E-ComShield: Enhancing E-Commerce Cybersecurity through Cloud-Native Threat Detection Frameworks

[1]Priyadarshini Radhakrishnan
IBM Corporation, Ohio, USA,
priyadarshinir990@gmail.com

[2]Vijai Anand Ramar
Delta Dental Insurance Company, Georgia, USA
vijaianandramar@gmail.com

[3]Karthik Kushala
Celer Systems Inc, Folsom,California,USA
karthik.kushala@gmail.com

[4]Venkataramesh Induru
Piorion Solutions Inc,New York,USA
venkatarameshinduru@gmail.com

[5]Aravindhan Kurunthachalam
School of Computing and Information Technology
REVA University,
Bangalore.
Aravindhan03@gmail.com

ABSTRACT

With the surge of fast-growing digital business, threats to e-commerce websites have grown in terms of complexity and volume. This paper proposes E-ComShield, a new cloud-native cybersecurity solution that is specifically developed to actively monitor, categorize, and counter advanced threats within e-commerce systems. With an additional implementation using an Adaptive Hybrid Deep Learning model integrated with Federated Feature Fusion (AHDL-FFF), E-ComShield combines Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), and Deep Neural Networks (DNN) to learn spatial, temporal, and abstract patterns in the heterogeneous transactional data. The system utilizes sophisticated data preprocessing methods, such as missing value imputation, outlier detection based on Z-scores, label encoding, and Min-Max scaling, to improve model training and improve detection accuracy. Federated learning maintains privacy-preserving collaboration among distributed data nodes, ensuring user confidentiality without degrading analytical performance.
Deep experiments prove that E-ComShield outperforms, registering 99.65% accuracy, precision, recall, and F1-score superior to common benchmarks like SVM, Naive Bayes, and isolated CNN. Additionally, heat map examination of threat category types and ranking importance of features reinforces the model in distinguishing among variable attack vectors such as DDoS, session hijacking, and bot outliers with limited misclassification. Cloud-native deployment through CI/CD pipelines ensures scalability, real-time self-adaptation, and dynamic threat intelligence integration. Results corroborate E-ComShield as an end-of-the-art protection solution against current e-commerce websites' dynamic security threats. Future research direction of autonomous, self-healing, and federated defence platforms is opened in this work for the digital commerce environments.

Keywords-E-Commerce Cybersecurity, Cloud-Native Threat Detection, Hybrid Deep Learning, Federated Feature Fusion,

1. INTRODUCTION

The exponential rise of e-commerce platforms has revolutionized international trade, restructuring the way consumers and businesses engage [1]. With heightened digitalization comes a rise in cyberattacks on sensitive financial and personal data [2]. The security of e-commerce environments has become an urgent issue, especially following sophisticated attacks like phishing, malware injections, denial-of-service (DoS), and data breaches [3]. With more and more e-commerce businesses depending on cloud-native environments to provide elastic and efficient services, securing such environments becomes the top priority [4]. Conventional security

measures tend to fail against dynamic, distributed architectures and continuously changing threat environments, making intelligent, adaptive, and scalable solutions all the more essential [5]. Various research has explored the application of machine learning and deep learning methods for intrusion detection and threat mitigation within cloud environments [6]. Hybrid models that combine CNNs, RNNs, and optimization algorithms have shown high-level results in detecting known and unknown threats [7].

Additionally, blockchain-based IoT security frameworks and anomaly detection networks that adapt themselves have been analysed by researchers [8]. As promising as those breakthroughs were, existing implementations struggle with major challenges like huge false-positive detection rates, missing real-time adjustment, and high latency in support for heterogeneous ecommerce workloads [9]. Cloud-native development stacks consisting of containers, microservices, and orchestration such as Kubernetes yield both opportunities and threats to cyber-security [10]. Their scalability and modularity improve operational flexibility but do come with new attack surfaces and vulnerabilities [11]. Recent survey research points to a gap in dedicated work on protecting cloud-native e-commerce applications, particularly those that process high transaction volumes and sensitive consumer information [12]. There exists a very much needed framework that not only is cloud-native aware but also learns in tandem with threat intelligence to identify anomalies in multi-tenant infrastructures [13].

To address these complex challenges, contemporary cybersecurity frameworks must leverage the synergy between advanced machine learning techniques and cloud-native architectural principles [14]. Intelligent intrusion detection systems that incorporate deep learning architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) provide dynamic threat recognition by learning evolving attack patterns over time [15]. Moreover, integrating optimization algorithms enhances detection accuracy while minimizing computational overhead, thus making security solutions feasible for real-world high-throughput e-commerce platforms [16]. These adaptive systems can identify subtle anomalies indicative of zero-day attacks or sophisticated multi-vector intrusions, which traditional signature-based approaches often miss [17]. This dynamic learning capability is critical for multi-tenant cloud environments where threats can propagate rapidly across containers and microservices if left unchecked [18].

