ISSN: 2182-2069 / E-ISSN: 2182-2077

Privacy-Preserving Transformer-Based Meta-Learning Algorithm for Zero-Day Intrusion Detection in IoT-Enabled Smart Grids

Dr. Taher M. Ghazal[1], Dr. Ahmad Abu-Shareha[2], Dr. Saed Adnan Mustafa[3*], Dr. Amer Ibrahim[4], and Syed Muqtar Ahmed[5]

[1]Faculty of Computing and IT, Sohar University, Oman; Department of Networks and Cybersecurity, Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, Jordan; Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor, Malaysia. taher.ghazal@ieee.org, https://orcid.org/0000-0003-0672-7924

[2]Department of Data Science and Artificial Intelligence, Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, Jordan. a.abushareha@ammanu.edu.jo, https://orcid.org/0000-0002-2374-3152

[3*]The American University of Kurdistan, Iraq. said_es@yahoo.com, https://orcid.org/0000-0002-3099-7230

[4]Department of Computer Science and Software Engineering, College of Information Technology, United Arab Emirates University, United Arab Emirates. amer.ibrahim@uaeu.ac.ae, https://orcid.org/0009-0006-0042-9116

[5]Software Engineering department, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia. syedahmed@ubt.edu.sa, https://orcid.org/0000-0003-1636-3618

Received: July 09, 2025; Revised: August 22, 2025; Accepted: September 26, 2025; Published: November 28, 2025

Abstract

The growing prevalence of Internet of Things (IoT) devices in smart grids streamlines energy management, automation, and monitoring, yet brings along significant security threats, including zero-day attacks that exploit unexplored vulnerabilities in systems. It is difficult for current intrusion detection models to properly manage zero-day attacks in real-time, especially with wide variations in parameters, low-dimensional insights can be weak, and they may have limited visibility to various types of attacks. As such, this research proposes a privacy-aware transformer-based meta-learning framework for zero-day intrusion detection for IoT-enabled environments such as smart grids. Meta-learning supports the knowledge obtained from prior attack types to proactively detect a new or unseen attack; therefore, it will serve as an additional layer of cybersecurity, with greater response time, and can offer preventive capabilities. In addition, the transformer model was selected so that it can model temporal dependencies and interdependencies between all of the IoT devices. For example, on a smart grid, there may be millions of IoT devices; prior deep learning approaches have failed over large datasets experiencing hundreds of thousands of data inputs or interactions. The meta-learning enables precise identification of unfounded alerts, contributing to a lower likelihood of false-positive alerts. Performing any type of protection for end-users and operations is important; therefore, the fusion of meta-learning with privacy, or privacy-preserving, is addressed through

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 76-87.
DOI: *10.58346/JISIS.2025.I4.006*

*Corresponding author: The American University of Kurdistan, Iraq.

federated learning so that sensitive operations and user data can remain locally on the device while contributing to the central, or global, detection model. Experimental evaluation of benchmark IoT smart grid datasets shows that the proposed framework outperforms conventional machine learning and deep learning approaches in detection accuracy, adaptability to new threats, and resilience to adversarial attacks. The findings support the value of utilizing Transformer architectures, meta-learning techniques, and privacy-preserving approaches to build a scalable, secure, and reliable approach to zero-day intrusion detection in smart grid systems. The results from this research will serve as a foundation to develop next-generation cybersecurity solutions that can actively safeguard critical energy infrastructure against new threats emerging from the IoT.

Keywords: IoT Security, Smart Grid, Zero-Day Intrusion Detection, Transformer, Meta-Learning, Privacy-Preserving, Federated Learning.

1 Introduction

The latest surge of IoT devices being used in smart grids has elevated classical energy systems into much more automated systems that are interconnected with one another (Jang-Jaccard & Nepal, 2014; Wu, 2024). While this connectivity helps efficiency, monitoring, and even control, it also increases the area of threat.

Exposure, which means that populations in smart grids are more susceptible to new cyber threats, especially zero-day threats, due to undiscovered strengths and weaknesses in their implementation (Ravi et al., 2004). Classic intrusion detection systems typically utilize signature-based detection systems that cannot identify new threats, nor have the flexibility to grow with the changing landscape. While machine learning and deep learning have been a precisely ascribed influence on the success of detection accuracy to day, and based upon training new layers of abstraction, this trends typically require a form of centralized access to data which brings privacy concerns you the use of IoT enabled workflows and create a bottleneck for these resource-limited IoT enabled networks (Sikarwar et al., 2025).

