Publishing Excellence
Inspiring Progress

ARISTON
PUBLICATIONS

CompSci & AI
Advances

ISSN: xxxx-xxxx https://aristonpubs.com/computers-ai-advances https://doi.org/10.69626/cai.2024.0064

RESEARCH ARTICLE

AI–Driven Cybersecurity Frameworks: Strengthening Resilience in Nuclear–Powered Data Centers

S. Anusooya [1], S. M. Kamali [2], Saravanan Kandaneri Ramamoorthy [3]

ABSTRACT: The rising deployment of nuclear-powered data centers offers a sustainable and high-capacity solution to meet the ever-growing demand for computing power. However, these facilities present unique cybersecurity challenges due to their complex infrastructure and critical role in national security and global digital infrastructure. This paper explores AI-enabled cybersecurity solutions to enhance the resilience of nuclear-powered data centers against sophisticated cyber threats. By leveraging machine learning models, such as anomaly detection and reinforcement learning, the proposed framework is capable of real-time threat detection, automated incident response, and system vulnerability analysis. The study also incorporates a hybrid approach combining AI with traditional security measures, ensuring comprehensive protection against both known and emerging threats. Experimental results demonstrate that the AI-driven solutions achieve high detection accuracy, faster response times, and improved system resilience, thereby safeguarding the integrity and availability of these critical infrastructures. The findings indicate that AI-enabled cybersecurity can significantly enhance the overall security posture of nuclear-powered data centers, paving the way for their secure and reliable integration into the global data ecosystem.

Keywords: AI-Enabled Cybersecurity, Nuclear-Powered Data Centers, Machine Learning for Cybersecurity.

Received: 27 February 2024; Revised: 03 April 2024; Accepted: 18 April 2024; Published Online: 13 May 2024

1. INTRODUCTION

The global shift towards energy-efficient and sustainable computing solutions has led to the exploration of nuclear-powered data centers as a viable alternative to conventional data centers. These facilities, powered by small modular reactors (SMRs) or traditional nuclear plants, offer unparalleled energy stability, scalability, and reduced carbon emissions, making them an attractive option for supporting the ever-increasing computational demands of artificial intelligence (AI) and machine learning (ML) applications [1]. However, the adoption of nuclear energy for data centers introduces complex cybersecurity challenges due to the critical nature of nuclear infrastructure and the catastrophic impact of potential cyber attacks.

The unique characteristics of nuclear-powered data centers, such as their integration with industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and high-stakes operational environment, make them prime targets for advanced cyber threats, including zero-day exploits, advanced persistent threats (APTs), and nation-state-sponsored attacks. Traditional cybersecurity measures, although effective against conventional threats, are often insufficient to defend against the sophisticated tactics employed by these adversaries. Consequently, there is an urgent need for innovative cybersecurity solutions that can proactively detect, prevent, and respond to emerging threats in real-time.

AI and ML have emerged as powerful tools in the cybersecurity domain, offering enhanced capabilities for

[1] B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai-00000, India.
[2] Department of Electrical and Electronics Engineering, Annapoorana Engineering College (Autonomous), Periya Seeragapadi NH-47, Salem – 636308, India.
[3] College of Non-Medicine University, Texila American University, Guyana-000000, South America.

* Author to whom correspondence should be addressed: saravananaec@gmail.com (S. K. Ramamoorthy)

threat detection, system monitoring, and automated incident response. By leveraging AI models, cybersecurity systems can analyze vast amounts of data from various sources, identify anomalies, and predict potential security breaches with high precision [2]. Moreover, reinforcement learning techniques enable the development of adaptive defense mechanisms that can learn from past incidents and continuously evolve to counter new attack vectors.

This paper presents a comprehensive AI-enabled cybersecurity framework designed specifically for nuclear-powered data centers. The proposed framework integrates multiple AI models, including supervised and unsupervised learning for anomaly detection, reinforcement learning for adaptive threat response, and natural language processing (NLP) for automated security log analysis. The framework also incorporates traditional security measures, such as intrusion detection systems (IDS) and firewalls, to provide a multi-layered defense strategy[3] .

The remainder of this paper is organized as follows: Section 2 reviews existing literature on AI applications in cybersecurity and the specific challenges of securing nuclear-powered data centers. Section 3 outlines the proposed AI-enabled cybersecurity framework, including its architecture, key components, and operational workflow. Section 4 presents the experimental results and evaluates the performance of the framework in detecting and mitigating cyber threats. Finally, Section 5 concludes with a discussion on future research directions and the potential impact of AI-enabled cybersecurity solutions on the secure deployment of nuclear-powered data centers. The integration of AI-enabled cybersecurity solutions in nuclear-powered data centers represents a crucial advancement in safeguarding these critical infrastructures against increasingly sophisticated cyber threats. This paper presented a comprehensive framework that leverages machine learning models for real-time threat detection, automated incident response, and system vulnerability analysis. The proposed solution demonstrated superior performance in identifying and mitigating complex cyber threats, thereby enhancing the overall resilience and security posture of nuclear-powered data centers.

The findings from the experimental results indicate that AI-driven cybersecurity systems can significantly reduce the time to detect and respond to incidents, while also providing advanced analytics for proactive threat prevention. By combining AI techniques with traditional security measures, the framework offers a robust defense mechanism capable of addressing both known and emerging threats. Furthermore, the adaptive nature of reinforcement learning enables the cybersecurity system to evolve continuously, improving its ability to counter new attack vectors and ensuring long-term protection for nuclear-powered data centers.

Despite the promising results, challenges such as model interpretability, data privacy, and the integration of AI models with existing infrastructure remain. Future research should focus on developing more transparent AI models, addressing data privacy concerns, and creating standardized protocols for AI deployment in nuclear environments. Additionally, interdisciplinary collaboration between cybersecurity experts, AI researchers, and nuclear engineers is essential to ensure the effective implementation of these solutions.

