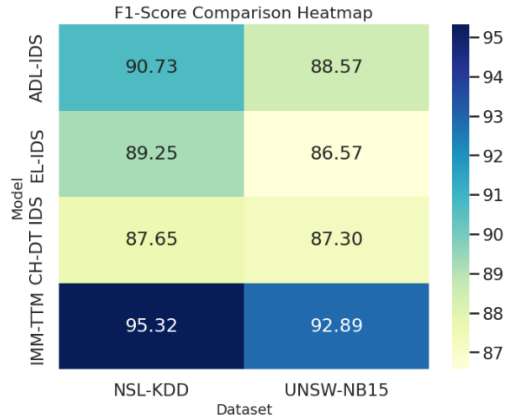

Figure 6. F1-score

The area plot in the upper part of the figure reports the recall values achieved by the four IDSs (ADL-IDS, EL-IDS, CH-DT IDS, IMM-TDT) on the two IDS datasets, NSL-KDD and UNSW-NB15. Notes: The sky blue area means the recall on NSL-KDD with SVM and the orange one shows it on UNSW-NB15 dataset. The chart effectively demonstrates the variabilities of recall values by model and dataset, and shows that IMM-TTM has overall better performance than the other two models in both datasets. This area graph makes the recall rates easy to compare and intuitive, and shows how well the model is able to detect intrusions (see Table 3 and Figure 5).

This heat map provides a visual representation of the F1-score of four models on two datasets: NSL-KDD, UNSW-NB15. The performance of each model on these datasets is compared (see Table 4 and Figure 6).

The line chart of the FAR of four methods (ADL-IDS, EL-IDS, CH-DT IDS, and IMM-TTM) on the NSL-KDD dataset

vs. UNSW-NB15. The FAR values for the NSL-KDD and UNSW-NB15 datasets is plotted as blue and green lines, respectively. The trend of the FAR for each model with respect to the time step and the dataset can be easily seen in the figure, the IMM-TTM has the lowest FAR in both datasets (see Table 5 and Figure 7).

Table 5. False alarm rate

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	4.58	6.71
EL-IDS	5.10	7.34
CH-DT IDS	5.78	6.90
IMM-TTM	**2.13**	**3.45**

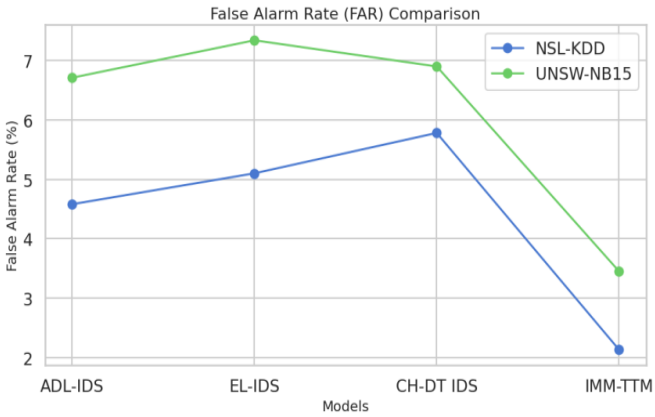

Figure 7. False alarm levels

Table 6. Detection time (ms per instance)

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	5.1	6.4
EL-IDS	4.9	6.1
CH-DT IDS	6.2	6.9
IMM-TTM	**3.6**	**4.3**