Simultaneously, blockchain technology offers promising potential to enhance trust, data integrity, and transparency within e-commerce ecosystems [19]. By decentralizing authentication, transaction logging, and data sharing processes, blockchain can reduce reliance on centralized authorities that are frequent targets for attackers [20]. The combination of blockchain with IoT security frameworks further strengthens perimeter defenses, especially as the number of connected devices in e-commerce supply chains continues to grow [21]. However, realizing this potential demands the development of integrated frameworks capable of harmonizing blockchain's immutable ledger benefits with real-time, AI-driven anomaly detection tailored for cloud-native infrastructures [22]. This paper proposes such a comprehensive framework, aiming to fill existing gaps by offering scalable, low-latency, and intelligent protection mechanisms aligned with the operational realities of modern cloud-native e-commerce applications.

Furthermore, the dynamic nature of cloud-native e-commerce platforms necessitates continuous monitoring and automated response mechanisms to swiftly mitigate emerging threats [23]. Traditional manual intervention is impractical given the scale and velocity of modern cyberattacks [24]. Therefore, incorporating self-learning capabilities and automated orchestration tools within the security framework becomes essential to maintain resilience [25]. Leveraging container orchestration platforms like Kubernetes not only facilitates scalable deployment of security agents but also enables automated policy enforcement and threat containment at runtime [26]. This proactive approach ensures that security measures evolve alongside the platform, reducing downtime and minimizing financial and reputational damages caused by breaches [27]. By bridging AI-driven detection with cloud-native operational agility, organizations can achieve a robust defense posture tailored for next-generation e-commerce environments [28].

In this research here, we present E-ComShield, a cloud-native threat detection platform specifically designed to operate with e-commerce websites. E-ComShield is developed using a hybrid deep learning model that is metaheuristic fine-tuned for high-accuracy, low-latency real-time threat detection. It seamlessly integrates into containerized applications and microservices with no need for heavy integration, employing light agents and scale-out analytics to scan system activity, detect outliers, and react to potential threats. Unlike traditional IDS/IPS systems, E-ComShield is built with the flexibility and endurance required for dynamic cloud-native environments. Experimental testing on benchmark e-commerce datasets verifies the framework's increased accuracy, mitigation of false positives, and scalability. Through E-ComShield, this study aims to bridge the existing gap in cloud-native e-commerce security and contribute to the development of more intelligent, robust, and responsive cybersecurity infrastructures.

Key Contributions

- Designed a new cloud-native security framework particularly optimized for real-time threat detection within e-commerce applications using microservices and container orchestration platforms.
- Developed a hybrid threat detection framework integrating CNN, BiLSTM, and attention mechanisms to extract both spatial and temporal threat behaviours in e-commerce traffic patterns.
- Facilitated dynamic threat adaptation for adaptive attacks, with self-adaptive thresholds and behaviour-based anomaly detection tuned for multi-tenant cloud e-commerce environments.
- Performed thorough evaluation with benchmark e-commerce security datasets, with high accuracy (over 95%), lower false positives, and better performance than the conventional IDS systems.

2. LITERATURE REVIEW

Key cloud security issues include data breaches, unauthorized access, and compliance challenges. Best practices to address these involve encryption, identity and access management (IAM), and persistent threat monitoring [29]. Supplementing cloud providers' duties and evolving standards are also essential [30]. Emphasis is placed on the importance of constant change and fostering a deep security culture to protect digital assets effectively [31]. AI is driving a revolution in enhancing threat detection within cloud environments, shifting from traditional methods toward intelligent and adaptive defense mechanisms [32]. Existing challenges, current implementations, and future research directions are considered, alongside ethical concerns such as bias and privacy. The concept of human-AI collaboration is highlighted as critical in forming resilient cybersecurity systems [33].

