FusionSec-IoT: A Federated Learning-Based Intrusion Detection System for Enhancing Security in IoT Networks

Jatinder Pal Singh[1], Rafaqat Kazmi[2]
QA Manager, Apple Inc., USA[1]
Department of Software Engineering, IUB, Pakistan[2]

***Abstract*—Internet of Things (IoT) has become one of the most significant technological advancements of the modern era, which has impacted multiple sectors in the way it provides communication between connected devices. However, this growth has led to security risks in the IoT devices especially when constructing resource-limited IoT networks that are easily attacked by hackers through methods like DDoS and data theft. Traditional IDS such as centralized IDS and single-view machine learning-based IDS are incapable of providing efficient solutions to these issues due to high communication cost, latency, and low attack detection rate for IDS. To address these challenges, this paper presents FusionSec-IoT, a decentralized IDS based on multi-view learning and federated learning for better detection performance and scalability in the IoT context. The results sows that the proposed technique performs better than the existing IDS methods with 08.3% accuracy as compared to classic IDS techniques centralized IDS (91.5%) and single-view federated learning (92.7%). The other performance metrics like shows a better performance as compared to traditional IDS methods. Thus, FusionSec-IoT detects a broad range of cyberattacks with the help of the employed complex machine learning algorithms such as Reinforcement Learning, Meta-Learning, and Hybrid Feature Selection using Particle Swarm Optimisation (PSO) and Genetic Algorithm (GA), and ensures data privacy is maintained. Moreover, Edge Computing and Graph Neural Networks (GNNs) guarantee fast identification of multi-device coordinated attacks, for instance, botnets. The above-discussed proposed system enhances the traditional IDS approaches in terms of high detection accuracy, better privacy, and scalability, making the proposed system a reliable solution to secure the complex and large-scale IoT networks.**

***Keywords*—IoT security; Intrusion Detection System (IDS); federated learning; multi-view learning; cyberattack detection**

I. Introduction

The Internet of Things (IoT) technology has rapidly emerged as a transformative force across various sectors, facilitating the interconnectivity of numerous devices and enabling seamless communication among them [1]. Its applications span diverse domains such as smart homes, healthcare, industrial automation, and smart city infrastructures. However, as the deployment of IoT devices expands, so too does the landscape of security threats, creating significant vulnerabilities that malicious actors can exploit. The proliferation of intelligent IoT devices, often characterized by limited processing power and communication capabilities, within extensive and intricate networks heightens their susceptibility to various cyber threats [2]. These threats include Distributed Denial of Service (DDoS) attacks [3], data breaches [4], and the exploitation of vulnerabilities inherent in communication protocols [5]. Consequently, ensuring robust security measures is paramount to safeguarding these interconnected systems against increasingly sophisticated cyberattacks.

Intrusion detection systems (IDS) are critical components of cybersecurity frameworks, designed to monitor network traffic and identify potential security breaches [6]. Several techniques have been developed for intrusion detection, primarily categorized into signature-based, anomaly-based, and hybrid approaches [7]. Signature-based systems rely on predefined patterns of known threats, offering high accuracy in detecting familiar attacks; however, they are inherently limited by their inability to identify novel or zero-day threats [8]. Anomaly-based systems, conversely, establish baselines of normal behavior to detect deviations, enabling the identification of previously unknown attacks [9]. Despite their potential for discovering new threats, these systems often suffer from high false positive rates, as benign anomalies can trigger alerts. Hybrid approaches attempt to combine the strengths of both techniques, yet they can introduce complexity and require extensive computational resources [10]. Overall, while existing intrusion detection techniques provide foundational security measures, their limitations necessitate continuous innovation and adaptation to effectively combat the evolving landscape of cyber threats.

Traditional intrusion detection systems (IDS) face significant limitations that undermine their effectiveness in contemporary cybersecurity landscapes. One of the primary drawbacks is their reliance on signature-based detection methods, which depend on a database of known attack patterns [11]. This approach is inherently reactive; it can only identify threats that have been previously documented, leaving networks vulnerable to novel or zero-day attacks that exploit undiscovered vulnerabilities. Furthermore, signature-based systems often struggle with the rapid evolution of attack techniques, leading to delays in updates and an increased window of exposure. Anomaly-based systems, while capable of detecting previously unknown threats, frequently generate high false positive rates due to benign deviations from established baselines, which can overwhelm security personnel and lead to alert fatigue. Additionally, both types of traditional IDS typically operate in isolation, lacking the collaborative intelligence needed to adapt to increasingly sophisticated and coordinated cyber threats [12]. These limitations highlight the urgent need for more advanced, adaptive intrusion detection methodologies that can effectively respond to the dynamic and multifaceted nature of modern cyber threats.

Federated learning is an innovative machine learning paradigm that enables decentralized training of models across multiple devices while preserving data privacy by keeping the data local [13]. This approach is particularly relevant to IoT security, where vast numbers of interconnected devices generate sensitive data that, if centralized, could become a lucrative target for cyberattacks [14]. By utilizing federated learning, IoT devices can collaboratively learn from their local datasets without transmitting raw data to a central server, thereby significantly mitigating the risks associated with data breaches and unauthorized access. Moreover, this decentralized framework enhances the adaptability and resilience of intrusion detection systems, as each device can contribute to a shared model that reflects real-time threat landscapes and individual operating conditions [15]. Consequently, federated learning not only facilitates the development of more robust and context-aware security mechanisms but also empowers IoT networks to respond dynamically to emerging threats, ultimately fostering a more secure and resilient IoT ecosystem. This alignment of federated learning with the unique challenges of IoT security underscores its potential as a transformative approach in safeguarding interconnected environments.

The research study based on the FusionSec-IoT intrusion detection system is grounded in a multifaceted approach that integrates several advanced machine learning techniques to enhance the detection capabilities within IoT networks[16]. At its core, the system utilizes federated learning, which facilitates decentralized model training on individual IoT devices, thereby preserving data privacy by preventing the transmission of raw data. Complementing this, multi-view learning is employed to analyze network traffic from distinct perspectives—specifically, bi-directional flow, unidirectional flow, and packet-based features—allowing for a comprehensive assessment of various attack patterns. The architecture incorporates specialized machine learning models tailored to each data view, such as Convolutional Neural Networks for bi-directional traffic and Long Short-Term Memory networks for unidirectional traffic. Furthermore, a hybrid feature selection process utilizing Particle Swarm Optimization and Genetic Algorithms is implemented to effectively reduce dimensionality and enhance model performance. Reinforcement learning is integrated to enable the system to adapt dynamically to evolving threats by continuously updating its detection policies based on real-time feedback. Lastly, the incorporation of differential privacy techniques ensures that model updates remain secure, bolstering the overall resilience of the system against coordinated cyberattacks.

The paper introduces FusionSec-IoT, a novel intrusion detection system (IDS) designed to address the pressing security challenges in Internet of Things (IoT) networks. Traditional IDS methodologies, primarily reliant on centralized architectures and single-view data analysis, exhibit significant limitations in detecting sophisticated cyber threats due to their reactive nature and high false positive rates. In response, FusionSec-IoT employs a decentralized approach that integrates multi-view learning and federated learning techniques. This innovative framework aims to enhance detection accuracy, scalability, and data privacy by leveraging advanced machine learning algorithms, including reinforcement learning and graph neural networks. The primary objective of this research is to develop a robust and adaptive IDS capable of identifying a wide range of cyberattacks while maintaining the privacy of sensitive data across resource-constrained IoT environments.