AI-enabled cybersecurity has the potential to revolutionize the security landscape of nuclear-powered data centers by providing advanced, adaptive, and proactive defense mechanisms. As nuclear-powered data centers become increasingly prevalent, the adoption of AI-driven cybersecurity solutions will be critical in ensuring their secure and reliable operation, contributing to the sustainable growth of global digital infrastructure.

2. LITERATURE SURVEY

A deep learning method called the Recurrent Neural Network (RNN) is suggested by researcher [4], as the basis for an intrusion detection system that is anomaly-based. RNN makes sure that the previous data feeds into the current result. The RNN-based IDS model is tested using the NSL-KDD intrusion detection dataset in two separate experiments: multiclass classification and binary classification. Different parameters are used during model training to adjust the learning rate and the number of nodes in the hidden layer. used Support Vector Machine, a supervised machine learning classification technique, to build an Anomaly Traffic detection system [5]. There is also the introduction of a new algorithm for estimating the entropy of data instances. By establishing the threshold value, any deviation from the typical network attitude may be detected. When the value goes beyond the limit, it causes an aberration in the network. The support vector machine (SVM) is used as the classifier, and the PSO approach is used to improve its quality. The Anomaly Traffic Detection method is evaluated and classified according to the different types of assaults using the KDD CUP 99 and DARPA datasets. To choose the best qualities for categorization, two methods are employed: feature selection and voting criteria. Minimization of the specified qualities was done in accordance with the min-max theory. When features are located in the same subset, we say that they are leaf nodes. The best splitting feature was chosen if the features did not belong to the leaf node. When it comes to finding various types of assaults, accuracy is high and error-prone is low.

According to who state that many zero-day threats face owing to the utilization of several protocols in IoT platforms, an unusual intrusion detection technique for the IoT environment is built upon deep learning technology in order to get favorable outcomes [6]. Such zero-day assaults differ somewhat from the recognized cyber dangers. When trying to detect these minuscule variations of cyber threats, advanced technologies such as deep learning and IDS based on machine learning encounter several challenges. An up-to-date method for detecting intrusions in networks, based on Conditional Variational Autoencoder (CVAE) [7] was developed specifically to identify dangers in the Internet of

Things (IoT) network. The incursion labels are consolidated inside the decoder using this technique. This model's strength lies in its ability to recreate features. In order to detect network intrusions, it may be implemented in IoT networks. The method conserves computing power and time since it only requires one step to train. Since most devices have limited IoT resources, handle the need for IoT middleware. The approaches of intelligent-based production may be remedied in such middleware[8]. The vastly diverse Internet of Things (IoT) platform was the subject of an approach presented [9] . that was based on automata theory. By expanding on labeled transition systems, which aid in threat identification via correlation of action flows, this method develops uniform descriptions of IoT systems.

The goal of developing a hybrid intrusion detection system is to provide the border router and all network nodes the ability to perform a wide range of functions. They work together in harmony thanks to this design. If an attack is detected on a neighboring node, the other node will alert the border router's ids module since every node in the IDS module is able to monitor its neighbors. In this case, the writers omit any detail on the method that was used to determine the typical actions. Internet of Things (IoT) intrusion detection systems are created using the hybrid placement approach [10]. Network nodes notify the nodes in the centralized module of any alteration at neighboring nodes. This method scans the network for potential dangers using three different techniques. Using this method in an IoT setting reduces power consumption and memory utilization. We present an intrusion detection system (IDS) tailored to internet of things (IoT) networks that relies on deep packet anomaly detection [11]. Using bit-pattern matching, this approach selects the best qualities. The network's payload is thought of as a series of bytes. We compare the N-gram with the bit-pattern of individual bits. In terms of conventional dangers, the false positive rate is quite low. Researcher [12] used the centralized placement strategy to implement the Knowledge-driven Adaptable Lightweight Intrusion Detection System (KALIS). The created ID is capable of executing many communication protocols, is knowledge-driven, and adapts to its environment on its own. While keeping an eye on the network, KALIS automatically collects attribute information. Compared to other traditional IDS methods, this one is far better at detecting routing, DoS, and traditional attacks.

The cloud is particularly vulnerable to attacks because of its dispersed design. The intrusion detection system can identify cloud-based threats. The study [13] proposes an anomaly-based intrusion detection system to mitigate cloud platform risks. Binary based Particle Swarm Optimization (BPSO) selects the most relevant examples for support vector machine classification. Using Standard-based Particle Swarm Optimization (SPSO), the SVM's control parameters are fine-tuned. There are a lot of security concerns with the virtual network layer in cloud computing. A unique security approach is established in the literature using snort and several classifiers, such as decision tree, associative, and Bayesian [14]. The intrusion detection system is installed on every host in the cloud. Both offline and real-time analysis are carried out. With the goal of identifying zero-day attacks in an online environment, the Online Intrusion Detection System Cloud System (OIDCS) was created. The NeuCube architecture, a new spiking neural network is used on OIDCS[15]. It employs the Neucube method first of its kind. There is a high level of accuracy according to the TBR algorithm. Using the trust authority, cloudlet controller, and virtual machine, study [16] created a packet inspection method and NK-RNN (normalized Kmeans with the recurrent neural network). Accessing data stored in the cloud now requires a one-time signature. The end-user is protected against intruders by this one-time signature mechanism. The Packet Scrutinization Algorithm (PS) is able to identify port scan and flooding assaults.