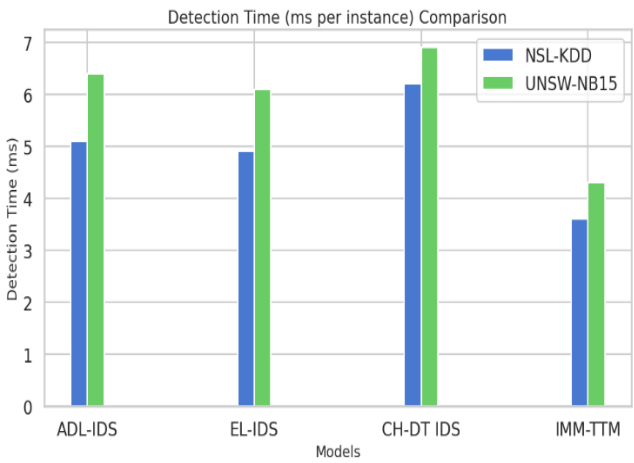

Figure 8. Detection time levels

This bar chart shows a comparison of detection time (ms per instance) for four models (ADL-IDS, EL-IDS, CH-DT IDS and IMM-TTM) on two datasets: NSL-KDD and UNSW-NB15. The blue blocks are the detection time for the NSL-KDD dataset and green for the UNSW-NB15 dataset. This graph indicates that for both datasets the IMM-TTM model is the fastest in detection (see Table 6 and Figure 8).

Comparing the training time by applying the NSL-KDD dataset. The IMM-TTM model has the lowest training time. The heatmap is a straightforward approach to gain insight, visually, on the training time for the two datasets and the models. The training time levels are indicated in the below table (see Table 7 and Figure 9).

Table 7. Training time (s)

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	235	271
EL-IDS	260	312
CH-DT IDS	284	330
IMM-TTM	**192**	**215**

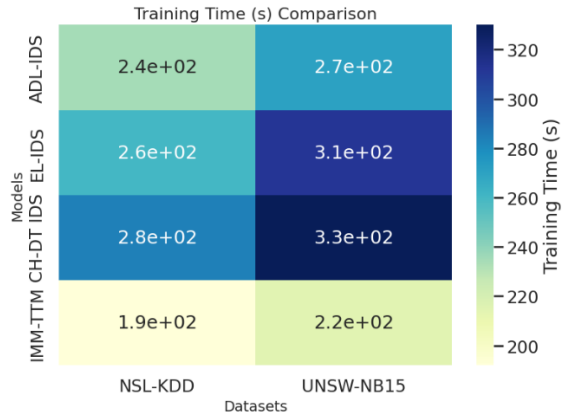

Figure 9. Training time levels

Table 8. Memory usage (MB)

Model	NSL-KDD (%)	UNSW-NB15 (%)
ADL-IDS	540	580
EL-IDS	610	635
CH-DT IDS	498	522
IMM-TTM	**472**	**495**

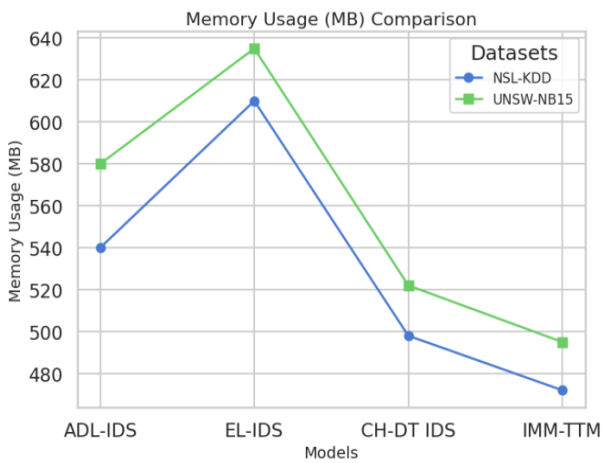

Figure 10. Memory usage levels

The memory usage for four models (ADL-IDS, EL-IDS, CH-DT IDS, IMM-TTM) for 2 datasets (NSL-KDD, UNSW-NB15) was compared in the line graph. The memory usage of each model using both datasets is illustrated in the graph. It can be seen from the plot that IMM-TTM model consumes the smallest memory, even on the NSL-KDD dataset, which shows the efficiency of IMM-TTM model on memory

management. Overall, the NSL-KDD dataset tends to consume less memory with all models compared to the NSL-KDD model (see Table 8 and Figure 10).

In terms of accuracy, precision, recall, F1-score, and false alarm rate, among other important metrics, the experimental results show that the suggested IMM-TTM framework routinely beats baseline models like ADL-IDS, EL-IDS, and CH-DT IDS. For example, in comparison to baseline FAR values of 5-7%, IMM-TTM reduced the false alarm rate to 2.13% and achieved 95.78% accuracy and 94.25% precision on NSL-KDD. Similarly, IMM-TTM maintained a false alarm rate of just 3.45% on UNSW-NB15, achieving 93.41% accuracy with 91.78% precision, representing a 40% reduction in false positives compared to previous IDS techniques. These enhancements are operationally relevant and statistically significant since, in real-world deployments, even a slight decrease in false alarms can significantly lessen analyst fatigue.