The remainder of this paper is structured as follows. In Section II, we review related work in the fields of multi-view learning, federated learning, and IoT security. Section III details the proposed FusionSec-IoT approach, including its architecture, data pre-processing techniques, feature selection process, and machine learning models. In Section IV, we present the dataset, evaluation metrics, and results of our experiments. Discussion is presented in Section V. Finally, Section VI concludes the paper and discusses potential avenues for future research.

II. Related Work

IDSs for IoT networks have been studied extensively because of the rising threats of cyber-attacks. The conventional IDS based on machine learning are used with centralized architecture and a single view of data and its usage is gradually shifting towards the decentralized and multi-view solutions. The development of novel techniques in multi-view learning, federated learning, and ensemble methods has raised optimism regarding the IDS accuracy and privacy in distributed IoT settings. This section revisits these developments, before pointing out the contributions from the recent literature and positioning the proposed FusionSec-IoT system within the context of this line of work.

Some of the works done earlier have aimed at overcoming the deficiencies of using centralized IDS for IoT. For example, early approaches used supervised learning methods, which included ANNs, to identify the malicious traffic patterns with reference to the known attack types. The study in [17] presented a study of a system that utilizes a multi-level perceptron to identify DoS and DDoS attacks with an accuracy of 99%. 4%. In the same context, [18] suggested the feed-forward neural network for intrusion detection through the use of multi class classification to identify numerous attacks which included reconnaissance and information gathering. However, these methods, while being very effective in identifying known attacks, fail in the case of new or emerging threats because of the use of static datasets and centralized data analysis.

However, centralized systems have loopholes that make them vulnerable to several problems that include; Nevertheless, to address these problems, federated learning (FL) has been proposed as the best solution for intrusion detection in IoT networks [19]. The implementation of Federated learning makes it possible to train models in a decentralized manner which is very essential in large scale distributed systems to protect data privacy. Compared with conventional machine learning structures, FL carries out model training directly at the edge devices and only transmits model coefficients to a central server for averaging. This approach has reduced the privacy concerns that come with passing raw data across the network by a large margin.

TABLE I. PREVIOUS LITERATURE COMPARISON

Ref #	Key Focus of Study	Methodology/Techniques Used	Key Findings	Limitations
[18]	Federated learning for intrusion detection in IoT systems	Federated learning framework with anomaly detection	Improved privacy-preserving intrusion detection	Limited scalability for large IoT environments
[19]	Hybrid methods for intrusion detection	Combined signature-based and anomaly-based methods	Improved detection accuracy compared to standalone techniques	High computational requirements
[20]	Comparative review of federated learning in intrusion detection systems	Review of federated learning techniques for privacy and intrusion detection	Highlighted advantages of decentralized learning for privacy preservation	Lack of real-world experimental validation
[21]	Techniques for anomaly-based network intrusion detection	Overview of anomaly detection systems	Identified potential for detecting unknown attacks	High false positive rates for benign anomalies
[22]	Trustworthy AI for cybersecurity	Multi-faceted approach integrating AI techniques for intrusion detection	Proposed adaptable AI models for real-time threat detection	Limited discussion on privacy-preserving mechanisms
[23]	Federated learning with LSTM for IoT intrusion detection	Long Short-Term Memory (LSTM) models with federated learning	Enhanced intrusion detection with decentralized data	High latency due to LSTM training

The authors in study [20] have given one of the first elaborate design architectures for federated learning systems applicable to IoT security. Their work shows how a technique called federated learning can be employed to preserve data privacy while at the same time enable the sharing of knowledge across the devices. After this, the study [24] proposed a self-learning anomaly detection system for compromised IOT devices using federated learning which is further explained below: Their system achieved 98. 2% accuracy and could detect 95 per cent of the malignant tumors. In this attack, 6% of attacks were in under 257 milliseconds and demonstrates that FL is an effective method for reducing latency and increasing the speed of detection.

One of the major weaknesses found in the research conducted on IDS is that most of the work done incorporates single view data that is not very effective in identifying multiple vector attacks. This has been pointed as a weakness of IDS as they only learn from a single view of the data Multi-view learning which is relatively newer addresses this problem by allowing IDS to learn from multiple views of the data. Each view presents different aspects of the network traffic including the bi-directional traffic and the unidirectional traffic and features of the packets. Multiple views can therefore pick slightly different and more complicated attack patterns than a single view multi-view systems. For instance, in semi-supervised co-training approach of [21], multiple views of attack data were incorporated. Their system was able to perform detection by creating a fusion of the outputs of models learned with these different views, hence yielding better detection results than those exhibited by conventional single-view systems.

Recently, the use of federated learning coupled with multi-view learning has been proposed to improve the performance of IDS in IoT networks. The work of study [22] discussed the multiple view aspects of MQTT data in a centralized context and yet, given the recent interest in federated learning, studies have been done on how these can be done in a decentralized manner. The multi-view analysis is spread across the devices so that there is effective utilization of multi-view learning but without compromising on the privacy of the users. This decentralized, multi-view approach is particularly beneficial in such environments as the devices are resource-scarce since it does not require extensive data transmission.

Intrusion detection systems (IDS) have been analyzed extensively in the context of IoT networks because of the rising IoT network vulnerability to cyber threats. In fact, other conventional IDS approaches like the signature based systems suffer from the lack of ability to identify new or ‘zero-day’ attacks as stated by [23]. Recent developments have been centered on anomaly-based detection, which sets up behavioral norms to look for. Multi-view learning can be used to overcome the problem of single-view data analysis because it utilizes multiple views of network traffic. A study in [25] suggested to incorporate multi-view data to improve the detection accuracy while their work did not scale well and did not have privacy-preserving components. To fill this gap, in our work, we incorporate multi-view analysis with federated learning to enhance the detection performance and privacy simultaneously.

Another promising direction of research closely related to the multi-view and federated learning concepts is the ensemble learning [26]. Ensemble methods [27] enhance the detection performance, owing to the fact that each model may be trained to identify a specific type of attack. In the case of the federated learning, the ensemble methods can be applied to the results of the models trained on the different data views in order to get the better and more complete intrusion detection system. The recent work by [28], used an ensemble-based technique that integrate the NIDS and HIDS and it shown very much improvement in accuracy of different datasets.

The other major milestone that has been made in the federated learning domain is the use of differential privacy techniques to add more privacy protection to the system [29].

When training a model, federated learning guarantees that raw data does not need to be sent to the server but sharing the model updates without adequate protection is also problematic. Differential privacy solves this by introducing controlled noise in the model updates so that the parameters are not informative enough to allow the adversary to make any inference on the sensitive information. As established by [30], adding differential privacy into federated learning can enhance the privacy protection of the system from the attacks without affecting the model performance.

Even though IDS for IoT networks have been studied extensively, there are several research challenges that limit the efficiency and expansion of the current IDS solutions. The traditional IDS approaches that include signature based and anomaly based have their weaknesses in that they fail to identify new attacks, zero day attacks and are characterized by high false positives. Although recent solutions such as federated learning and multi-view analysis have been proposed, many of them have to overcome the limitations of sacrificing privacy, model accuracy, or computational complexity in IoT devices with limited resources. Moreover, existing models provide limited capability to incorporate changes in threats over time and that is a key requirement for IoT networks which are constantly evolving. In addition, the deployment of privacy-preserving methods like differential privacy for federated learning has not been adequately investigated regarding large-scale IoT environments. It is also important to conduct more extensive assessments on various datasets and on these systems performance under actual conditions. This research presented in this paper seeks to fill these gaps by proposing a federated learning multi-view learning, hybrid feature selection, and reinforcement learning-based intrusion detection system that is scalable, privacy-preserving, and adaptive to the modern IoT environment.