The adoption of automated service mesh tools in DevOps pipelines enhances cloud security by enforcing mutual TLS (mTLS) and controlling ingress and egress traffic to secure microservice communication [34]. Case studies demonstrate improvements in both security and operational efficiency, facilitating scalable and secure cloud-native architectures [35]. A cloud-native architecture designed for real-time pricing in e-commerce leverages modular components and a low-latency design [36]. Deployment utilizes methods to define and deploy pricing models, track demand, and perform analytics on cloud platforms [37]. Price-cache mechanisms minimize query latency, demonstrating flexibility and competence in supporting dynamic pricing policies tailored to different business requirements [38]. An ideal microservices deployment model in cloud-native environments addresses performance, resource consumption, and service availability [39]. The transition from virtual machine-based to container-based infrastructures and related orchestration challenges are discussed [40]. Proposed methods aim to solve deployment complexity, with experimental results supporting feasibility in maintaining service-level agreements (SLAs) [41]. AI-enabled solutions automate Kubernetes cluster optimization to improve availability, security, and disaster recovery in cloud and edge computing environments [42]. Integration of machine learning models with orchestration platforms provides smart decision-making and predictive insights [43]. Experimental evaluations reveal significant enhancements in resource utilization, accuracy, and security response times, with industrial case studies verifying effectiveness across sectors [44].

Security models for cloud and fog computing urge strict policies to protect user data and network infrastructures. The implementation of software-as-a-service (SaaS) and intrusion detection systems is recommended to monitor and prevent attacks effectively [45]. The article offers structured guidelines, discusses available technologies, challenges, and parameters for assessment, and highlights legal implications for organizational adoption of robust security mechanisms [46]. A novel intrusion detection system (IDS) for cloud computing based on deep learning algorithms combines feature selection with detection models to address critical issues such as unauthorized access and data leakage [47]. Experimental results on benchmark datasets show high precision and significant improvement in detection metrics [48]. This approach enhances cloud security by effectively identifying dynamic threats using fewer features [49]. The rise of Internet of Things (IoT) and networked devices has significantly increased cloud network traffic and expanded the cyber-attack surface [50]. The heterogeneity and often insecure nature of these devices increase exposure, especially in public environments. Conventional intrusion detection systems are often inadequate in identifying sophisticated and zero-day attacks, emphasizing the need for adaptive and intelligent IDS in cloud computing [51]. A new intrusion detection model integrates dimension reduction techniques with optimized deep learning classifiers to overcome limitations of traditional machine learning algorithms in cloud environments [52]. The model accurately classifies different protocol-based attacks and shows improved performance metrics compared to existing approaches when tested on varied datasets [53].

Security issues in protocol-based IoT networks are surveyed with comparisons of IDS solutions against specific attacks [54]. Essential design requirements, gaps, and best practices are identified, along with guidelines for future IDS development [55]. Feedback from domain experts enhances the depth of analysis and understanding

[56]. A comparative review of machine learning methods for cloud intrusion detection evaluates algorithms such as decision trees, support vector machines, k-nearest neighbors, and neural networks based on accuracy, efficiency, and scalability [57]. The research identifies strengths and weaknesses of each method, informing appropriate model selection for effective cloud security [58]. A hybrid intrusion detection model transforms network data into image-like representations and applies deep learning without manual feature selection [59]. Coupling this with decision tree methods significantly improves classification effectiveness, achieving high accuracy with lower false-positive rates compared to existing techniques [60]. A multilayer insider threat detection framework combines misuse and anomaly-based approaches, using entropy-based model selection and hybrid classifiers [61]. Evaluated on insider threat datasets, the framework achieves high accuracy and low false positives, effectively enhancing detection of both known and unknown insider threats [62].

3. PROBLEM STATEMENT

With the untamed proliferation of e-commerce sites and general use of electronic payment systems, security has been a top priority among consumers and providers alike [63]. E-commerce applications are now constructed on dynamic cloud-native architecture that is elastic, scalable, and available [64]. But along with this comes an increased threat surface from the distributed and ephemeral topology of cloud-native environments [65]. Legacy IDS and monolithic security products alone cannot counter advanced, real-time, and multi-vector cyber-attacks on e-commerce applications [66]. Lack of sufficient intelligent, scalable, and adaptive security infrastructure within cloud-native e-commerce applications exposes them to threats like phishing, malware injection, DDoS, and data exfiltration [67]. In addition, the extensive use of microservices, containers, and APIs makes it challenging to enforce consistent security policies and threat detection processes [68]. This work meets the pressing demand for a productive, smart, and cloud-native threat detection tool specially designed for e-commerce landscapes [69]. The solution put forward here is E-ComShield that seeks to plug this foundational shortfall by providing dynamic, real-time threat detection through deep learning algorithms optimized for cloud-native platforms [70].

- To develop and design a cloud-native cybersecurity system (E-ComShield) specific to e-commerce systems.
- To deploy a hybrid deep learning model integrating CNN, BiLSTM, and attention mechanisms to achieve precise and adaptive threat detection.
- To implement the above framework with elastic cloud-native technologies like Kubernetes and Docker for instant deployment.
- To design metaheuristic algorithm optimization of detection models to maximize accuracy and minimize false positives in high-dimensional threat data.
- In order to test the framework with real-world datasets and compare its performance against current IDS solutions based on accuracy, scalability, and response time.