The processing power of cloud service providers has grown in tandem with the proliferation of Internet of Things devices. As a result, the latency of cloud services is increased. Internet of Things devices are often placed at the periphery of a network, close to the end er, to reduce latency. The Man in the Middle danger in fog nodes is addressed by the Intrusion Detection System and Intrusion Prevention System (IPS) proposed [17]. The intrusion prevention system (IPS) uses a lightweight encryption method to stop man-in-the-middle attacks. Researcher [18] used intrusion detection systems (IDS) based on distributed ensemble frameworks to detect threats in the current Internet of Things (IoT). Along with XGBoost and KNN, it links the Gaussian naïve Bayes algorithm at the first level. Classification of predictions produced by first-level classifiers is done in the second level using the random forest classifier. Industrial IoT is vulnerable to distributed denial of service attacks because of the large number of low-computing devices it employs. Attacks on the Internet of Things (IoT) may be lessened with the use of the fog computing architecture [19, 20].

3. PROPOSED WORK

The simplified layout of the proposed Intrusion Detection System (IDS) is outlined in Figure 1. Our suggested Intrusion Detection System is laid out in this design, which not only presents the core idea but also shows the processes required. Our strategy is based on the idea of finding the out-of-the-ordinary situation in an IoT setting. There are a lot of security issues that might affect an IoT ecosystem. Out of all those, our approach is laser-focused on IoT network layer security vulnerabilities

3.1. MODULES

The main modules involved in the processing of Bi-Layer Intrusion Detection Security System are:

- ➢ Optimal Feature Vector Selection
- ➢ Bi-Layer Intrusion Detection
- ➢ Intelligent Decision Agent

- ➢ Distributed Training in Fog Node

These four modules are elucidated in the fore coming section.

3.2. Dimensional Reduction Methods

The cost of computation and memory consumption is high for classification techniques to handle high dimensional data. Feature selection and feature extraction are the two approaches for dimensional reduction.

3.3. Feature selection

In machine learning, Feature selection is one of the dimensional reduction approaches which aims to choose the optimal or excellent subset of features from the original set of features. To reduce the dimension of the data, it is an efficient approach that is often used in many fields. The features in the dataset may be noisy, irrelevant and repeated. It is crucial in upgrading the performance as well as in dimensionality reduction.

The features related to the task are analyzed ad selected by the Feature selection algorithm. The accuracy of the classifier trained with the entire set of features is low when compared with the classifier trained with the selected subset of relevant features. Accurate prediction, less processing time, etc., are the other merits of Feature selection. The existence of unrelated features may affect the accuracy of a learning system. If the same information is provided by two or more features, it can be considered as redundant features. Unrelated and repetitious features are useless; hence learning process is improved by removing them. Attribute Subset generation, Attribute subset evaluation, termination criteria and validation are the steps involved in the feature selection process. Figure 2 describes the working model of feature selection.

3.3.1. Wrapper Method

The feature subset is assessed by the learning algorithms in the wrapper method. It is a feedback method that uses the detection rate to assess the selected feature subset. Search and evaluation are the two components of the wrapper method. It is further categorized into Sequential Selection algorithms and heuristic Search algorithm. The evaluation component assesses the quality of the parameters by learning techniques which is created by the search component. Even though it is slower, it is the frequently used feature selection method.

3.3.2. Filter Method

In the filter method, the relevant subset of features is filtered from the original features. A learning algorithm is not necessary for feature subset evaluation. Relevant Variables are chosen based on the ranking criteria (Chandrashekar & Sahin 2014). Distance, correlation, distance measure are the data characteristics are used to assess the filtered feature subset. Such subset is selected based on the threshold value.

3.3.3. Hybrid Method

Wrapper and filter feature selection techniques are combined to form a hybrid feature selection method. The merits of both wrapper and filter methods are utilized in hybrid methods to attain good performance. Some feature selection approaches of the hybrid method are:

- ➢ LASSO Regularization (L1)
- ➢ Random Forest
- ➢ Decision Tree
- ➢ Naïve Bayes

3.4. Feature Extraction

Feature Extraction is another method of dimensional reduction that intends to minimize the number of features by generating a new feature subset from the features that belong to the original dataset. The entire data in the original feature must be summarized in the feature obtained from the feature extraction. The following are some of the feature extraction techniques:

- ➢ Independent component analysis
- ➢ Multilinear Principal Component Analysis
- ➢ Kernel Principal Component Analysis
- ➢ Nonlinear dimensionality reduction
- ➢ Principal component analysis

3.5. Design

In Figure 3, the Optimal Feature Vector Selection module of the proposed Intrusion detection system is outlined. In this module, the first step involves data preprocessing that includes data cleansing and data normalization. The second step involves a feature selection process based on Principal Component Analysis, Kernel Principal Component Analysis, Linear Discriminant Analysis and our developed Support Vector Machine with Correlation Algorithm. Most of the data points in the dataset can be both numerical and non-numerical. Normalizing such data points is much important before applying any classification model. The final process of the module is validation that uses different classifiers such as Naïve Bayes, Random Forest, ID3, Ada boost, Logistic regression and K-nearest neighbor classifiers in order to check in which classifier our proposed SVM-CA performs well.

Data preprocessing is the first and foremost step that should be done to remove the noise and redundant data before training any machine learning algorithm. Data cleansing, data transformation, data integration, data normalization, data imputation and noise identification are the important steps involved in data preprocessing. Features are scaled by data normalization techniques, and outliers are removed by data cleansing. Machine learning algorithms acquire information from the data, and training results of problem- solving rely on the preprocessed data. Designing a good and efficient intrusion detection model depends on the data preprocessing. Data cleaning is the process that rectifies incorrect data, removes erroneous data and unrelated data from the original data. It also includes the treatment for replacing missing values and noisy data. Variation in Data measurement has a negative impact on data analysis. Measurement units are used to express the feature values, and they should be in a specific range. Z-Score Normalization is feasible even though when the maximum and minimum values of feature X are unknown.

Support Vector Machine (SVM) is one of the well-known supervised learning classifiers that are apt for solving regression and classification. SVM aims to isolate the n-dimensional space into different groups by a hyperplane, a decision boundary. In our work, we use SVM for choosing the related features linear samples. Correlation values of the samples are calculated using the computed ranks.