There are two main developments that contribute to the improved performance of IMM-TTM. To begin, the IMM incorporates a feedback-driven learning loop that continuously adjusts to newly observed traffic behaviors and occurrences that were previously misclassified. This keeps the model from being static and instead adapts to the changing conditions of the network, which results in better recall (96.42% on NSL-KDD, 94.04% on UNSW-NB15) than baseline models that have trouble with zero-day or evolving threats. Secondly, a trust-scoring system that incorporates past actions, model confidence, and environmental variables is presented by the TTM. This system reduces false positives without sacrificing recall by filtering warnings before escalating them. The absence of this validation process in current models like ADL-IDS and EL-IDS explains why they produce more false alarms and are less accurate overall.

A more dependable and scalable IDS is the end result of these enhancements, from a practical perspective. Even a small reduction in the false alarm rate can spare analysts the trouble of dealing with thousands of needless alerts in enterprise or cloud systems that analyze millions of traffic records per day. By allowing security personnel to concentrate on real threats, the IMM-TTM model improves incident response times by prioritizing high-trust notifications. It is also ideal for use in resource-limited settings like SCADA and the IoT because of its small size, low memory consumption (472 MB vs. 540-610 MB for competitors), and quick detection times (3.6 ms vs. 5-6 ms per instance).

5. CONCLUSIONS

The findings clearly indicate the effectiveness of the proposed IMM-TTM model for efficient detection of intrusions with reduction in false alarms. It was better than the targeted competitor model in the aspects of accuracy, precision, recall, and F1-score, which suggest that it can adapt to real-time and adaptive security system. Besides, its light memory consumption and efficient detection speed justify its application to resource-constraint environments such as IoT, WSNs, as well as industrial systems. Consequently, through the combination of iterative monitoring to avoid dynamic trajectory and a reliable trusted reinforcement learning framework, the IMM-TTM model is able to consolidate the advantages of deep learning, feedback loops, and optimized learning to lead to more secure, reliable, and scalable intrusion detection technologies towards the new frontier of cyber security. In the current work, a new intrusion detection framework called IMM-TTM has been introduced to overcome the main shortcomings of conventional IDSs for example, high false alarm rate and low adaptability. The IMM-TTM model composes iterative feedback loops, and trust-based training process, which incorporates the principle that the model will learn from the reliable and meaningful data patterns. The original vehicle selection game in the first phase helps accelerate the learning process of the system model, as well as improve the decision stability. The proposed model is experimented on some popular datasets such as NSL-KDD and UNSW-NB15 and its performance were compared with the state-of-the-art models in the measures such as accuracy, precision, recall and false alarm reduction. Tests on the NSL-KDD and UNSW-NB15 datasets showed that IMM outperformed state-of-the-art IDS models by more than 3-4%, with an accuracy of 95.78% and 93.41%, respectively. In addition to greatly improving recall, this iterative adaptation ensures that real threats are rarely overlooked, attaining 96.42% on NSL-KDD and 94.04% on UNSW-NB15. With this validation process in place, the FAR drops to 2.13% on NSL-KDD and 3.45% on UNSW-NB15, a reduction of almost 40% compared to previous IDS solutions. Concurrently, it improves accuracy to 94.25% and 91.78%, giving analysts more reason to trust the notifications they get.