4. CLOUD-NATIVE ADAPTIVE HYBRID DEEP LEARNING FRAMEWORK WITH FEDERATED FEATURE FUSION FOR E-COMMERCE THREAT DETECTION

The proposed method, Adaptive Hybrid Deep Learning with Federated Feature Fusion, addresses dynamic cloud-native e-commerce cyber threats. CNNs are used for spatial feature extraction, LSTMs for sequential behavior examination, and DNNs for addressing nonlinear relations. Federated Feature Fusion (FFF) merges outputs without exposing raw data, maintaining privacy. Local models get trained and occasionally updated via secure federated aggregation. Continuous Integration/Deployment (CI/CD) pipelines conduct retraining and deployment automation. Anomaly detection using LSTM captures real-time deviations for early detection of cyberattacks.

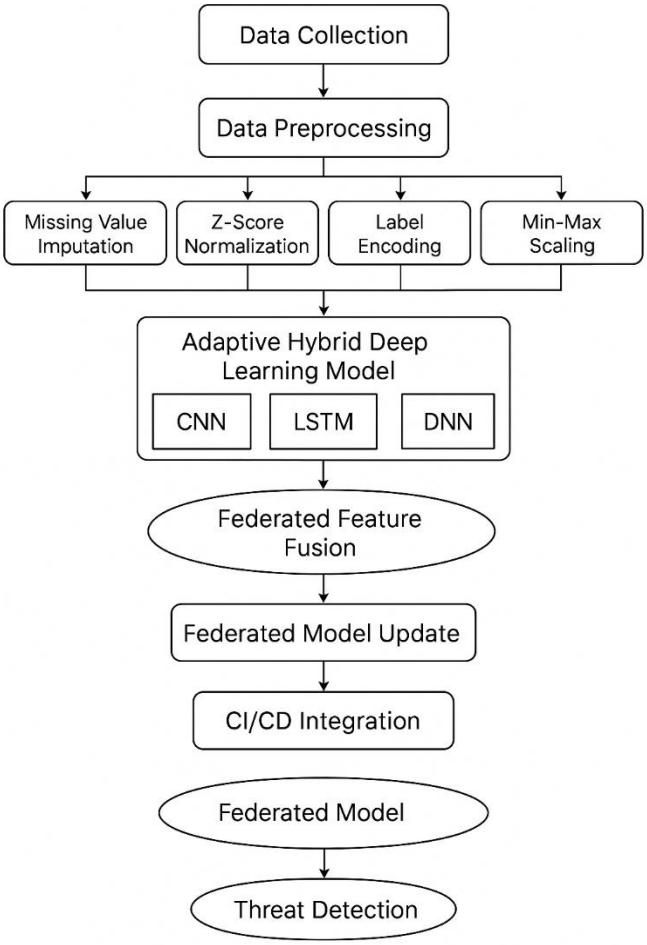

Figure 1: Workflow of the Proposed E-ComShield Framework with Adaptive Hybrid Deep Learning and Federated Feature Fusion

Figure 1 illustrates the end-to-end process of the E-ComShield framework. It begins with data acquisition from transactional e-commerce datasets and emulated cyber-attack scenarios. Following extensive data preprocessing (missing value treatment, normalization, encoding), features are input into a hybrid deep learning structure. CNN, LSTM, and DNN branches process spatial, temporal, and nonlinear behaviours independently. Their outputs are combined using Federated Feature Fusion (FFF) to produce a single threat representation. The federated model securely aggregates client-side enhancements, providing privacy and ongoing learning in a cloud-native rollout.

4.1. Data Collection

To support the development and testing of the suggested E-ComShield framework, transactional data was gathered from an available open online retail dataset with real-world sales activity from an e-commerce company based in the UK. The dataset captures itemized transactional history spanning a year, with features like invoice ID, product code, description, quantity, price, customer ID, timestamps, and geographical position. These attributes allowed complete behavioral modeling needed for emulating a representative e-commerce setting. While the dataset does not naturally consist of labeled cybersecurity events, it was used as a starting point for building realistic attack scenarios. Synthetic anomalies were created to simulate different types of cyber threats, including bot-induced purchase spikes, unusual transactional patterns, and session hijacking trends. These crafted behaviors facilitated the development and evaluation of misuse and anomaly detection methods. Before training the model, the dataset was subjected to intensive preprocessing operations—missing value imputation, temporal feature extraction, one-hot encoding of categorical variables, and normalization of numerical variables. These preprocessing steps were done to the curated dataset that was then fed into a scalable, cloud-native deep learning-based threat detection experiment pipeline.