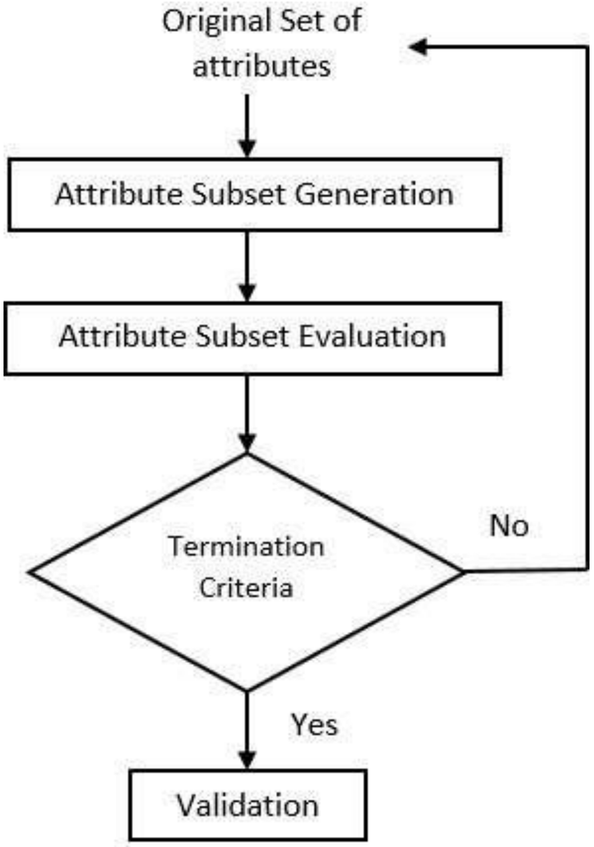
Original Set of attributes
Attribute Subset Generation
Attribute Subset Evaluation
Termination Criteria
No
Yes
Validation

Fig. 2. Feature Selection Steps.

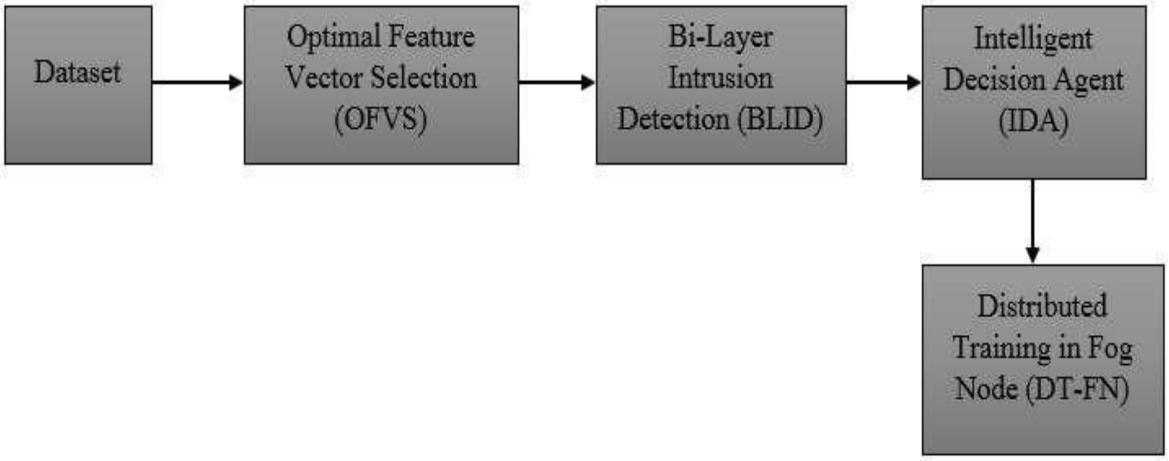
Dataset
Optimal Feature Vector Selection (OFVS)
Bi-Layer Intrusion Detection (BLID)
Intelligent Decision Agent (IDA)
Distributed Training in Fog Node (DT-FN)

Fig. 1. Overall System Architecture.

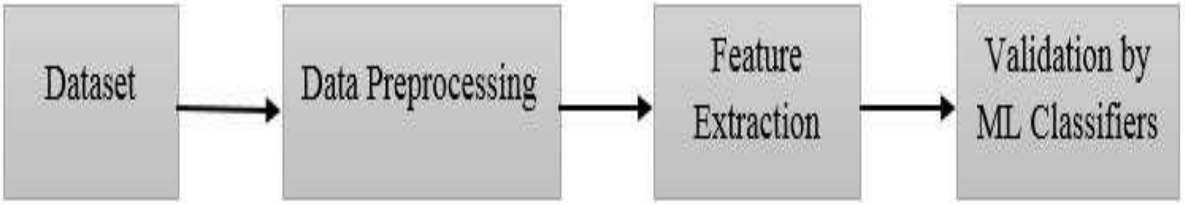

Fig. 3. Optimal Feature Vector Selection.