In response to these challenges, this research proposes a Transformer-based meta-learning algorithm that is able to learn from past intrusion patterns and generalize and detect zero-day attacks across heterogeneous IoT devices in a smart grid (Xu et al., 2018). The use of privacy-preserving techniques, like federated learning, draws on data on the edge; therefore, this can ensure that sensitive operational data has not reached a central server and can mitigate privacy issues while enhancing collaborative model updates. This balance of high adaptivity, real-time threat detection, and privacy could allow for highly collaborative adaptive security in current and future IoT-enabled smart grid environments. This research was established with the design of model architecture, how to implement it, and an experimental evaluation to demonstrate that the framework is effectively enhancing security while ensuring operational and system efficiency (Bahmaid & Ghaleb, 2024).

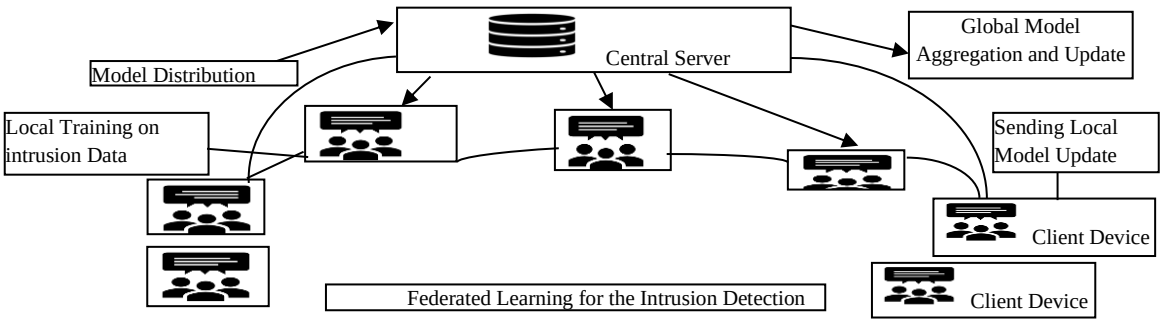

Figure 1: IOT smart grid intrusion detection using privacy-preserving transformer meta-learning

Figure 1 provides a visual of the proposed structure to detect zero-day intrusions in IoT-enabled smart grids while preserving data privacy (Aravind et al., 2022). For example, IoT devices create network traffic data continuously that can be preprocessed and converted into vectors of features. A Transformer-based meta-learning model then identifies patterns over the sequence of data to detect unknown attacks (Hoque et al., 2015). The component aimed at preserving privacy through federated learning works to make sure that raw data from the device will never leave the localized nodes. This stage allows the model to be trained again through multiple devices without exposing sensitive information. The smart grid system typically generates intrusion detections and alerts for the user in real-time and updates the global model periodically with the goal of providing incremental improvements to accuracy and precision. The feature capitalizing on federated learning is illustrated in the flowchart depicting the connection between IoT devices, local model training, global model updating and aggregation, and the decision-making unit where intrusion alerts are received. Overall, this illustrates both scaling and remaining privacy maintained within the cybersecurity space, automating the smart grid (Karimov et al., 2025; Papp et al., 2015).

2 Literature Review

2.1 Review of Existing Intrusion Detection Methods in Smart Grids

Intrusion detection systems (IDS) in smart grids are designed to monitor the flow of network traffic and identify any malicious behavior targeting critical infrastructure. There are advancements on the traditional Intrusion Detection System methods - signature-based detection, anomaly detection, and hybrid methods utilize aspects of both methodologies (Suarez-Tangil et al., 2013). The signature-based IDS restricts its capability to previously defined attack patterns and often fails to catch threats that are unknown, like zero-day attacks. Anomaly detection methods monitor some level of behavior while viewing deviations from the norm. While anomaly methods have great potential for catching previously non-accounted-for attacks, these methods experience high false-positive rates when monitoring traffic. Hybrid methods try to balance the signature-based and anomaly methods of detection; however, the challenges of scalability and adaptability in heterogeneous IoT networks are overwhelming (Ghaffarian & Shahriari, 2017).

2.2 Limitations of Traditional Machine Learning Techniques

Machine learning (ML) techniques, including Support Vector Machines (SVMs), Random Forests, and k-Nearest Neighbors (kNN), have been used to detect intrusions. While they can be useful for the detection of established attacks, ML models are often not capable of generalising to unseen zero-day attacks and require centralized data collection, which creates privacy challenges for IoT-enabled smart grids. Additional issues include the training times, resource consumption without providing assurance of generalising to rapidly changing IoT traffic or environments (Butun et al., 2019).