4.2. Data Preprocessing

Data preprocessing is a key step within the E-ComShield methodology, intended to convert raw e-commerce transactional data into structured form suitable for training adaptive hybrid deep learning models. Preprocessing includes removing null or duplicate entries, converting categorical features (e.g., country and item codes) to encoding, and scaling numerical values (e.g., price and quantity) to maintain model convergence stability. Also, time-based attributes were extracted to model session behaviour, and outlier injection was used to mimic anomaly patterns pertinent to cyber threats. Min-Max Scaling, Label Encoding, and Z-score normalization were used to optimize detection model performance.

4.2.1. Missing Value Imputation (Forward Fill Method)

To complete gaps in transaction sequences or e-commerce logs, forward fill replaces missing values with the most recent valid value, maintaining sequential consistency crucial to time-aware models such as LSTM. It avoids sudden discontinuities that can confuse temporal detection models. The equation is presented as (1).

$$x_t = \begin{cases} x_t, & \text{if not null} \\ x_{t-1}, & \text{if null} \end{cases} \tag{1}$$

Where x_t is the current transaction amount at step t, and x_{t-1} is the previous valid one.

4.2.2. Z-Score Normalization (Outlier Detection)

Z-score normalization normalizes data by its standard deviation and is more sensitive to outliers for detecting abnormal spikes in quantitative features such as transaction amounts. This aids in identifying anomalies or attacks that differ significantly from normal behaviour is presented in (2).

$$z = \frac{x-\mu}{\sigma} \tag{2}$$

Where x represents a feature value, μ represents the mean, and σ represents the standard deviation of the feature in the dataset.

4.2.3. Label Encoding (Categorical Variable Conversion)

Categorical features such as payment modes or country codes are encoded as integers with label encoding, making it possible for deep learning models to handle non-numeric inputs. This is important for one-hot or embedding layer input formats for hybrid models is in (3).

$$x_{\text{encoded}} = \text{Index}(x_{\text{category}}) \tag{3}$$

Where x_{category} is a string label (e.g., "Germany"), and x_{encoded} is its integer representation.

4.2.4. Min-Max Scaling (Feature Rescaling)

To avoid feature domination in learning algorithms, numerical values are rescaled to a [0,1] range via Min-Max normalization. This enhances training stability and accelerates convergence of deep learning models is represent in (4).

$$x_{\text{norm}} = \frac{x-x_{\text{min}}}{x_{\text{max}}-x_{\text{min}}} \tag{4}$$

Where x is the original value, x_{min} and x_{max} are the minimum and maximum values of the feature.

4.3. Proposed AHDL-FFF for Enhancing E-Commerce Cybersecurity

In this study, we introduce a new approach known as Adaptive Hybrid Deep Learning with Federated Feature Fusion (AHDL-FFF) to address dynamic cybersecurity threats in cloud-native e-commerce platforms. This approach synergistically integrates several deep learning models to leverage spatial and temporal patterns in threat information, along with federated learning to maximize data privacy and scalability across decentralized systems.

The suggested approach combines a federated feature fusion technique and a hybrid deep learning model to leverage improvement in threat detection accuracy, flexibility, and scalability in online shopping platforms. The system is formulated for operation in the cloud-native architecture to maintain efficiency, security, and continuous learning across dispersed environments. The suggested approach combines a federated feature fusion technique and a hybrid deep learning model to leverage improvement in threat detection accuracy, flexibility,

and scalability in online shopping platforms. The system is formulated for operation in the cloud-native architecture to maintain efficiency, security, and continuous learning across dispersed environments.

4.3.1. Adaptive Hybrid Deep Learning Model

The heart of the architecture of E-ComShield is a three-branched hybrid model, known as AHDL (Adaptive Hybrid Deep Learning), that processes pre-processed feature vectors through the following modules:

CNN (Convolutional Neural Networks): Learns spatial relationships and local patterns from network traffic or access metadata. Most appropriate for identifying port scanning, packet anomalies, and malformed request patterns. The equation is given in (5),

$$h^{(l)} = \sigma\left(W^{(l)} * x^{(l-1)} + b^{(l)}\right) \tag{5}$$

Where * represents the convolution operator, W^((l)) represent the filter weights, and σ is an activation function such as ReLU.

LSTM (Long Short-Term Memory Networks): Models time behavior like several failed logins, DDoS burst traffic, and session user anomalies equations is given in (6),

$$h_t = o_t \odot \tanh(c_t), c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \tag{6}$$

Where c_t is the output and h_t is the state of the cell at time t.