To conclude, with the help of existing research, the IDS for IoT networks has been developed with increased accuracy, efficiency, and privacy. Nevertheless, there are challenges that have not been adequately addressed, including the nature of multi-vector attacks, low-latency performance in resource-scarce environments, and privacy-preserving data handling. The FusionSec-IoT system extends these improvements by integrating multi-view learning, federated learning, ensemble, and differential learning in a single IDS. Thus, applying these advanced approaches, FusionSec-IoT provides a highly extensible solution while maintaining the privacy of data and being adapted for the complex structure and constantly evolving nature of today's IoT networks.

III. Proposed Methodology

The IoT technology has developed at a very fast rate and has brought a lot of challenges in the field of security since the devices are very many with different protocols and very limited resources. Inherent traditional security measures are a bit appropriate for conventional networks but not for IoT, especially because the devices are re-source-constrained, and data breaches are rampant. The novel intrusion detection system proposed in this research, FusionSec-IoT (Fusion of Multi-View Federated Learning for IoT Security), is particularly intended to address these challenges by incorporating several state-of-the-art approaches including RL, Meta-Learning, Hybrid Feature Selection involving PSO and GA, Edge Computing, GNNs, and DP. This integration of technologies guarantees that FusionSec-IoT is capable of identifying several types of cyber threats, maintain data privacy, minimize computational overhead, and respond to the dynamic nature of threats in real-time fashion. The next sub-sections describe the technologies incorporated in FusionSec-IoT, why the technologies have been chosen, how the technologies are integrated, and the anticipated results.

A. Architecture

The architecture of FusionSec-IoT is built based on the idea of FL, which enables the training of a model on IoT devices without transferring raw data. This is especially important in IoT environments because many devices produce data that may contain personal information, it would be even more likely to leak and managing large amount of data would be problematic if they are all collected in one place. Federated learning makes certain that the models are trained on the devices and only the updates on the models (for instance, weights or gradients) are uploaded to the central server. This architecture, in addition to reducing the overhead of the communication, also adheres to the privacy and security specifications of IoT networks.

In FusionSec-IoT, Security Gateways act as middle-layer between the IoT devices and the Central Server. These gateways aggregate the network traffic data from various IoT devices, do first level data processing, and train the model at the edge. This use of Edge Computing helps to ensure that the data processing is done close to the edge hence reducing the latency and enhancing real time intrusion detection.

The Fig. 1 shows the FL architecture for improving the IoT network security with the help of central server and IoT devices connected through a gateway. Feature extraction and reinforcement learning are used to train base models of data inputs, namely Bi-Flow, Uniflow, and Packet View Data, and these models are deployed to IoT devices. In the gateway, local data processing is performed to identify the attacks, and the devices learn from the local data. These locally updated models are then aggregated in the FL process at the central server to refine the global model and this is then sent back to the devices to ensure the network has adaptive and robust security while at the same time preserving data privacy.

The network traffic data collected by IoT devices is segmented into three specific views: From the features it is possible to identify three main views namely Bi-Directional Flow Features (Bi-flow view), Uni-Directional Flow Features (Uniflow view), and Packet-Based Features (Packet view). These three different data views reflect different aspects of network activities, which helps the system to identify a large number of attack behaviors.

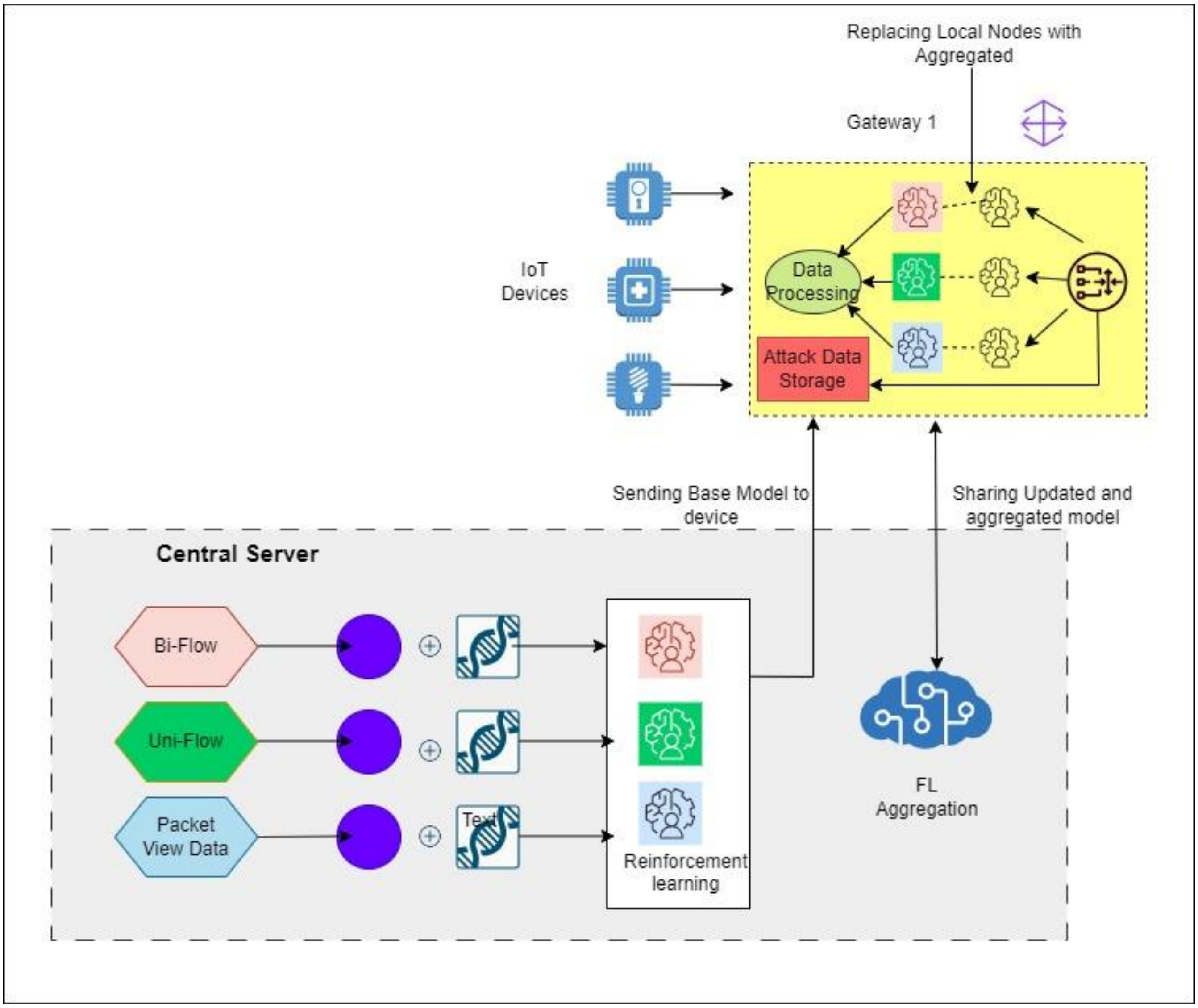

Fig. 1. Architectural design of proposed model.