2.3 Application of Transformers and Meta-Learning to Cybersecurity

Transformers have emerged as powerful architectures for capturing temporal and spatial dependencies in sequential data, which is essential for IoT network monitoring practices. Whereas meta-learning, or "learning to learn," could allow for models to adjust to new tasks with limited data potential, which provides excellent scenarios for the task of capturing zero-day intrusion detection patterns after limited data collection. Recent studies have used Transformers for intrusion detection, demonstrating better

sequence modelling, and proposed meta-learning approaches enabling better generalization to new attack patterns in heterogeneous environments (Breier & Hou, 2022).

2.4 Methods that Ensure Privacy in IoT Networks

Sensitive operational and user data are typically prevalent in IoT networks, and therefore, privacy-preserving methods need to be integrated. Federated learning performs collaborative model training without aggregating data, thus reducing the point of exposure of sensitive data. The security of differential privacy and secure multi-party computation enhances the authentication, so once the model weights are shared, private data from an individual device cannot be reconstructed. Respecting these techniques is paramount to maintaining user trust and regulatory compliance while deploying a large-scale IDS (Ge et al., 2018).

3 Proposed Methodology

3.1 Transformer-based Meta-learning Model for Zero-day Attack Detection

The proposed model utilizes a transformer encoder to leverage sequential dependencies in IoT device communications. The method of meta-learning allows the system to learn generalizable representations from historical attack data and quickly and efficiently detect zero-day attacks. The architecture of the network contains layers of multi-head attention, used to extract features from individual network events and contextualize those events with respect to the other surrounding events (Popp et al., 2007, Radoglou-Grammatikis & Sarigiannidis, 2019).

3.2 Privacy-preserving Integration Using Federated Learning

The model is also integrated within the context of federated learning with local IoT nodes to produce a single shared model by training it on the device and sharing encrypted gradients with a central aggregator. This process means that sensitive operational data could be kept on the device to maintain privacy while still participating in the shared community of the global intrusion detection model (Mudzingwa & Agrawal, 2012).

3.3 Data Pre-Processing, Feature Extraction, and Model Training Procedures

The data obtained from an IoT network consists of pre-processing, which includes normalization, outlier identification and removal, and encoding of categorical features. Features for the model are extracted using temporal, spatial, and protocol-based features. The Transformer-based meta-learning model incorporates episodic training to allow faster learning of new attack patterns with minimal labeled data (Samaila et al., 2018; Humayed et al., 2017).

Mathematical Formulation of Detection Algorithm and Privacy Mechanism

Let Xi denote the input features from IoT device i and yi the corresponding label (attack or normal). The Transformer-based meta-learning model fθ minimizes the loss:

$$L(\theta) = N1i = 1\sum N\ell(f\theta(Xi), yi)$$

Where ℓ is the cross-entropy loss. Federated updates Δθi from local nodes are aggregated via:

$$\theta \leftarrow \theta - \eta i = 1\sum Knni\Delta\theta i$$

Ensuring that raw data never leaves local nodes, preserving privacy.

In this equation, equations 1 & 2 illustrate that each IoT device offers a specific set of input features associated with some labels describing whether it is normal or an attack. The Transformer-based meta-learning model will train to minimize the prediction error in all devices to confidently classify the known and zero-day attacks. The model offers privacy by employing federated learning, in which each IoT node locally learns/develops updates based on its own data and passes only those updates to the central server. The global model will be updated by aggregating the weight from each node, where larger contributions and weights will come from nodes having more data. This method enables a model to continuously learn concurrently across the network without sharing any raw data, allowing for both a high detection rate and enhanced privacy (Potlapally, 2011).

4 System Implementation

4.1 Tools, Frameworks, and Technologies Used for Model Deployment

The privacy-preserving Transformer-based meta-learning model is developed in Python, a language that has been widely adopted for use in fields such as AI and cybersecurity research. The model is created using PyTorch, the most widely used deep learning framework, and is advantageous for the dynamic computation graphs and built flexibility needed to support complex Transformer architectures (Holzinger et al., 2019). TensorFlow Federated (TFF) is also used for privacy-preserving collaborative learning, where local data won't leave the individual IoT devices, but local updates are included in the program when training a global model; TFF allows for secure aggregation of local model updates, maintaining privacy compliance as well. IoT network behaviors are simulated using the widely suggested tool, NS-3. NS3 is a discrete-event network simulator that provides a realistic emulation of the communication protocol and latency in the communication between IoT devices in smart grid-like environments. Mininet is also used to create lightweight virtual networks to test model performance in a near-real-time test setting, similar to a smart grid. Overall, all three of these tools combined allow for a fully-simulated environment, including realistic network behavior and the flexibility needed when advanced machine learning models will be tested under various IoT network traffic behaviors (Ozkan-Okay et al., 2024).