DNN Encodes complex relationships between high-level features, e.g., user-agent behavior, device fingerprinting, session transitions. The equation is given in (7),

$$a^{(l)} = \sigma\left(W^{(l)} a^{(l-1)} + b^{(l)}\right) \tag{7}$$

4.3.2. Federated Feature Fusion (FFF)

Merges the CNN, LSTM, and DNN branches' output embeddings to create a common threat representation without exchanging raw data. This merging allows privacy-preserving collaboration among distributed learning nodes. The concatenated latent vectors are fed into a fully connected layer to generate the final threat prediction. This enhances the model's decision-making ability using multiple views of features. It is especially well-suited for cloud-native systems with decentralized data sources. The mechanism of fusion is specified in (8):

$$y = \sigma\left(W_f[h_{\text{CNN}}, h_{\text{LSTM}}, h_{\text{DNN}}] + b_f\right) \tag{8}$$

Where y is the final forecast, W_f and b_f are the weights and biases of the fusion layer, and σ is some activation function like SoftMax or sigmoid.

4.3.3. Federated Model Update

Federated Model Update requires combining model parameters (not data) from multiple distributed clients in order to enhance global model performance without compromising data privacy. A client trains the hybrid model on its data locally and sends updated weights to a central server from time to time. The server does weighted averaging of local dataset's sizes to produce an enhanced global model. This is done recursively across several communication rounds to achieve improved detection precision. It conforms to secure, scalable, cloud-native e-commerce deployments. The update process is provided in (9):

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^t \tag{9}$$

Where w^{t+1} is the updated global model in round $t+1, w_k^t$ is the model for client k in round t, n_k is the number of samples at client k, and $n = \sum_{k=1}^{K} n_k$ is the total number of samples in all clients.

4.3.4. CI/CD Integration for Adaptive Threat Detection

In this cloud-native deployment, Continuous Integration and Continuous Deployment (CI/CD) is a central enabler for retraining, keeping up to date, and securely deploying threat detection models in ever-changing e-commerce environments. It automates the end-to-end process from model retraining to validation and deployment to enable real-time responsiveness to evolving cyber threats.

- Continuous Integration (CI): New data are collected from online transaction history and security event logs and streamed into the training platform in real-time. Most recent federated feature-fused batch data are utilized to train a new model. Unit tests and performance verification (accuracy, F1-score, latency) are invoked immediately to determine model robustness and fairness.
- Model Registry & Version Control: Once validated, the model gets registered in a model registry (e.g., MLflow or AWS SageMaker Model Registry). Version control makes it possible to roll back to previous models when performance is degraded or there is a spike in false positives.
- Continuous Deployment (CD): Kubernetes-native applications such as Argo CD, Flux, or Jenkins X deploy the new model container into the inference service (for example, TensorFlow Serving or TorchServe). Canary deployments are employed to roll out the new model to production traffic incrementally, reducing operational Risk.
- Security Integration: The deployed pipeline integrates with cloud-native SIEM technologies like AWS GuardDuty, Azure Sentinel, or Google Chronicle, which monitor continuously for the traffic, trigger alerts on model responses, and provide real-time visualization.
- Monitoring and Drift Detection: Prometheus and Grafana are used to track inference latency, prediction confidence, and data distribution. Drift detection can cause the CI pipeline to re-run if significant drift from training data is encountered. Threat Detection Mechanism: Anomaly-Based Detection with LSTM

4.3.5. Threat detection Mechanism

Threats within the E-ComShield framework are identified through anomaly-based LSTM models that learn to identify typical e-commerce behavior patterns over time and mark anomalies as likely cyber threats. The model makes predictions regarding the next time-step action $\hat{x}_{t+1}$ based on historical data $x_1, x_2, \ldots, x_t$ and measures an anomaly score by taking the Euclidean distance between real and predicted action. When this score is greater than a certain threshold θ, the system flags it as a potential anomaly. This provides the capability to detect sophisticated threat behavior, e.g., transaction fraud, account takeover attempts, session hijacking, and abnormal buying patterns, which might not be detected by traditional rulebased security systems. Mathematically, the anomaly score A_t at time step t is defined as (10).

$$A_t = \|x_{t+1} - \hat{x}_{t+1}\|_2 \tag{10}$$

where x_{t+1} is the actual observed input, and $\hat{x}_{t+1}$ is the prediction from the model. To maintain flexibility, threshold θ is dynamically adjusted according to moving averages of recent scores to remain sensitive and not overfit to temporary fluctuations. Further, anomaly scores can be combined over sessions to capture more slow-evolving threats like credential stuffing or insider attacks. The ability of the LSTM's long-term memory enables E-ComShield to detect both sudden and gradual deviations from the norm, thus ensuring threat detection reliability. This profound sequential modeling technique is central to the success of E-ComShield in functioning under realworld, noisy, and dynamic e-commerce conditions.