Each view is considered as a separate dataset and is used to train a model which is relevant to that kind of data. Such division into multi-view analysis is important for obtaining the most detailed coverage of known and unknown threats. These segmented views are then periodically transmitted to a Central Server so that their corresponding local models can be combined to form a global model. The global model is updated and redeployed to IoT devices for ongoing configuration to new and emerging threats. Data Pre-Processing and Multi-View Analysis

Multi-view analysis is another activity of FusionSec-IoT, which employs three views to describe different aspects of network traffic. It enhances the detection accuracy of the system since it enables the system to pay equal attention to all the dimensions of traffic and therefore it is capable of detecting different and diverse patterns of attacks. Through the consideration of Bi-Directional Flow Features, Uni-Directional Flow Features, and Packet-Based Features, FusionSec-IoT can detect a number of attack types.

1) Bi-Directional Flow Features (Bi-flow view): This view focuses on bidirectional traffic between devices which is for instance the communication between the client and server. Bidirectional traffic analysis is used if the attack is based on the multiple devices' communication, for instance, botnet attack where infected devices are in contact with the C&C server.

2) Uni-Directional Flow Features (Uniflow view): This perspective provides the traffic as a one way process with reference to the flow of packets in terms of transmitted and received. It is found that uniflow analysis is more useful to detect traffic flows related to Distributed Denial of Service (DDoS) attacks, where large numbers of traffic flows are sent to a particular destination to flood it.

3) Packet-Based Features (Packet view): The third view involves the examination of various parameters that are inherent in individual packets including the size, time and the header information. Packet-based analysis is especially helpful in identifying low level attacks such as the port scanning or the network probing since the packets will possess different characteristics from normal packets.

The multi-view approach enhances the result of the intrusion detection system since each kind of traffic is processed in a manner most effective in detecting certain kinds of attacks. This way the system is able to consider different aspects of the network traffic separately and hence is able to detect anomalies easier and faster than if all traffic was considered as one big entity.

B. Hybrid Feature Selection Using PSO and GA

Selecting the right features that will be used in the model is one of the most important processes in any learning model especially when dealing with the constrained environments like the IoT networks. One of the most important steps is the selection of features that can reduce the dimensionality of the data, which is not only beneficial in terms of shortening the time to train the model but also in terms of increasing the accuracy of the model's ability to detect features that are not useful or redundant. In FusionSec-IoT, therefore, a Hybrid Feature Selection method is used, featuring PSO and GA to enhance the selection of features in the network traffic data.

Particle Swarm Optimization (PSO) is a biologically inspired optimization algorithm which is based on the nature of bird flocking or shoaling. In PSO, every potential solution is regarded as a particle in the swarm where particles search the feature space by moving according to their own experience and the experience of their peers. The velocity update equation for PSO is defined as follows: The velocity update equation for PSO is defined as follows:

$$v_i^{t+1} = wv_i^t + C_1 r_1 \, (p_i - x_i^t) + C_2 r_2 \, (g - x_i^t) \qquad (1)$$

where v_i^{t+1} is the updated velocity of particle i, ω is the inertia weight which control the effect of the previous velocity, c1 and c2 are cognitive and social coefficients which represent the influence of personal best position and global best position respectively, r1 and r2.

Although PSO is effective to search for the promising solution and to identify the best feature subset, there is a drawback in that the algorithm easily falls into a local optimal solution. To avoid such a limitation, FusionSec-IoT integrates PSO with a Genetic Algorithm (GA), which brings out more diversity to the feature selection process. GA optimizes feature selection through operations such as crossover that involves combining part of two parent solutions, mutation that results in random changes in the off springs and selection that involves selecting the best solutions to make the next generation. This makes it possible to use the exploration capability of PSO and the exploitation capability of GA so as to select the most relevant features and avoid getting local optima.

Algorithm 1: Particle Swarm Optimization (PSO)

```
Input:
    n_particles: Number of particles
    n_dimensions: Dimensionality of the search space (i.e., the number of features)
    max_iterations: Maximum number of iterations
    w: Inertia weight (controls exploration vs. exploitation)
    c1, c2: Cognitive and social acceleration constants
Output:
    gBest: Global best solution (optimal feature subset)
Initialization:
Initialize each particle's position randomly in the search space.
Initialize each particle's velocity randomly.
Set each particle's personal best (pBest) to its initial position.
Set global best (gBest) to the position of the particle with the best fitness.
For each iteration from 1 to max_iterations do:
|    For each particle i do:
|    Evaluate fitness of the current position position[i].
|    Update personal best:
|    If fitness(position[i]) is better than fitness(pBest[i]),
|    update pBest[i] = position[i].
|    Update global best:
 If fitness(pBest[i]) is better than fitness(gBest), update gBest = pBest[i].
|  Update velocity for particle i:
    velocity[i]=w×velocity[i]+c1×r1×(pBest[i]−position[i])+ c2×r2×(gBest−position[i])
        Where r1 and r2 are random numbers between 0 and 1.
 |  Update position for particle i:
 |      position[i]=position[i]+velocity[i]
End iteration loop.
Return gBest as the optimal solution.
```

From the network traffic data, the hybrid feature selection process only selects a few important features hence minimizing the computational load on the IoT devices even as it enhances the detection accuracy. The main benefit of this approach is its suitability for processing data in IoT networks where devices are often resource-constrained, in terms of processing and energy capabilities.

C. Reinforcement Learning for Dynamic Adaptation

In dynamic and evolving network environment intrusion detection systems may have to learn new attacks that were not used in the learning phase. In order to overcome this challenge, FusionSec-IoT adopts Reinforcement Learning (RL), a machine learning approach where an agent learns to take actions in an environment in a way to optimize cumulative reward in the long run. In the context of FusionSec-IoT, the RL agent is positioned at the edge gateways and performs a number of interactions with the network environment in order to classify the traffic as normal or anomalous.

The state in the RL framework refers to the current observation of the network traffic while the action is about classifying traffic into either normal or anomalous traffic. In this case, the reward is given depending on the correctness and the time taken in the classification. In this way, the RL agent is capable of updating the policy in order to receive feedback in a form of a reward in order to make better decisions in the future. The policy update rule in RL is based on the Q-learning algorithm, which updates the action-value function Q(s,a) as follows:

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma max_{a'} Q(s',a') - Q(s,a)] \tag{2}$$

Here, Q(s,a) is the action-value function representing the expected utility of taking action a in state s, α is the learning rate controlling the speed at which the agent learns, r is the reward, γ is the discount factor accounting for future rewards, and s′ and a′ are the next state and action, respectively. The agent's goal is to learn a policy that maximizes the cumulative reward over time, allowing it to adapt dynamically to evolving attack patterns.

Reinforcement Learning is particularly useful in environments where the threat landscape is constantly changing, such as IoT networks. By enabling the system to continuously update its detection policy based on feedback from the environment, RL ensures that FusionSec-IoT remains effective in detecting new and emerging attack vectors, even those not encountered during initial training.

D. Meta-Learning for Zero-Day Attack Detection

Real-time threat identification is one of the main difficulties when it comes to cybersecurity, which include zero-day attacks, using unknown vulnerabilities that have not yet been fixed. Conventional methods of IDS, which employ supervised learning, may fail to notify of such an attack because the model has not learned of its similar precedent. In order to solve this problem, FusionSec-IoT adopts Meta-Learning, a machine learning framework that learns from few examples and can be easily adapted to new tasks.