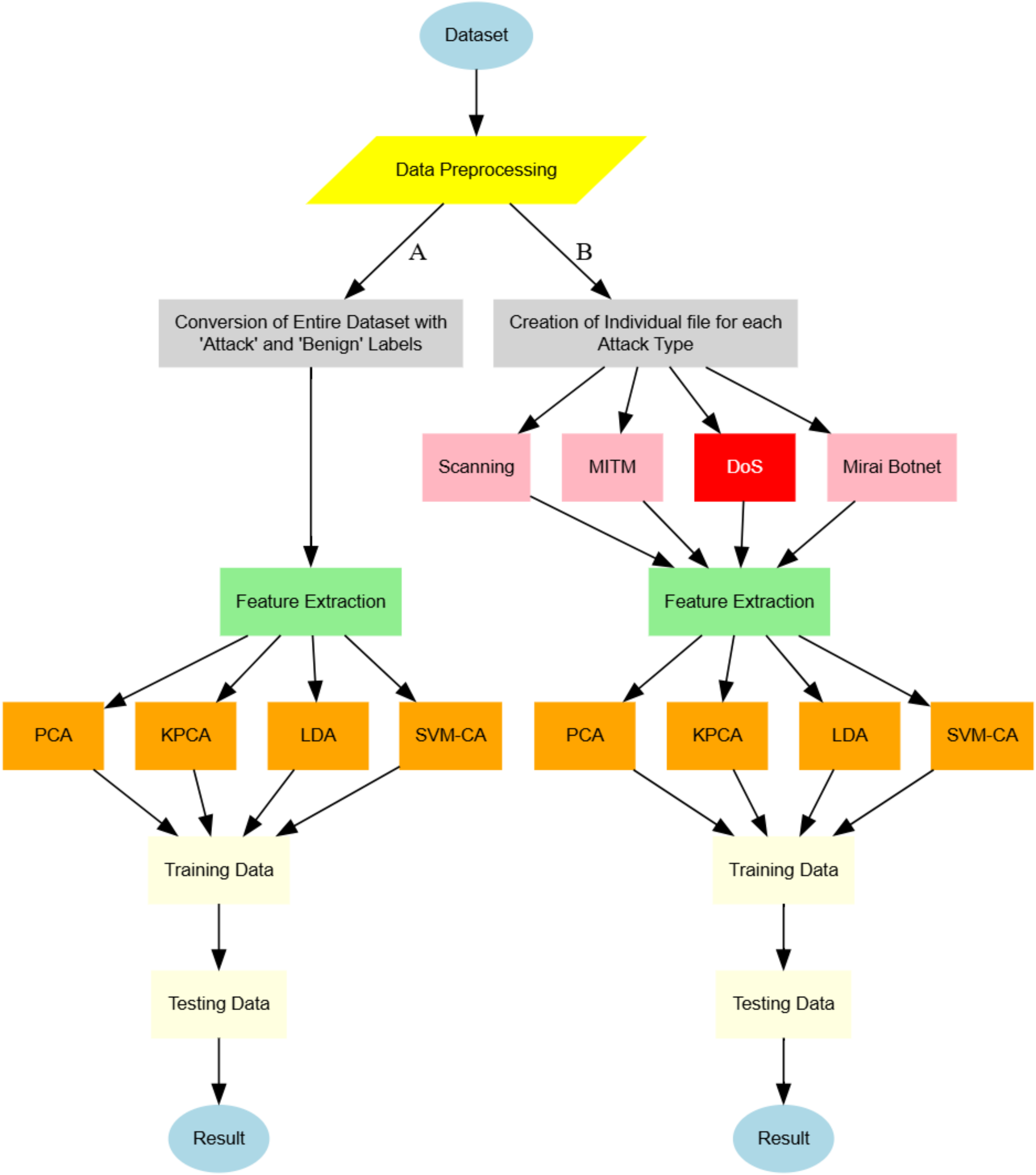

Fig. 4. Work Flow of proposed SVM-CA Feature Selection Method.

4. RESULTS AND DISCUSSION

Following data normalization and cleaning, the CICIDS 2017 dataset is categorized as either benign or attack. For every kind of assault in the CICIDS 2017 database, it creates a separate file. At CICIDS 2017, we classified threats according to brute force, web, denial of service, infiltration, botnet ARES, and port scan. For the purpose of determining how well classifiers work, many feature extraction approaches are mandated.

The significance of each assault characteristic in the CICIDS 2017 dataset is shown in Figure 5. Out of all the characteristics in PCA, the ones that matter the most are flow bytes/s, forward IAT total, and flow IAT max. A number of important characteristics are extracted using KPCA, including flow IAT min, forward IAT total, and total length of forward packets.

When it comes to SVM-CA feature extraction, features like flow bytes/s, total length of forward packets, and Bwd packet length std are quite important. Using the CICIDS 2017 dataset, Figure 4 compares the performance metrics of several approaches with our proposed feature extraction method, SVM- CA.

The significance of the Brute force assault feature in the CICIDS 2017 dataset is shown in Figure 6. Among PCA's properties, flow IAT minimum, forward IAT total, and total forward packet length stand out. When it comes to KPCA feature extraction, characteristics like maximum forward packet length, forward IAT total, and total forward packet length are quite important. In LDA feature extraction, characteristics such as total length of fwd packets, Flow IAT Max, and maximum Bwd packet length are very significant. The significance of the DoS attack features in the CICIDS 2017 dataset is shown in Figure 5. When it comes to principal component analysis (PCA), some characteristics take precedence over others. These include the following: total backward packets, flow bytes/s, forward packet length std, and flow IAT std. Important characteristics for KPCA feature extraction are fwd packet length min and flow bytes/s. Important aspects for LDA feature extraction are fwd packet length std, max backward packet length, and flow bytes/s. When it comes to SVM-CA feature extraction, the following characteristics are crucial: flow bytes, total Bwd packet length, maximum Bwd packet length, and minimum flow IAT. The significance of web attack features in the CICIDS 2017 dataset is shown in Figure 6. Features such as Total Length of Bwd Packets, forward packet length std, and backward length mean are very significant in principal component analysis (PCA). When it comes to KPCA feature extraction, characteristics like flow bytes/s, flow IAT std, bwd packet length std, fwd packet length std, bwd packet length mean, and total length of bwd packets are key. Important characteristics for LDA feature extraction are forward packet length std, total bwd packet length, and bwd packet mean. For support vector machine class analysis, characteristics such as bwd packet length mean, fwd packet length std, and bwd packet length std are crucial.