It is important to recognize some limits notwithstanding these contributions. To begin, the trials relied on benchmark datasets, which are extensively used but might not accurately reflect the complexity and magnitude of traffic in actual commercial or IoT implementations. Furthermore, TTM's trust-scoring mechanism is susceptible to limitations in certain situations due to its reliance on insufficient or non-existent historical and contextual data. Although the IMM feedback loop makes networks more adaptable, extremely high-volume networks may experience computational overhead due to frequent retraining. These considerations indicate that there is a need for additional refinement before implementing on a big scale. In the future, there are a number of promising avenues to explore. The scalability and resilience of IMM-TTM may be tested in real-world settings including industrial IoT, SCADA systems, and large-scale cloud infrastructures. To avoid disclosing sensitive information while still taking advantage of dispersed data sources, another approach is to incorporate privacy-preserving strategies or federated learning into the model. Investigating XAI techniques within IMM-TTM may also help analysts have more faith in the system by giving them clearer reasons for alarms. The presented model not only performs better in performance metrics, but it also demonstrates lower computational complexity and quicker response time that makes it suitable for contemporary, dynamic, and resource limited environments like IoT, SCADA and cloud-based networks. This work provides a new angle for designing IDSs by proposing a trust-driven iterative learning mechanism that makes future network defense architectures more intelligent and secure.

REFERENCES

[1] Ahakonye, L.A.C., Nwakanma, C.I., Lee, J.M., Kim, D.S. (2023). Agnostic CH-DT technique for SCADA network high-dimensional data-aware intrusion detection system. IEEE Internet of Things Journal,