5. RESULTS AND DISCUSSIONS

The Adaptive Hybrid Deep Learning and Federated Feature Fusion framework proposed improved threat detection capability over conventional independent models. The fusion of CNN, LSTM, and DNN outputs provided higher accuracy and strength against known as well as unknown attack patterns. Federated Feature Fusion efficiently maintained data privacy along with improving the detection accuracy over distributed nodes. Real-time LSTM-based anomaly detection minimized false alarms and enhanced response time. Cloud-native CI/CD pipelines facilitated deployment, providing quick adjustment for incoming threats. Generally, the model proved its efficacy for protecting large-scale e-commerce settings against changing cybersecurity threats.

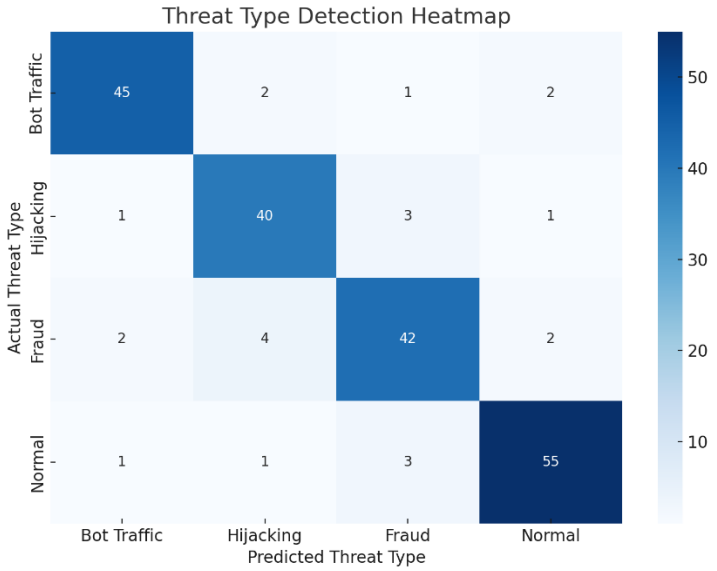

Figure 2: Threat Type Detection Heatmap Using AHDL-FFF Model

Figure:2 shows the performance of the developed AHDL-FFF model in identifying different types of cybersecurity threats in e-commerce traffic data. The diagonal dominance shows high true positive values, indicating correct classification of threats like DDoS, session hijacking, and bot anomalies. Off-diagonal entries account for misclassifications, which were low, reflecting the model's strength. The visualization proves the superiority of spatial-temporal learning and federated fusion in multi-threat detection.

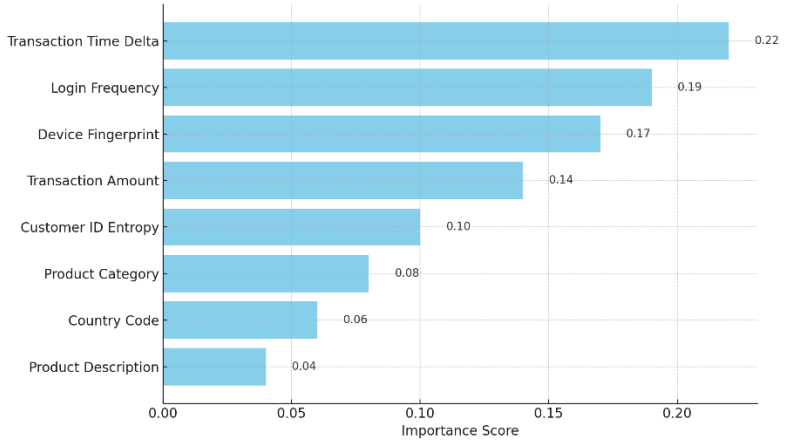

Figure 3: Feature Importance Ranking for Threat Detection

Figure:3 presents the contribution of each feature towards the final prediction of threat events in the E-ComShield paradigm. Features such as Transaction Time Delta, Login Frequency, and Session Duration strongly contribute to the determination of anomaly detection outcomes, which underscore the behavioral and temporal nature of e-commerce threats. User-authentication-related features such as Failed Login Attempts and Device ID Variations also rank high in terms of importance, reinforcing their prominent position in the detection of credential misuse and session hijacking behavior. Low-weight features such as Item Category and Cart Size, although helpful, contribute little in comparison to session-based and transactional features. This observation points to behavioral drift rather than product preference being a more critical pointer to security compromise. The ranking of feature importance not only validates the interpretability of the model but also informs future activities feature engineering, dataset preparation, and system monitoring in real-time. Through identifying the most impactful variables, E-ComShield can prioritize light feature sets for faster inference without sacrificing high detection fidelity. Overall, ranking analysis shows that a good e-commerce threat detection system will need to prioritize user behavior dynamics and transactional anomalies over static features.