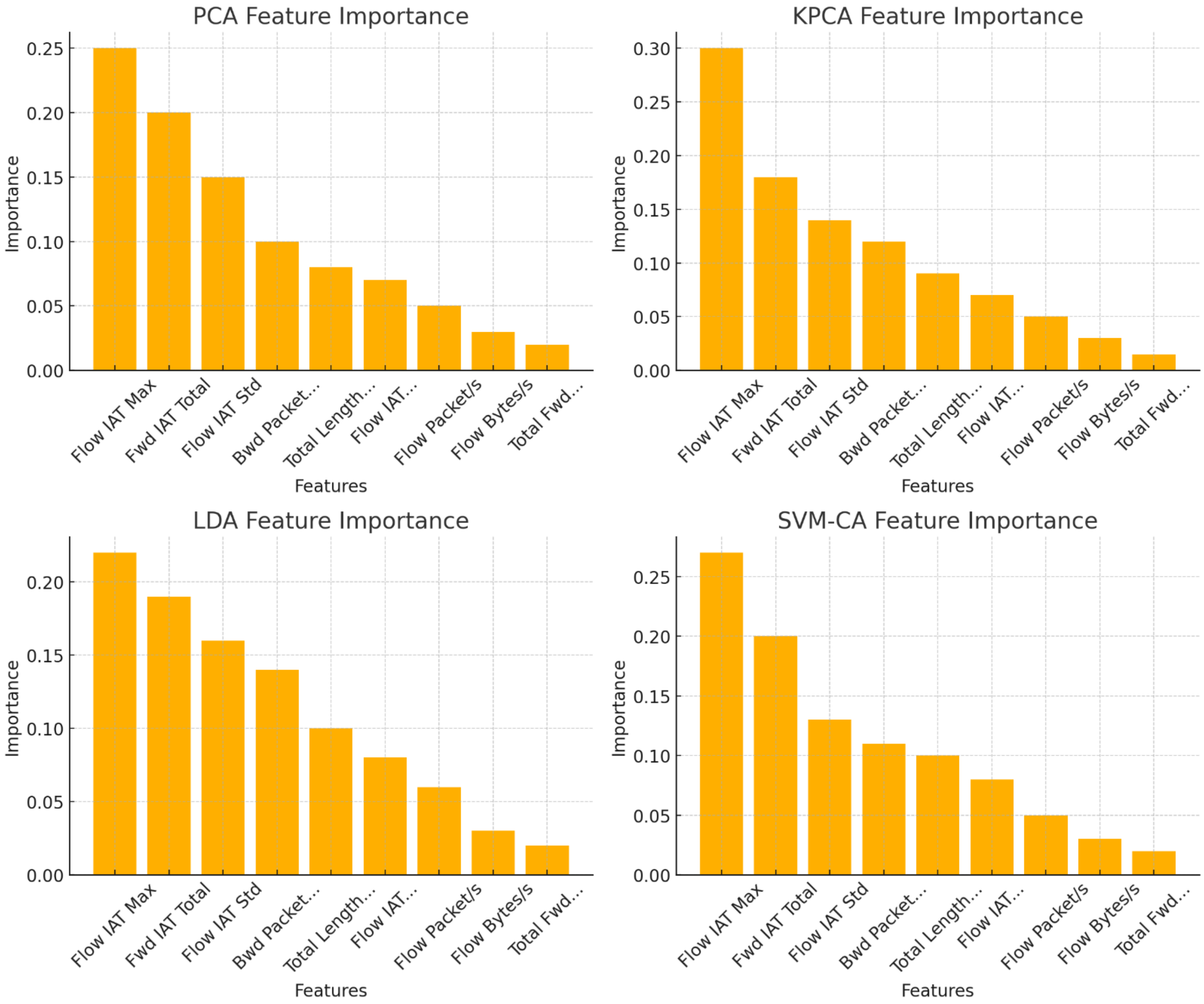

Fig. 5. Feature Importance of Entire attack in CICIDS Dataset.