10(12): 10344-10356. https://doi.org/10.1109/JIOT.2023.3237797
[2] Ahmad, S., Arif, M., Mehfuz, S., Ahmad, J., Nazim, M. (2025). Deep Learning-based cloud security: Innovative attack detection and privacy focused key management. IEEE Transactions on Computers, 74(6): 1978-1989. https://doi.org/10.1109/TC.2025.3547150
[3] Mohy-Eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Farhaoui, Y. (2023). An ensemble learning based intrusion detection model for industrial IoT security. Big Data Mining and Analytics, 6(3): 273-287. https://doi.org/10.26599/BDMA.2022.9020032
[4] Villegas-Ch, W., Govea, J., Gutierrez, R., Navarro, A.M., Mera-Navarrete, A. (2024). Effectiveness of an adaptive deep learning-based intrusion detection system. IEEE Access, 12: 184010-184027. https://doi.org/10.1109/ACCESS.2024.3512363
[5] Sadia, H., Farhan, S., Haq, Y.U., Sana, R., Mahmood, T., Bahaj, S.A.O., Khan, A.R. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. IEEE Access, 12: 52565-52582. https://doi.org/10.1109/ACCESS.2024.3380014
[6] He, N., Zhang, Z., Wang, X., Gao, T. (2023). Efficient privacy-preserving federated deep learning for network intrusion of industrial IoT. International Journal of Intelligent Systems, 2023(1): 2956990. https://doi.org/10.1155/2023/2956990
[7] Marir, N., Wang, H., Feng, G., Li, B., Jia, M. (2018). Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using spark. IEEE Access, 6: 59657-59671. https://doi.org/10.1109/ACCESS.2018.2875045
[8] Malik, M., Dutta, M. (2023). Feature engineering and machine learning framework for DDoS attack detection in the standardized internet of things. IEEE Internet of Things Journal, 10(10): 8658-8669. https://doi.org/10.1109/JIOT.2023.3245153
[9] Magdy, M.E., Matter, A.M., Hussin, S., Hassan, D., Elsaid, S.A. (2023). Anomaly-based intrusion detection system based on feature selection and majority voting. Indonesian Journal of Electrical Engineering and Computer Science, 30(3): 1699-1706. https://doi.org/10.11591/ijeecs.v30.i3.pp1699-1706
[10] Chiche, A., Meshesha, M. (2021). Towards a scalable and adaptive learning approach for network intrusion detection. Journal of Computer Networks and Communications, 2021(1): 8845540. https://doi.org/10.1155/2021/8845540
[11] Narayana, V.L., Bharathi, C.R. (2018). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs. In Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, pp. 649-658. https://doi.org/10.1007/978-981-13-1921-1_63
[12] Platonov, V.V., Semenov, P.O. (2017). An adaptive model of a distributed intrusion detection system. Automatic Control and Computer Sciences, 51(8): 894-898. https://doi.org/10.3103/S0146411617080168
[13] Abou El Houda, Z., Hafid, A.S., Khoukhi, L. (2023). MiTFed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain. IEEE Transactions on Network Science and Engineering, 10(4): 1985-2001. https://doi.org/10.1109/TNSE.2023.3237367
[14] Asif, M., Abbas, S., Khan, M.A., Fatima, A., Khan, M. A., Lee, S.W. (2022). MapReduce based intelligent model for intrusion detection using machine learning technique. Journal of King Saud University-Computer and Information Sciences, 34(10): 9723-9731. https://doi.org/10.1016/j.jksuci.2021.12.008
[15] Cao, Y., Zhang, L., Zhao, X., Jin, K., Chen, Z. (2022). An intrusion detection method for industrial control system based on machine learning. Information, 13(7): 322. https://doi.org/10.3390/info13070322
[16] Zhang, Y., Li, P., Wang, X. (2019). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEe Access, 7: 31711-31722. https://doi.org/10.1109/ACCESS.2019.2903723
[17] Sarada, K., Narayana, V.L., Gopi, P., Pavani, V. (2020). An iterative group based anomaly detection method for secure data communication in networks. Journal of Critical Reviews, 7(6): 208-212.
[18] Lin, H., Xue, Q., Feng, J., Bai, D. (2023). Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. Digital Communications and Networks, 9(1): 111-124. https://doi.org/10.1016/j.dcan.2022.09.021
[19] Tabassum, T., Toker, O., Khalghani, M.R. (2024). Cyber–physical anomaly detection for inverter-based microgrid using autoencoder neural network. Applied Energy, 355: 122283. https://doi.org/10.1016/j.apenergy.2023.122283
[20] Eshiett, I.O., Eshiett, O.E. (2024). Artificial intelligence marketing and customer satisfaction: An employee job security threat review. World Journal of Advanced Research and Reviews, 21(1): 446-456. https://doi.org/10.30574/wjarr.2024.21.1.2655
[21] Jia, L., Wang, Y., Siong, T.C., Li, X., Zhao, L., Wei, F. (2022). A hybrid interpretable deep structure based on adaptive neuro-fuzzy inference system, decision tree, and K-means for intrusion detection. Scientific Reports, 12(1): 20770. https://doi.org/10.1038/s41598-022-23765-x
[22] Choudhary, S., Kesswani, N. (2020). Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. Procedia Computer Science, 167: 1561-1573. https://doi.org/10.1016/j.procs.2020.03.367
[23] Sambhus, K., Liu, Y. (2024). Automating SQL injection and cross-site scripting vulnerability remediation in code. Software, 3(1): 28-46. https://doi.org/10.3390/software3010002
[24] Narayana, V.L., Gopi, A.P., Anveshini, D., Lakshmi, G.V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4): 391-397. https://doi.org/10.1504/IJWMC.2020.108539
[25] Lombardo, L. (2022). Distributed measurement systems: Advantages and challenges of wireless sensor networks. IEEE Instrumentation & Measurement Magazine, 25(4): 21-28. https://doi.org/10.1109/MIM.2022.9777775
[26] Temene, N., Sergiou, C., Georgiou, C., Vassiliou, V. (2022). A survey on mobility in wireless sensor networks. Ad Hoc Networks, 125: 102726. https://doi.org/10.1016/j.adhoc.2021.102726
[27] Majid, M., Habib, S., Javed, A.R., Rizwan, M.,

Srivastava, G., Gadekallu, T.R., Lin, J.C.W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6): 2087. https://doi.org/10.3390/s22062087

[28] Jain, S., Choudhari, P., Srivastava, A. (2021). The fundamentals of Internet of Things: Architectures, enabling technologies, and applications. In Healthcare Paradigms in the Internet of Things Ecosystem, pp. 1-20. https://doi.org/10.1016/B978-0-12-819664-9.00001-6

[29] Mukherjee, A., Shome, S.K., Bhattacharjee, P. (2021). Survey on internet of things based intelligent wireless sensor network for fire detection system in building. In Communication and Control for Robotic Systems, pp. 193-200. https://doi.org/10.1007/978-981-16-1777-5_12