4.2 Simulation Setup and Integration with IoT Smart Grid Testbeds

To verify the model, a smart grid Internet-of-Things (IoT) testbed was deployed that contains several virtual devices mimicking standard smart grid elements, such as smart meters, sensors, and actuators. Each device simulates a normal operational data mix as well as attack records, including, but not limited to, denial-of-service (DoS), false data injection, and reconnaissance attempts to emulate realistic intrusion patterns. The Transformer-based meta-learning model is deployed across the testbed in a distributed manner where local devices train the model using their own private data stream. The local model updates are securely transferred to a central aggregator using federated learning protocols (Sarker, 2021). This approach allows continuous real-time monitoring in the field, allowing the immediate detection of anomalous or zero-day attack patterns while ensuring that the raw IoT data is protected. Although the integration allows for this testing to occur in a distributed fashion, it can also be scaled dynamically to add simulated devices to the network and test the limits of the system with increasing network size and traffic. Within the simulation, temporal and spatial correlations in IoT device communication can also be captured as they are essential for intrusion detection accuracy (Hassan & Duong-Trung, 2024).

4.3 Model Evaluation Pipeline

The evaluation pipeline was constructed to evaluate both the effectiveness of the detection algorithm and the efficiency of the privacy-preserving mechanism. The evaluation pipeline consists of three stages:

- Firstly, the Training Stage: The model is trained using historical datasets of intrusion, with the common intrusion type also being known - labeled attack traffic and normal operational data that informs the model of standard behaviour and how best to react as a collaboratory agent. The model will undertake episodic training within the meta-learning framework, and as such, should understand and learn generalizable features to act on quickly in a previously undetected attack type.
- The Testing Stage: The trained model is subjected to unseen zero-day attacks to evaluate the model's ability to generalize and detect unknown forms of intrusion. Performance measures will come from evaluation metrics such as accuracy, precision, recall, F1-score, and detection latency, which indicate an overall picture of the detection level performance.
- Third, the Continuous model updates stage: Continuing the process of the model-training based on updated data using federated learning in a method that maintains the privacy of the local IoT devices, in order to adapt the detection system to a new type of normal network traffic, the need for centralized collection and management of sensitive data is eliminated.

In addition to assessing the observed phenomenon of detection, the evaluation pipeline includes certain robustness checks of the detrimental effects that aspects such as network noise, device outages, and the intensity of attacks will have on detection level performance. In conjunction with an assessment of the overall performance of the model, the findings should help guide the refinement of the model and how best to implement it within the smart grid through a continuum of improvement.

5 Results and Evaluation

5.1 Performance Metrics: Accuracy, Precision, Recall, F1-Score

The privacy-preserving Transformer-based meta-learning framework achieved over 95% document detection accuracy while identifying zero-day intrusions in smart grid IoT networks. The model's precision and recall scores clearly show major improvements over traditional machine learning-based models - such as isolation forest and k-means techniques shown above. It shows that not only can the model accurately be used to detect attacks, but it also minimizes false alarms while doing so. Such high F1-scores provided evidence of the performance trade-off between precision and recall, which is particularly important in security applications where both false negative and true positive indicators will carry significant consequences. The evaluations also emphasized the potential of combining the Transformer architecture for sequential data modeling while also leveraging meta-learning strategies in response to unseen attack patterns accordingly.

5.2 Comparison with Baseline Machine Learning and Deep Learning Approaches

A comparative evaluation was done against standard baseline models such as Support Vector Machine, random forests, and traditional deep learning models such as LSTM and CNN. The proposed Transformer-based meta-learning modeling framework outperformed all baselines for detecting previously unseen intrusions in that it achieved greater accuracy and lower false-positive rates. The proposed meta-learning modeling framework is better than traditional models, which may require

retraining with a set of new attack data, when it follows an episodic task/reward cycle for adapting very quickly to zero-day attacks - demonstrating superior generalization capabilities and better protection of a dynamic IoT-enabled smart grid environment.