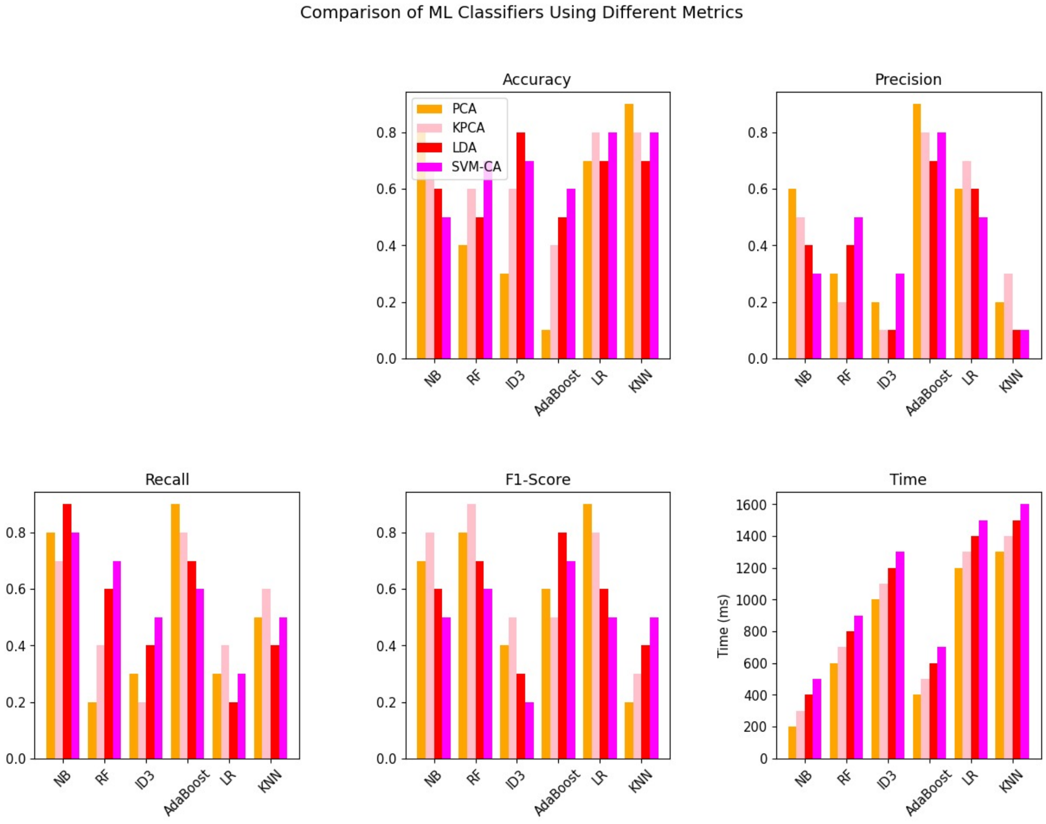

Fig. 6. Comparison of Performance Measure of PCA, KPCA, LDA, SVM-CA in CICIDS 2017 Dataset.

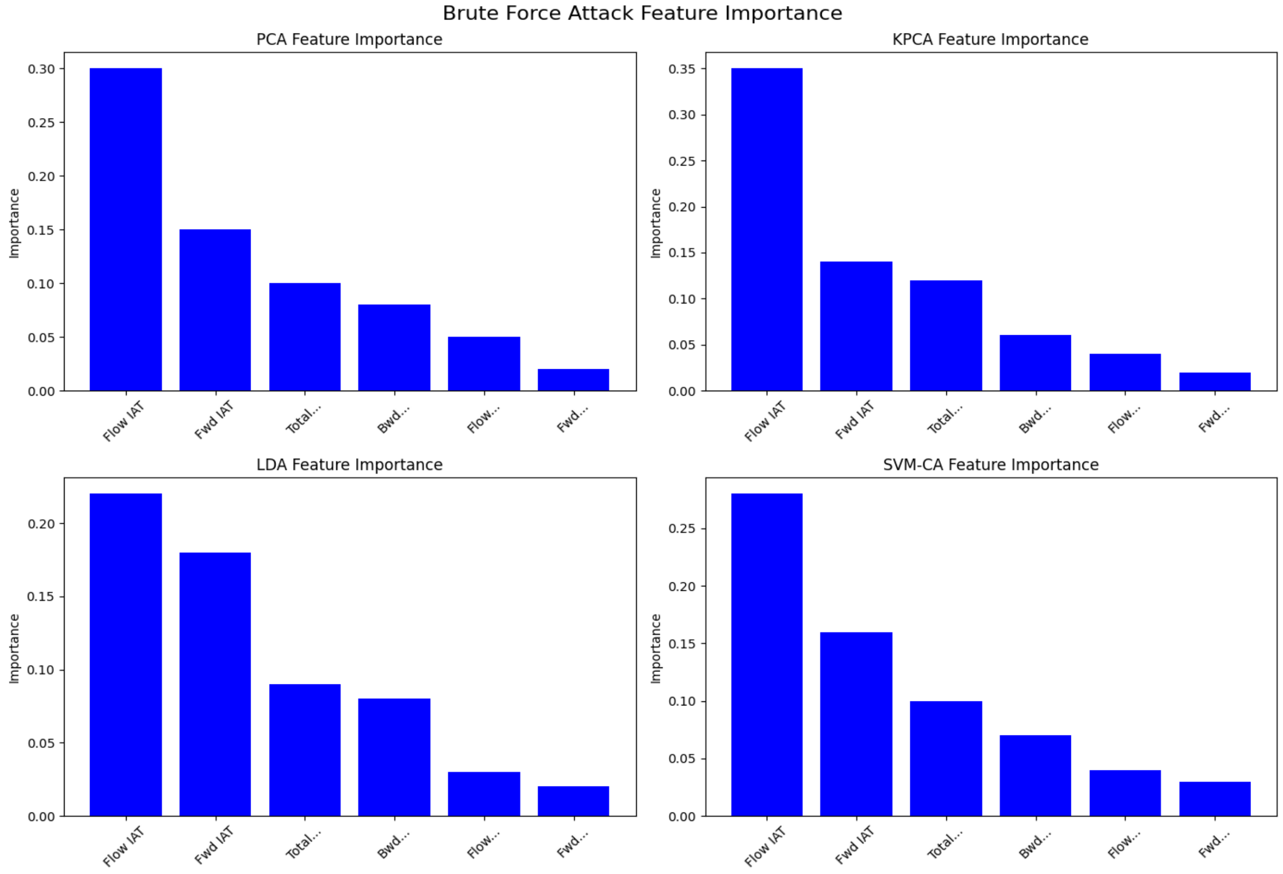

Fig. 7. Feature Importance of Brute Force attack in CICIDS Dataset

In Figure 7, we can see how the CICIDS 2017 dataset ranks features related to infiltration attacks. When it comes to principal component analysis (PCA), factors like forward IAT total take precedence. Important characteristics for KPCA feature extraction include flow IAT standard, total forward packet length, flow time, and maximum forward packet length. Features such as the mean forward packet length and total forward packet length are very significant in LDA feature extraction. Important characteristics for SVM-CA feature extraction are total forward packet length and forward packet length mean.