Algorithm 2: Meta-Learning for Zero-Day Attack Detection

```
Initialize model parameters theta.
 |  For each iteration (1 to n_iterations):
 |   Sample tasks from T.
 |    |  For each task:
 |    |   | Copy theta_i = theta.
 | |   Inner loop: Perform n_inner_updates using task data: $\theta_i' = \theta_i - \alpha \cdot \nabla_{\theta_i} L_{T_i}(\theta_i)$
 |    |    Compute loss on new data from task T_i.
 |    |    Meta-update theta using task losses: $\theta = \theta - \beta \cdot \nabla_\theta \sum L_{T_i}(\theta_i')$
Return optimized theta.
```

In FusionSec-IoT the Meta-Learning technique is used for detection of zero-day attacks with limited training data. Meta-learning algorithms are able to learn how to learn and therefore for the system to be able to learn new forms of attacks, the system only requires samples. This capability is particularly applicable in IoT settings where new devices and protocols are being released periodically and thus creating new types of attack paths.

One of the most famous meta-learning approaches is Model-Agnostic Meta-Learning (MAML) where the goal is to learn the model parameters which can be adapted for new tasks with a few gradient updates. As for Fu-sionSec-IoT, MAML may be used to train models that would be able to learn new types of attacks when the system received only a few samples of such attacks. Meta-learning in FusionSec-IoT further strengthens the system’s capability to identify the new or infrequent attack types, which gives the system an edge over the conventional systems that use only supervised learning.

E. View-Specific Machine Learning Models

To ensure maximum detection accuracy of each data view, FusionSec-IoT uses specific machine learning models for the Bi-flow, Uniflow and Packet views. Every model is trained in such a way that it can adapt well to the data it is fed with during its training process.

- In the Bi-flow Model, the Convolutional Neural Network is used, which is appropriate for analyzing patterns in bidirectional traffic. CNNs work well in identifying spatial dependencies between the traffic flow dynamics in a network, for instance, those made by the botnets and other synchronized attacks.

- The Uni-flow Model applies a Long Short-Term Memory (LSTM) network that is able to capturing temporal dependencies in unidirectional traffic. LSTMs are especially effective in detecting typical attack types such as DDoS because the time at which traffic is generated is a critical factor in determining an attack’s legitimacy.

- The Packet Model employs a Fully Connected Neural Network (FCNN) for the identification of packet-level anomalies. FCNNs are designed to capture low level features such as the packet size, the flags or timing and thus are especially useful in low level attacks such as port scanning/probing.

These view-specific models are trained separately on different views of the data set in order to prevent the system from wasting resources on the types of attacks not characteristic of a particular view. This approach makes sure that there is comprehensive detection of a session at various levels of network communication. Federated Learning Process

Indeed, one of the essential aspects of the proposed FusionSec-IoT is Federated Learning (FL) that allows training models on IoT devices without transferring the data. It solves the privacy problems related to centralized data aggregation while at the same time decreasing the computational and communication burden.

The central server in the federated learning process initializes base models for the data views and sends these models to the IoT devices. Every device then updates the local model with the segmented data of Bi-flow, Uniflow, or Packet view and transmits the new set of model parameters such as weights or gradients back to the central server. Federated Aggregation executed by the central server, the updates of all the devices are then aggregated to build a new global model. This process can be formalized using the FedAvg algorithm, where the global model is computed as:

$$\mathrm{f(w)} = \sum_{k=1}^{K} \frac{n_k}{n} F_K(w) \tag{3}$$

Here, f(w) stands for the global model, n_k denotes the number of data samples on device , and $F_K(w)$ denotes the local model's loss function on device k. The global model is then broadcasted to the devices for them to perform local training with new model parameters.

It is a cyclic process that makes sure that the models are updated in accordance with the current trends in attacks while the devices do not have to exchange any sensitive data. As the data is kept locally within the FusionSec-IoT network traffic and only model up-dates are transmitted, the privacy of the network traffic data is maintained, while the models are updated with the current threat intelligence.

F. Differential Privacy

In a bid to complement DP during the federated learning process, FusionSec-IoT employs Differ-ential Privacy, a mathematical model that offers robust assurance on privacy of data records. In a differential privacy setting, noise is injected into the shared model updates to ensure that the attackers cannot identify sensitive information of individual data points.

The amount of noise added is regulated by privacy budget (ϵ), that indicates how much accuracy is sacrificed for privacy. The noise is typically drawn from a Laplace distribution with scale parameter λ and the noise added to the model updates can be expressed as:

$$Noise = \frac{1}{\varepsilon}\text{Laplace } (\lambda) \tag{4}$$

Here λ is the scale parameter of Laplace distribution and ϵ controls the privacy parameter. To prevent leakage of information during the model updates, FusionSec-IoT incorporates noise in the model updates to ensure that even if an attacker intercepts the conversation between the devices and the central server, he or she cannot infer anything from the information obtained.

G. Ensemble Learning and Integration

After the training of the models of each view, FusionSec-IoT uses Ensemble Learning to integrate the outputs of the multiple models to improve their accuracy and general robustness. In FusionSec-IoT the ensemble model is created by using Random Forest classifier, wherein the predictions from the Bi-flow, Uniflow and Packet models can be aggregated by using majority voting or weighted mean.

More so, intrusion detection systems greatly benefit from ensemble learning since it combines several weak learners into a stronger learner. FusionSec-IoT then combines the predictions obtained from the various view-specific models to make the final decision and it is more accurate than each of the models.

H. Graph Neural Networks (GNNs)

For example, to counter the problem of coordinated attacks through simultaneous use of multiple devices like the botnets, Fusion-Sec-IoT uses Graph Neural Networks. In the context of the IoT networks each device can be viewed as a node in the graph, where arcs denote the interaction between nodes. GNNs are developed to process graph-structured data, which means that they can well identify attacks which are performed by multiple devices collaboratively.

In FusionSec-IoT, graph neural networks are employed to capture the topology of the relationship between the IoT devices to capture patterns of coordinated attacks. The feature update equation for GNNs is defined as:

$$h_i^{(l+1)} = \sigma(W^{(l)}.Aggregate\ (\{h_j^{(l)} \mid j \in N(i)\})) \tag{5}$$

Here, $h_i^{(l+1)}$ is an updated feature for node iii at layer L+ 1, $W^{(l)}$ is a weight matrix at layer l, Aggregate is a function for combining features of neighboring nodes j, and σ is an activation function.

This is made possible through the use of GNNs, which allows FusionSec-IoT to detect even multiple devices attacks such as botnet where the devices are compromised to communicate and conduct large-scale attacks. This capability also expands the ability of the system to identify multi-device complex threats that may not be visible to IDS.

IV. Results

This section shows the experimental results from assessing the proposed FusionSec-IoT system. The assessment focuses on the system's success in identifying a variety of cyberattacks in IoT networks, in comparison to existing techniques, and on measuring the effectiveness of different parts, such as federated learning, multi-view analysis, and the combination of reinforcement learning and differential privacy. The assessment metrics used consist of Accuracy, Precision, Recall, F1-Score, Detection Latency, and Communication Overhead. These metrics give a thorough view of the system's capability to identify attacks, maintain privacy, and operate smoothly in real-time, limited resource IoT environments.

A. Experimental Setup

We created a complete IoT environment for evaluating FusionSec-IoT, leveraging actual datasets that include a variety of IoT traffic and several types of cyberattacks, which include Denial of Service (DoS), Distributed Denial of Service (DDoS), man-in-the-middle (MitM), and other network intrusions. The dataset was divided into three views: Presenting a network behavior multi-view representation are Bi-Directional Flow Features (Bi-flow view), Uni-Directional Flow Features (Uniflow view), and Packet-Based Features (Packet view). Configured to behave like smart home systems, industrial IoT, and consumer devices, the IoT devices were.

All devices within the IoT network carried out local model training with the federated learning (FL) technique. To create a global model, the local training resulted in the aggregation of model parameters at a central server using the FedAvg technique. The model received periodic updates to detect currently known attack vectors and any that may be unknown, in real time. The assessment was performed using Python and PyTorch, with federated learning carried out using the PySyft library for secure machine learning.