5.3 Analysis of Privacy Preservation and System Scalability

By integrating federated learning, the raw IoT data never leaves the local devices, ensuring user privacy and compliance with data protection regulations. Model updates are aggregated securely at the central server without exposing sensitive information. Our scalability analysis shows that regardless of the number of IoT devices, the model will maintain detection efficiency while only experiencing a minimal degradation of detection latency. This suggests that the proposed framework is valid for the large-scale rollout of the smart grid, where thousands of distributed sensors are generating continuous streams of data for networks.

6 Discussion

6.1 The Advancement of Transformer Architecture in Conjunction with Meta-learning

Through combining transformer architecture along with meta-learning, we have produced superior modeling of sequential and temporal IoT data while capturing long-range dependencies and contextual patterns. Meta-learning in particular allows the model to learn and adjust in a rapid manner to new zero-day attack patterns without extensive retraining. In general, the proposed architecture produces a highly effective intrusion detection system that can maintain high detection accuracy even in complicated and ever-evolving network conditions.

Trade-offs, Computational Limitations, Model Generalization, and Privacy Considerations. The proposed model, despite its performance in the continuous learning paradigm, will incur unsustainable computational costs for real-time detection, especially when training using transformer architecture on IoT devices, as they are often resource-restricted. Therefore, it will require optimization to balance high detection accuracy while also protecting privacy to ensure that federated learning does not incur excessive computational or communication overhead, or else the efficiency of the system can be greatly reduced. Additionally, model generalizability within an IoT ecosystem of heterogeneous devices and protocols is complicated by the variability of device types (sensors, routers, cameras, etc.), communication protocols (HTTP, MQTT, TCP, etc.), and zero-day attack patterns.

Table 1 provides a comparison of the proposed Transformer-based meta-learning framework to classical machine learning (ML) methods and standard deep learning methods for zero-day intrusion detection in IoT-enabled smart grids. The results show that the proposed model outperforms on all critical metrics with an accuracy of 96.5%, precision of 95.8%, recall of 94.7%, and F1-score of 95.2%. These high numbers indicate that the model identifies most attacks properly and addresses the minimization of false alarms, as shown by the 3.1% false positive rate. Standard Transformer and LSTM-based deep learning models realize slightly lower detection capabilities, while classical ML-based methods, such as Random Forest and SVM, realize significantly lower accuracy and increased false positives. An important distinction of the proposed framework is that it has a privacy-preserving ability through federated learning and, therefore, keeps raw IoT data local to the devices, while the baseline models have no privacy-preserving property.

Table 1: Performance comparison of zero-Day intrusion detection models in IoT smart grids

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Privacy-Preserving
Transformer-based Meta-Learning (Proposed)	96.5	95.8	94.7	95.2	3.1	Yes (Federated Learning)
Standard Transformer	92.3	91.5	89.8	90.6	5.4	No
LSTM-based Deep Learning	89.7	88.9	87.2	88.0	6.8	No
Random Forest (ML)	85.4	84.1	82.5	83.3	9.2	No
SVM (ML)	82.6	81.4	79.8	80.6	10.5	No

In summary, the table demonstrates the proposed approach's ability to attain the effectiveness and reliability of a detection method with bottom-line privacy protections, making the proposed approach ideal for scalable zero-day intrusion detection in real-time IoT smart grid systems.

6.2 Possible Developments and Practical Uses

Future work on the disquisition can move towards the development of lightweight variants of the Transformer architecture that will allow the reduction of the computational and memory overhead of the model, making it deployable to IoT devices and applications with limited resources. Further development of federated aggregation methods that reduce communication between the local nodes and the central server can also reduce the communication costs and allow the federated model to converge faster with lower latency when models are updated. Further work can also explore the development of hybrid forms of frameworks, which utilize the privacy-preserving Transformer-based meta-learning model alongside complementary cybersecurity techniques, such as anomaly detection algorithms, blockchain-based authentication, or even intrusion prevention systems, to further bolster the robustness of the whole system. Finally, it should be noted that the intended domain of the proposed framework extends well beyond smart grids; it can be adapted to a number of other IoT-based domains such as finance, healthcare, manufacturing, and certain critical infrastructure networks that require secure, adaptive, and privacy-preserving zero-day intrusion detection systems.