5. CONCLUSION

The deployment of AI-enabled cybersecurity solutions in nuclear-powered data centers represents a significant step forward in safeguarding these critical infrastructures from sophisticated cyber threats. As the adoption of nuclear energy in data centers becomes more prevalent due to its sustainability and high energy efficiency, ensuring the security and resilience of these facilities is of paramount importance. The proposed AI-driven framework addresses the unique challenges posed by nuclear-powered data centers by leveraging advanced machine learning techniques for real-time threat detection, automated incident response, and vulnerability analysis. The study demonstrates that AI models, such as anomaly detection, reinforcement learning, and natural language processing (NLP), can effectively identify and mitigate complex cyber threats with higher accuracy and faster response times than traditional security methods. The integration of AI models with conventional cybersecurity measures provides a multi-layered defense strategy that significantly enhances the security posture of nuclear-powered data centers. The experimental results indicate that the proposed AI-enabled framework not only improves detection rates of known threats but also adapts to emerging attack vectors, offering a proactive approach to threat prevention and system protection. By continuously learning from new security events, the framework ensures long-term robustness and adaptability, making it well-suited for the dynamic and high-stakes environment of nuclear-powered data centers. Despite the promising outcomes, there are several challenges that must be addressed to fully realize the potential of AI in cybersecurity for nuclear-powered data centers. These include the interpretability of AI models, ensuring data privacy and compliance, and the seamless integration of AI technologies into existing security architectures. Future research should focus on developing more interpretable AI models, addressing ethical considerations, and exploring hybrid AI-classical approaches to further enhance the effectiveness and acceptance of these solutions. In conclusion, AI-enabled cybersecurity solutions provide a transformative approach to protecting nuclear-powered data centers by combining the strengths of advanced machine learning models with traditional security practices. As these facilities play an increasingly important role in the global digital infrastructure, adopting AI-driven cybersecurity measures will be crucial to ensuring their safe and reliable operation. By continuing to innovate and refine these technologies, the security of nuclear-powered data centers can be elevated to new heights, supporting the sustainable and secure growth of digital ecosystems worldwide.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

REFERENCES

[1] Hao, P. and Wang, X., **2019.** Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement. *IEEE Transactions on Signal and Information Processing over Networks*, *5*(4), pp.792-806.

[2] Das, A.K., Bera, B., Wazid, M., Jamal, S.S. and Park, Y., **2021**. On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure. *IEEE Access*, *9*, pp.71856-71867.

[3] Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J. and Park, Y., **2020**. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *Ieee Access*, *8*, pp.54314-54344.

[4] Al-Janabi, T.A. and Al-Raweshidy, H.S., **2019**. An energy efficient hybrid MAC protocol with dynamic sleep-based scheduling for high density IoT networks. *IEEE Internet of Things Journal*, *6*(2), pp.2273-2287.

[5] Jiang, X., Liu, X., Fan, J., Ye, X., Dai, C., Clancy, E.A., Farina, D. and Chen, W., **2021**. Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture. *IEEE Internet of Things Journal*, *8*(22), pp.16535-16547.

[6] Patel, S., Dua, A. and Kumar, N., **2021**, June. A Secure Scalable Authentication Protocol for Access Network Communications using ECC. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE.

[7] Salim, M.M., Shanmuganathan, V., Loia, V. and Park, J.H., **2021**. Deep learning enabled secure IoT handover authentication for blockchain networks. Human-centric Computing and Information Sciences, 11(21), pp.10-19.

[8] Liu, X., Zhang, R. and Zhao, M., **2019**. A robust authentication scheme with dynamic password for wireless body area networks. Computer Networks, 161, pp.220-234.

[9] Fang, H., Wang, X., Zhao, N. and Al-Dhahir, N., **2021**. Lightweight continuous authentication via intelligently

arranged pseudo-random access in 5G-and-beyond. IEEE Transactions on Communications, 69(6), pp.4011-4023.

[10] Zong, Y., Liu, S., Liu, X., Gao, S., Dai, X. and Gao, Z., **2022.** Robust synchronized data acquisition for biometric authentication. IEEE Transactions on Industrial Informatics, 18(12), pp.9072-9082.

[11] Gong, S., El Azzaoui, A., Cha, J. and Park, J.H., **2020**. Secure secondary authentication framework for efficient mutual authentication on a 5G data network. Applied Sciences, 10(2), p.727.

[12] Jain, J.K., **2019.** Secure and energy-efficient route adjustment model for internet of things. Wireless Personal Communications, 108, pp.633-657.

[13] Haseeb, K., Almogren, A., Ud Din, I., Islam, N. and Altameem, A., **2020.** SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things. Sensors, 20(9), p.2468.

[14] Salman, E.H., Taher, M.A., Hammadi, Y.I., Mahmood, O.A., Muthanna, A. and Koucheryavy, A., **2022.** An anomaly intrusion detection for high-density internet of things wireless communication network based deep learning algorithms. Sensors, 23(1), p.206.

[15] Ruan, N., Li, M. and Li, J., **2017.** A novel broadcast authentication protocol for internet of vehicles. Peer-to-Peer Networking and Applications, 10, pp.1331-1343

[16] Nath, H.J. and Choudhury, H., **2022**. A privacy-preserving mutual authentication scheme for group communication in VANET. Computer Communications, 192, pp.357-372.

[17] Dhanasekaran, S., Ramalingam, S., Baskaran, K. and Vivek Karthick, P., **2024.** Efficient distance and connectivity-based traffic density stable routing protocol for vehicular Ad Hoc networks. IETE Journal of Research, 70(2), pp.1150-1166.

[18] Chen, Z., Ao, J., Luo, W., Cheng, Z., Liu, Y., Sheng, K. and Chen, L., **2022.** A dual-factor access authentication scheme for IoT terminal in 5G environments with network slice selection. Journal of Information Security and Applications, 68, p.103247.

[19] Gope, P., Millwood, O. and Sikdar, B., **2021.** A scalable protocol level approach to prevent machine learning attacks on physically unclonable function-based authentication mechanisms for Internet of Medical Things. IEEE Transactions on Industrial Informatics, 18(3), pp.1971-1980.

[20] Cao, J., Ma, M., Fu, Y., Li, H. and Zhang, Y., **2019.** CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets. IEEE transactions on dependable and secure computing, 18(3), pp.1182-1195.