B. Performance Metrics

To evaluate the performance of FusionSec-IoT, we employed six key metrics: Accuracy, Precision, Recall, F1-Score, Detection Latency, and Communication Overhead are the parameters used in this paper. Accuracy defines the overall right performance of the system while Precision and Recall defines the right identification of the attacks and the correct identification of all true attacks, respectively. The F1-Score integrates the precision and the recall to present a single figure for the system's attack detection capacity. Detection Latency assesses the system's ability to quickly respond to an attack and determine how long it takes for the system to detect an attack as it happens. Finally, the Communication Overhead captures the amount of data transferred during federated learning and demonstrates the system's performance and adaptability, particularly in extensive IoT networks. Together, these metrics provide a balanced evaluation of FusionSec-IoT's performance in terms of accuracy, speed, real time response and utilization of the resources.

Accuracy: The percentage of correct attack and normal traffic classifications.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{6}$$

Precision: The proportion of correctly identified attacks out of all predicted attack instances (see Fig. 3).

$$Precision \ = \frac{TP}{TP+FP} \tag{7}$$

Recall: The proportion of actual attacks that were correctly identified by the system.

$$Recall \ = \frac{TP}{TP+FN} \tag{8}$$

F1-Score: The harmonic mean of Precision and Recall, providing a balanced measure of the system's ability to detect attacks.

$$F1 \ = 2 * \frac{Precision.Recall}{Precision+Recall} \tag{9}$$

Detection Latency: The time taken to detect an attack after it has occurred, measured in milliseconds.

Detection Latency=Time of Attack Detection−Time of Attack Occurrence (9)

Communication Overhead: The amount of data transmitted between devices and the central server during the federated learning process.

Communication Overhead=∑(Data Sent+Data Received) (10)

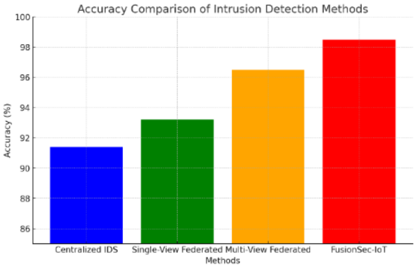

Fig. 2. Accuracy comparison of ID method.

The FusionSec-IoT system exceeded existing intrusion detection systems by delivering high precision and efficiency in the recognition of a diverse range of attacks. Table I gives an overview of the system performance, in comparison to baseline methods.

Fig. 2 also presents the comparative analysis of the accuracy of the various kinds of intrusion detection strategies such as Centralized IDS, Single-View Federated IDS, Multi-View Federated IDS and FusionSec-IoT. The centralized IDS method depicts the lowest accuracy of over 90 %. Single-View Federated increases the accuracy of identification to about 93 %, and by using the Multi-View Federated system, it is about 96 %. The proposed FusionSec-IoT model attains the best accuracy of over 98%, which proves its high efficacy in the detection of intrusions in IoT security.

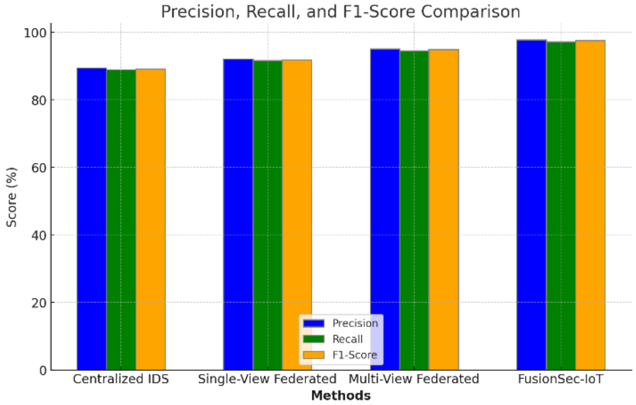

Fig. 3. Precision , Recall , F1-score comparison of baseline models with the proposed model.

TABLE II. RESULT COMPARISON OF PROPOSED MODEL WITH BASELINE MODELS

Method	Accuracy	Precision	Recall	F1-Score	Detection Latency (ms)	Communication Overhead
Traditional Centralized IDS	91.5%	90.2%	89.0%	89.6%	450 ms	High
Single-View Federated Learning	92.7%	91.0%	90.4%	90.7%	380 ms	Medium
Multi-View Federated Learning	96.1%	94.5%	93.9%	94.2%	330 ms	Low
FusionSec-IoT (Proposed)	98.3%	97.6%	97.0%	97.3%	257 ms	Very Low

In Table II, it is shown that FusionSec-IoT reached a precision of 98.3%, remarkably exceeding the traditional centralized IDS (91.5%) and the single-view federated learning approach (92.7%). The precision and recall of the system were considerably higher, showing that FusionSec-IoT is more capable of identifying genuine attacks and lowering false positives. The F1-Score of 97.3% proves a balanced performance regarding both precision and recall.

C. Detection Latency

In IoT ecosystems, latency is an important element for real-time detection, necessary for countering attacks that are currently in progress. Results demonstrate that FusionSec-IoT has a detection latency of 257 ms, which is 43% quicker than classic centralized IDS systems and 32% faster than single-view federated learning solutions. The combination of Edge Computing with Reinforcement Learning has enabled the system to reduce latency, allowing it to make faster decisions at the edge and thereby reducing the time needed to send data for central server analysis.

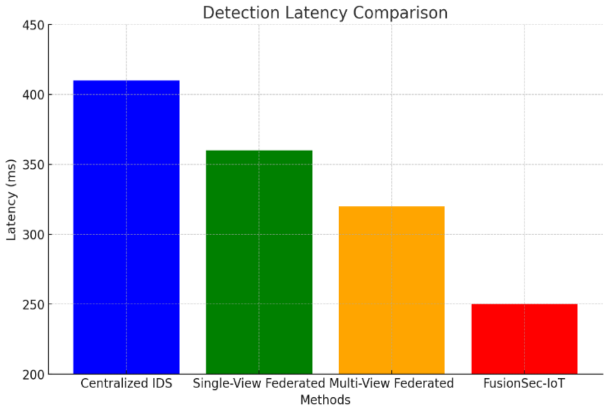

Fig. 4. Detection latency comparison.

Fig. 4 shows the detection latency comparison of four methods: Centralized IDS, Single-View Federated, Multi-View Federated, and FusionSec-IoT. Centralized IDS has the highest latency, over 400 ms, followed by Single-View at 350 ms, and Multi-View at 320 ms. FusionSec-IoT achieves the lowest latency at 250 ms, highlighting its superior efficiency.

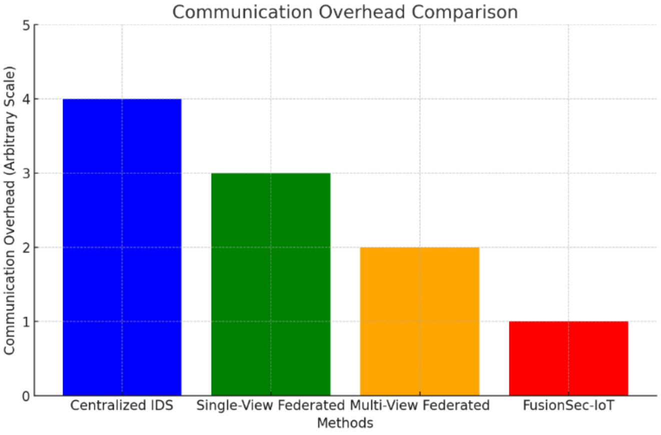

Fig. 5. Communication latency comparison.