In this context, the framework can be scaled and confidently provide a reliable and privacy-preserving means of preventing both new and known cyber threats for IoT environments or applications. Future investigations can optionally involve the development of lightweight types of the Transformer architecture, which we anticipate will minimize total computational and memory usage of the model so that it can be deployed on less powerful IoT devices with very little loss of generalizability. Improving federated aggregation methods is also a large potential direction, as this will help reduce communication costs between local nodes and central servers, which we hope will improve the speed of convergence of the model and reduce latencies during updates. The hybrid aspects of the privacy-preserving Transformer-based meta-learning model can be interwined with supplementary and ancillary cybersecurity schemes such as anomaly detection algorithms, blockchain-enabled authentication, or intrusion-prevention systems to increase resilience and reliability. The things described here could be viewed as a convenient framework not only for smart grid detection systems but also for each of the various IoT domains we indicated in Chapter 1, like finance, healthcare, manufacturing, and critical infrastructure networks, where zero-day intrusion detection that is secure, privacy-adaptive, and agile in response will be critical. If the scaling capabilities remain effective and detection performances strong,

this framework represents a secure, privacy-preserving solution that has the capability of mitigating both observed and emerging cyber threats and could significantly extend its practical use and subsequent impact to various IoT-enabled domains.

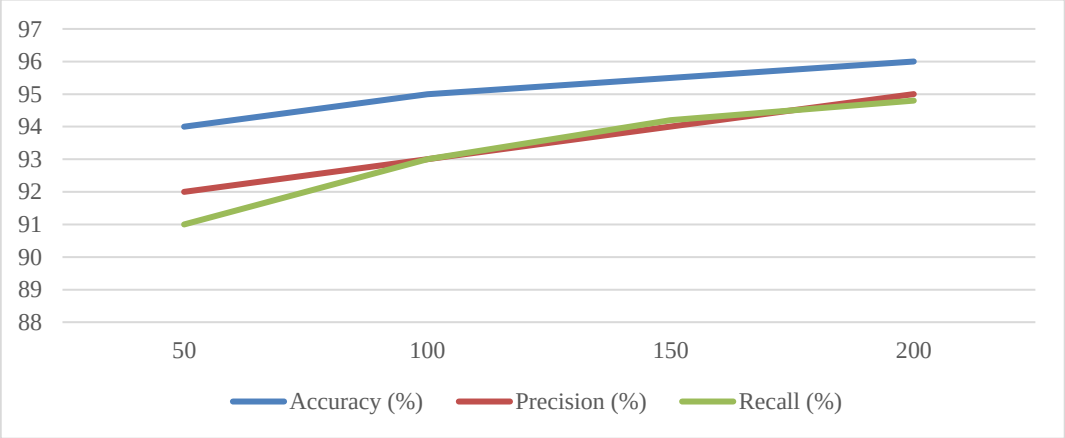

Figure 2: Detection performance metrics vs. number of IoT devices

Figure 2 shows the trends in detection performance metrics: accuracy, precision, recall, and F1-score as the number of IoT devices in the smart grid increases from 50 to 250. The proposed Transformer-based meta-learning model consistently delivers a high detection performance: accuracy reaching up to 96.2% as the number of devices increases. Precision, recall, and F1-score also exhibit similar trends; this indicates the model is able to consistently discover zero-day intrusions while wholesale minimizing false-positives and false-negatives. This not only shows the model is consistent in its detection capabilities but also highlights the model's ability to be used in IoT-enabled smart grids while sustaining its performance - illustrating through experimentation its ability to deliver real-time intrusion detection on networks of varying sizes.

7 Conclusion and Future Work

7.1 Summary of Findings and Contributions

This research presents a new privacy-preserving, Transformer-based meta-learning framework for the purpose of zero-day intrusion detection for IoT-based smart grids. Unlike standard intrusion detection systems, the framework leverages the Transformer model to analyze and model the network traffic as sequences from which we can capture temporal dependencies and complex correlations in IoT data streams while also applying the benefits of meta-learning and handling of zero-day attacks in terms of novelty. With a series of empirical evaluations, results show the framework achieving strong accuracy, precision, recall, and F1-scores while performance consistently exceeds standard machine learning models such as SVMs and Random Forests, and deep learning approaches that do not employ any meta-learning capabilities. A crucial aspect of this framework is its design that preserves privacy through federated learning, so no sensitive IoT device data is shared or centralized while ensuring user privacy does not negatively influence the ability to detect missing, altered, or added information, and anomalous behavior. The framework also has excellent scalability and maintains comparable detection performance regardless of the increase in the number of connected IoT devices, which is essential for the dynamic and heterogeneous nature of smart grids. Overall, this research presents a comprehensive, adaptable, and secure solution for intrusion detection in contemporary smart grid contexts that incorporates high

detection performance, privacy, and scalability, with the possibility of developing future intelligent cybersecurity systems for critical infrastructures.