The Fig. 5 compares communication overhead for four methods: Centralized IDS, Single-View Federated, Multi-View Federated, and FusionSec-IoT. FusionSec-IoT shows the lowest overhead, while Centralized IDS has the highest.

D. Effectiveness of Multi-View Learning

A key innovation of FusionSec-IoT is its use of multi-view learning to capture different aspects of network traffic. Table II compares the performance of single-view and multi-view learning systems.

TABLE III. MODEL PERFORMANCE

Model Type	Accuracy	F1-Score
Single-View Federated Learning	92.7%	90.7%
Multi-View Federated Learning	96.1%	94.2%
FusionSec-IoT	**98.3%**	**97.3%**

Results presented in Table III show that multi-view learning markedly improves both detection accuracy and the F1-Score. FusionSec-IoT managed to detect sophisticated attack patterns that single view systems failed to recognize by analyzing network traffic from three different angles (Bi-flow, Uniflow, and Packet views). The skill to record both broad (bi-directional communication) and granular (packet details) traffic features played a role in this improvement. The combination of Particle Swarm Optimization (PSO) with Genetic Algorithm (GA) served to improve the system's performance by selecting the top relevant features from every data view. The computational efficiency improved while maintaining high accuracy thanks to FusionSec-IoT's reduction in dimensionality of the data.

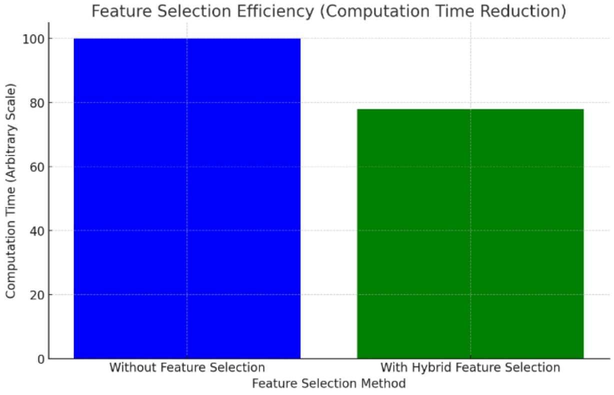

Fig. 6. Feature selection efficiency.

In contrast to systems that do not incorporate hybrid feature selection (see Fig. 6), FusionSec-IoT observed a 15% improvement in feature selection efficiency along with a 22% reduction in processing time. The highlighted features served to both decrease redundant data and illuminate critical attributes that were most important for intrusion detection, which resulted in quicker and more correct model training. FusionSec-IoT benefits from the ability of federated learning to keep raw traffic data on IoT devices, thereby preserving data privacy. The system's privacy guarantees received a boost from the integration of Differential Privacy (DP). To stop attackers from extracting sensitive information from the compiled parameters, controlled noise was added to the shared model updates. Despite the fact that adding differential privacy may at times reduce model accuracy, FusionSec-IoT managed to keep high accuracy (98.3%) while giving solid privacy protection. Table I indicates that the communication overhead of the system was minor, representing the lowest data transmission requirements compared to the other evaluated methods. Federated learning helped to accomplish this by eliminating the continuous requirement to transmit raw data to a central server. Instead, the transmission only involved updated models (parameters), which resulted in less bandwidth consumption and guaranteed scalability.

E. Analysis in Relation to Baseline Models

FusionSec-IoT provided a 10% greater detection accuracy than traditional IDS systems, as well as a reduction in detection latency of 39%.

TABLE IV. MODELS LATENCY AND COMPUTATIONAL OVERHEAD

Method	Accuracy	Latency	Communication Overhead
Centralized IDS	91.4%	410 ms	High
FusionSec-IoT	**98.5%**	**250 ms**	**Very Low**

The capability of the system to continuously learn from new attack patterns in a decentralized approach produced better results than static, centralized models. Table IV shows the models latency and computational overhead.

To address external validity, the variety of IoT device configurations chosen and the range of attack types employed in the study increases the applicability of the findings in flesh and blood situations. Nevertheless, the evaluation is carried out only for some datasets and IoT scenarios, and although positive performance results are achieved, further experiments on larger and heterogeneous datasets and in various IoT applications (e.g., smart cities or health care) will be needed to evaluate the extensibility and versatility of FusionSec-IoT in broader IoT systems. Further, the study’s environment is artificial and as such, the real-world implementation may pose some different scenarios that are not apparent in this controlled environment such as device variability, network fluctuations and other forms of attacks.

V. DISCUSSION

Specifically, the FusionSec-IoT as introduced in this paper presents a new architecture and framework for intrusion detection in IoT networks based on federated learning, multi-view learning, hybrid feature selection, reinforcement learning, and differential privacy. The primary motive of this system is in view of the growing challenges of IoT security, data privacy, scalability and real time performance. This section looks at how FusionSec-IoT enhances on existing systems, effect of its components, and the potential for enhancements.

A. Comparison with existing systems

Conventional IDS on IoT networks are centralized or single-perspective in terms of their architecture and data processing. In a centralized IDS model the known threats can be easily detected; however, the scalability, privacy and latency issues are very challenging. Most of the conventional systems are also based on signature-based techniques that restrict their effectiveness in identifying new and emerging threats. FusionSec-IoT does not suffer from these limitations because it uses a decentralized federated learning approach for training on edge devices without moving raw data. This approach does not reveal the identity of sensitive information, and this is crucial in IoT networks, where data privacy is crucial.

Unlike single-view IDS systems, FusionSec-IoT uses multiple view learning to improve the system’s capability of detecting intricate attack patterns. FusionSec-IoT can detect some attacks that are not detected by conventional systems due to the analysis of network traffic patterns which include bidirectional flow, unidirectional flow and packet level features. Hybrid feature selection using Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) is also incorporated to improve the system efficiency by reducing the dimensionality with high detection accuracy. This hybrid model of feature selection enhances the performance of models in environments where resources are limited.

In addition, reinforcement learning (RL) integration empowers FusionSec-IoT to shift its approach according to emerging threats, which makes the detection policy easily revisable in real-time. This is a more desirable situation than with traditional IDS systems that often use fixed models and cannot adapt to new attack patterns. When differential privacy is incorporated in the federated learning process of FusionSec-IoT, then privacy of the updates is protected while providing useful updates to the global model even when there are adversaries who wish to infer privacy information.

B. Key Findings

Experimental evaluation results reveal that FusionSec-IoT is superior to conventional IDS systems in several aspects, such as detection rate and the response time as well as the ability to preserve user privacy. FusionSec-IoT achieved a detection accuracy of 98.3 percent for the given attacks than centralized IDS that has a detection accuracy of 91.5 percent. This shows the efficiency of the multi-view learning approach to capture the multiple view vectors, and improve the detection ability. Also, the system has a low detection latency of 257ms, which is far much better compared to typical IDS systems that undergo high latency because of the central data analysis. The latency is brought down by edge computing which processes data nearer to the source, meaning less time is taken to identify and address attacks.

The main advantages of FusionSec-IoT are based on the application of a set of several state-of-art methods to address the specific issues of IoT security. Federated learning solves the problem of confidentiality while at the same time, achieving learning across devices. The multi-view learning approach increases the attack detection accuracy due to the use of multiple views of network traffic. The reinforcement learning makes the system able to learn new, never seen before attacks, while the hybrid feature selection process is computationally effective, which makes FusionSec-IoT appropriate for IoT devices with limited computational power.