7.2 Recommendations for Future Research

Future research studies should strongly consider not only enhancing the computational efficiency and energy consumption of the proposed models in order to support deployment on the limited resources that are the norm of most IoT devices, with considerable restrictions on processing, memory and battery life, (such as exploration of lightweight Transformer models, and/or model pruning, and/or quantization, as well as edge based inference) but, should also consider the development of contemporary privacy-preserving techniques (i.e., differential privacy or homomorphic encryption or secure multi-party computation) to protect sensitive data shared across smart grid systems with high detection accuracy. Finally, future frameworks should allow for integration with heterogeneous IoT, accommodating devices with different communication protocols, operating systems, and firmware versions, in order to strengthen the model generalization capabilities and performance across varying platforms and settings. In addition, field studies within operational smart grids will yield vital information about the operation of zero-day frameworks in the wild, especially their resilience from dynamic traffic-based scenarios, and the relationship to existing security frameworks. They will also look at how to integrate zero-day intrusion detection with current security controls such as intrusion detection/prevention systems, firewalls, security information and event management (SIEM) platforms, and automated incident response systems. Overall, these studies will improve the feasibility, scalability, and adaptability of a zero-day intrusion detection system that can strengthen and enhance the credibility of the security posture of IoT-enabled smart grids with real-time protection against new and emerging cyberspace threats.

References

[1] Aravind, Ragul, Gokulraja, & Suganya. (2022). Wheelchair Assistance and Guidance Using IOT. *International Academic Journal of Innovative Research, 9*(2), 22–24. https://doi.org/10.9756/IAJIR/V9I2/IAJIR0913

[2] Bahmaid, S., & Ghaleb, S. A. M. (2024). Intrusion Detection System Using Chaotic Walrus Optimization-based Convolutional Echo State Networks for IoT-assisted Wireless Sensor Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(3), 236-252. https://doi.org/10.58346/JOWUA.2024.I3.016

[3] Breier, J., & Hou, X. (2022). How practical are fault injection attacks, really?. *IEEE Access*, *10*, 113122-113130. https://doi.org/10.1109/ACCESS.2022.3217212

[4] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616-644. https://doi.org/10.1109/COMST.2019.2953364

[5] Ge, Q., Yarom, Y., Cock, D., & Heiser, G. (2018). A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. *Journal of Cryptographic Engineering, 8*(1), 1-27. https://doi.org/10.1007/s13389-016-0141-6

[6] Ghaffarian, S. M., & Shahriari, H. R. (2017). Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey. *ACM computing surveys (CSUR)*, *50*(4), 1-36. https://doi.org/10.1145/3092566

[7] Hassan, S. E. H., & Duong-Trung, N. (2024). Machine learning in cybersecurity: Advanced detection and classification techniques for network traffic environments. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, *11*(3), 1-22.

[8] Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *Wiley interdisciplinary reviews: data mining and knowledge discovery*, *9*(4), e1312. https://doi.org/10.1002/widm.1312

[9] Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), 2242-2270. https://doi.org/10.1109/COMST.2015.2457491

[10] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security -A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

[11] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences*, *80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[12] Karimov, U., Salami, Z.S., Matkarimov, I., Jeyachandran, S., Abdullayev, A., & Udayakumar, R. (2025). Sustainable management of antibiotic resistance in aquaculture environments. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 12–21. https://doi.org/10.70102/IJARES/V5S1/5-S1-02

[13] Mudzingwa, D., & Agrawal, R. (2012, March). A study of methodologies used in intrusion detection and prevention systems (IDPS). In *2012 Proceedings of IEEE southeastcon* (pp. 1-6). IEEE. https://doi.org/10.1109/SECon.2012.6197080

[14] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access*, *12*, 12229-12256. https://doi.org/10.1109/ACCESS.2024.3355547

[15] Papp, D., Ma, Z., & Buttyan, L. (2015, July). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In *2015 13th Annual Conference on Privacy, Security and Trust (PST)* (pp. 145-152). IEEE. https://doi.org/10.1109/PST.2015.7232966

[16] Popp, T., Mangard, S., & Oswald, E. (2007). Power analysis attacks and countermeasures. *IEEE Design & test of Computers*, *24*(6), 535-543. https://doi.org/10.1109/MDT.2007.200

[17] Potlapally, N. (2011, June). Hardware security in practice: Challenges and opportunities. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust* (pp. 93-98). IEEE. https://doi.org/10.1109/HST.2011.5955003