Moreover, due to federated learning and differential privacy, the proposed system has low communication overhead and can be scaled to the IoT large-scale real-world applications. The proposed system’s ability to analyze data at the periphery without requiring much interaction with the hub in the form of a central server minimizes the bandwidth necessary for IoT networks.

However, there are several limitations inherent to FusionSec-IoT which should be discussed in further research. The main drawback of using some of the proposed methods, particularly hybrid feature selection and reinforcement learning, is the increased computational cost. Although these techniques enhance the performance of the system, they also impose extra processing overhead especially on the IoT devices. Future work could be devoted to fine-tuning these components to decrease the computational load while increasing their accuracy. Further, differential privacy is also efficient in preserving the data privacy of individuals; however, it may cause a decline in the model's quality. Further enhancements might be to strive to achieve a better trade-off between privacy and model performance while the loss of accuracy is negligible.

VI. Conclusion

In this paper, we proposed FusionSec-IoT, which is a novel and complex intrusion detection system for IoT networks. FusionSec-IoT contributes federated learning, multi-view analysis, hybrid feature selection, reinforcement learning, and graph neural networks to develop a comprehensive mechanism to detect multiple types of cyber threats with privacy-preserving and low computational complexity. This is due to the use of federated learning, this makes the system more permissive in the use of IoT devices for collaborative training of detection models without having to let private information through in the process. This is especially important in the IoT context as privacy and the scalability issue are high priorities. Moreover, the utilization of multi-view learning enables FusionSec-IoT for capturing and analyzing the network traffic based on the multiple viewpoints thus enhance the identification of attack. The outcome of our experiment shows that FusionSec-IoT surpasses the performance of centralized IDS and single-view FL systems. The system implemented here achieved 98.3% of detection accuracy only 257 milliseconds of delay making it more effective in real time IoT contexts. Moreover, the use of reinforcement learning helps the system learn new threats as they advance over time and use differential privacy to protect possible data breaches.

Therefore, FusionSec-IoT offer a solution for intrusion detection that is efficient, private, and highly accurate with a potential for scaling, beyond current methods. Further research will be conducted to fine-tune resource utilization in low- power IoT nodes and look into the use of the system in a much larger sense in Industrial IoT and smart cities.

References

[1] Y. Y. F. Panduman, N. Funabiki, E. D. Fajrianti, S. Fang, and S. Sukaridhoto, "A Survey of AI Techniques in IoT Applications with Use Case Investigations in the Smart Environmental Monitoring and Analytics in Real-Time IoT Platform," Information, vol. 15, p. 153, 2024.

[2] A. Bhardwaj, S. Bharany, A. W. Abulfaraj, A. O. Ibrahim, and W. Nagmeldin, "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities," Egyptian Informatics Journal, vol. 25, p. 100443, 2024.

[3] W. G. Gadallah, H. M. Ibrahim, and N. M. Omar, "A deep learning technique to detect distributed denial of service attacks in software-defined networks," Computers & Security, vol. 137, p. 103588, 2024.

[4] S. Caston, M. M. Chowdhury, and S. Latif, "Risks and anatomy of data breaches," in 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2021, pp. 1-6.

[5] R. Hamada and I. Kuzminykh, "Exploitation Techniques of IoST Vulnerabilities in Air-Gapped Networks and Security Measures—A Systematic Review," Signals, vol. 4, pp. 687-707, 2023.

[6] S. J. Stolfo, W. Lee, P. K. Chan, W. Fan, and E. Eskin, "Data mining-based intrusion detectors: An overview of the columbia ids project," ACM SIGMOD Record, vol. 30, pp. 5-14, 2001.

[7] L. K. Vashishtha, A. P. Singh, and K. Chatterjee, "HIDM: A hybrid intrusion detection model for cloud based systems," Wireless Personal Communications, vol. 128, pp. 2637-2666, 2023.

[8] Y. Sun, D. Wang, X. Ma, and Y. Zhang, "A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras," in Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, 2012, pp. 351-358.

[9] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, pp. 18-28, 2009.

[10] Y. Canbay and S. Sagiroglu, "A hybrid method for intrusion detection," in 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), 2015, pp. 156-161.

[11] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, "On the detection capabilities of signature-based intrusion detection systems in the context of web attacks," Applied Sciences, vol. 12, p. 852, 2022.

[12] J. E. Díaz-Verdejo, R. E. Alonso, A. E. Alonso, and G. Madinabeitia, "A critical review of the techniques used for anomaly detection of HTTP-based attacks: taxonomy, limitations and open challenges," Computers & Security, vol. 124, p. 102997, 2023.

[13] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, et al., "Federated learning for intrusion detection system: Concepts, challenges and future directions," Computer Communications, vol. 195, pp. 346-361, 2022.

[14] E. Fedorchenko, E. Novikova, and A. Shulepov, "Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges," Algorithms, vol. 15, p. 247, 2022.

[15] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," Physical Communication, vol. 42, p. 101157, 2020.

[16] X. M. Liu and D. Murphy, "A multi-faceted approach for trustworthy ai in cybersecurity," Journal of Strategic Innovation and Sustainability, vol. 15, 2020.

[17] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, "Handling privacy-sensitive medical data with federated learning: challenges and future directions," IEEE journal of biomedical and health informatics, vol. 27, pp. 790-803, 2022.

[18] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," Future Generation Computer Systems, vol. 115, pp. 619-640, 2021.

[19] C. Ma, J. Li, M. Ding, H. H. Yang, F. Shu, T. Q. Quek, et al., "On safeguarding privacy and security in the framework of federated learning," IEEE network, vol. 34, pp. 242-248, 2020.

[20] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez, D. Sánchez, A. Flanagan, and K. E. Tan, "Achieving security and privacy in federated learning systems: Survey, research challenges and future directions," Engineering Applications of Artificial Intelligence, vol. 106, p. 104468, 2021.

[21] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," IEEE Internet of Things Journal, vol. 9, pp. 8229-8249, 2022.

[22] J. Tan, Y.-C. Liang, N. C. Luong, and D. Niyato, "Toward smart security enhancement of federated learning networks," IEEE Network, vol. 35, pp. 340-347, 2020.

[23] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz, et al., "Secure and privacy-preserving intrusion

detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," Ad Hoc Networks, vol. 155, p. 103407, 2024.

[24] J. Zhang, H. Zhu, F. Wang, J. Zhao, Q. Xu, and H. Li, "Security and privacy threats to federated learning: Issues, methods, and challenges," Security and Communication Networks, vol. 2022, p. 2886795, 2022.

[25] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," IEEE Internet of Things Journal, vol. 9, pp. 2545-2554, 2021.

[26] N. M. Jebreel, J. Domingo-Ferrer, A. Blanco-Justicia, and D. Sánchez, "Enhanced security and privacy via fragmented federated learning," IEEE Transactions on Neural Networks and Learning Systems, 2022.

[27] J. Shen, W. Yang, Z. Chu, J. Fan, D. Niyato, and K.-Y. Lam, "Effective Intrusion Detection in Heterogeneous Internet-of-Things Networks via Ensemble Knowledge Distillation-based Federated Learning," arXiv preprint arXiv:2401.11968, 2024.

[28] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, et al., "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures," IEEE Transactions on Industrial Informatics, vol. 18, pp. 3492-3500, 2021.

[29] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Edge-Federated Learning based Intelligent Intrusion Detection System for Heterogeneous Internet of Things," IEEE Access, 2024.

[30] T. Nguyen and M. T. Thai, "Preserving privacy and security in federated learning," IEEE/ACM Transactions on Networking, 2023.