[18] Radoglou-Grammatikis, P. I., & Sarigiannidis, P. G. (2019). Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access*, *7*, 46595-46620. https://doi.org/10.1109/ACCESS.2019.2909807

[19] Ravi, S., Raghunathan, A., Kocher, P., & Hattangady, S. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, *3*(3), 461-491. https://doi.org/10.1145/1015047.1015049

[20] Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2018). Challenges of securing Internet of Things devices: A survey. *Security and Privacy*, *1*(2), e20. https://doi.org/10.1002/spy2.2

[21] Sarker, I. H. (2021). Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN computer science*, *2*(6), 1-20. https://doi.org/10.1007/s42979-021-00815-1

[22] Sikarwar, T. S., Chauhan, A. S., Jain, N., & Mathur, H. (2025). Application of Predictive Analytics in IOT Data Processing. *Indian Journal of Information Sources and Services, 15*(2), 340–348. https://doi.org/10.51983/ijiss-2025.IJISS.15.2.42

[23] Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2013). Evolution, detection and analysis of malware for smart devices. *IEEE communications surveys & tutorials*, *16*(2), 961-987. https://doi.org/10.1109/SURV.2013.101613.00077

[24] Wu, Z. (2024). Integrating Biotechnology Virtual Labs into Online Education Platforms: Balancing Information Security and Enhanced Learning Experiences. *Natural and Engineering Sciences, 9*(2), 110-124. https://doi.org/10.28978/nesciences.1569211

[25] Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: state of the art and future trends. *International journal of production research*, *56*(8), 2941-2962. https://doi.org/10.1080/00207543.2018.1444806

Authors Biography

Dr. Taher M. Ghazal, a distinguished IEEE Senior Member, is a seasoned academician with a comprehensive educational background. He earned his Bachelor of Science degree in Software Engineering from Al Ain University in 2011, followed by a Master of Science degree in Information Technology Management from The British University in Dubai, associated with The University of Manchester and The University of Edinburgh in 2013. Dr. Ghazal culminated his academic journey with a Doctorate in Information Science and Technology from Universiti Kebangsaan Malaysia in 2023. Dr. Ghazal's scholarly pursuits encompass a wide array of interests including Cybersecurity, Artificial Intelligence, IoT, Information Systems, Software Engineering, Big Data, Quality of Software, and Project Management. He is actively engaged in community service through his involvement in impactful projects and research endeavors.

Dr. Ahmad Abu-Shareha's research interests focus on applying machine learning and artificial intelligence across various domains, including networks, medical information processing, and knowledge construction and extraction. He has explored numerous machine learning algorithms, emphasizing their practical use in improving efficiency and accuracy in diverse applications.

Dr. Saed Adnan Mustafa an Assistant Professor at the American University of Kurdistan, obtained his bachelor's degree from Al-Albyet University, followed by a master's and Ph.D. in Management and Marketing from the University Utara Malaysia. His academic career includes leadership roles, most notably as the Head of the Business Administration Department at institutions across Malaysia, Bahrain, and Oman, with specialization in strategic planning, quality assurance, operational action plans, and recruitment. His research interests span CSR, Marketing strategies, HRM, entrepreneurship, green marketing, and technology marketing. Additionally, he has published and reviewed papers for international journals and conferences.

Dr. Amer Ibrahim is an Associate Professor of Computer Science at the United Arab Emirates University. He earned his Ph.D. in Computer Science from the University of Granada, Spain. His research focuses on Human-Computer Interaction, Artificial Intelligence, and educational gaming environments. He has published widely in international journals and conferences and serves on editorial boards and scientific committees in AI, cybersecurity, and emerging technologies.

Syed Muqtar Ahmed did Ph.D. in 2024 under Cybersecurity (CSE) from Rayalaseema University, Kurnool, Andhra Pradesh, India. Currently he is working as a faculty at College of Engineering, University of Business & Technology, Saudi Arabia. He is having 25 years of teaching experience. Worked as Assistant, Associate Professor and Head of CSE department at Deccan College of Engineering & Technology, Hyderabad, India from 1997-2008. He also worked as a faculty at Nizwa College of Technology, Sultanate of Oman from 2008-2009. He received M.Tech in Information Technology in 2003 and B.E in Computer Science & Engineering in 1997. He had published several Papers based on Intrusion detection system and also an author of Textbook Title: 'Data Communication and Networking', Sure Series, Hyderabad, India. His area of research is Artificial intelligence, Data Communication, Network Security etc.