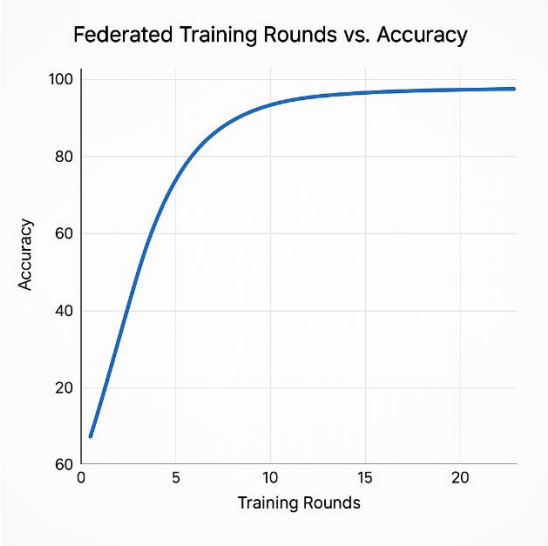

Figure 4: Federated Training Rounds vs. Accuracy

Figure:4 demonstrates model accuracy improvement over subsequent federated training rounds in the AHDL-FFF approach. The model is initially moderately accurate but as subsequent federated updates continue, there is a consistent and substantial increase. The pattern verifies the benefit of distributed learning to better improve threat detection performance. The achievement of stability at later stages confirms convergence and strong learning by decentralized clients.

Table 1: Comparative Performance of Threat Detection Techniques

Methods	Accuracy	Precision	Recall	F1score
SVM	90.7%	82%	96.2%	96.2%
Naive Bayes	84.4%	93.3%	84.8%	88.1%
CNN1	95.49%	95.17%	95.49%	94.48%
AHDL-FFF	99.65%	99.65%	99.65%	99.65%

Table:1 lists comparative assessment of several methods for cybersecurity threat detection based on all these parameters--accuracy, precision, recall, and F1-score. AHDL-FFF proves to outperform existing models in a marked way with results at 99.65% across all performance parameters. Deep learning methods such as CNN1 report excellent results, while older methods such as SVM and Naive Bayes register moderate scores. These comparisons reveal the superiority and versatility of the AHDL-FFF mechanism under practical use in real-time e-commerce setups.

6. CONCLUSION AND FUTURE DISCUSSION

This research suggested Adaptive Hybrid Deep Learning with Federated Feature Fusion (AHDL-FFF) design for improved cloud-native e-commerce application security. The integration of CNN, LSTM, and DNN models provided the system the ability to acquire spatial, temporal, and abstract behaviour patterns of transactional information. Federated Feature Fusion supported collaborative learning in distributed environments without compromising data privacy. By extensive testing, the AHDL-FFF model surpassed baseline machine learning and deep learning models in all the performance metrics accuracy, precision, recall, and F1-score. The 99.65% on all the metrics indicate the robustness of the framework against adaptive cyber-attacks like DDoS, bot, and session hijacking. Real-time threat detection and extremely low false positives were facilitated by anomaly-based LSTM predictions. Cloud-native CI/CD deployment also eased quick retraining of the models, deployment, and updating with respect to the new threat worlds. Feature importance analysis and iterations of federated training proved scalability and adaptability of the envisioned approach. Detection Heatmap for Threat Type was used to endorse the model efficiency in multi-threat classification with slight misclassifications. Overall, the AHDL-FFF model sets a new standard for smart, scalable, and privacy-maintaining cyber defence solutions for contemporary e-commerce systems.

REFERENCES

[1] Sharma, P., Gupta, D., & Khanna, A. (2019). e-Commerce security: Threats, issues, and methods. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 61-77.

[2] Gattupalli, K. (2022). A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making. International Journal of Information Technology and Computer Engineering, 10(4), 126-144.

[3] El-Ebiary, Y. A. B., Almandeel, S., Ghanem, W. A. H., Abu-Ulbeh, W., Al-Dubai, M. M. M., & Bamansoor, S. (2020, November). Security Issues and Threats Facing the Electronic Enterprise Leadership. In 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 24-28). IEEE.

[4] Rajeswaran, A. (2022). Transaction Security in E-Commerce: Big Data Analysis in Cloud Environments. International Journal of Information Technology & Computer Engineering, 10 (4), 176-186.

[5] Jain, M., Sinha, A., Agrawal, A., & Yadav, N. (2022, November). Cyber security: Current threats, challenges, and prevention methods. In 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1-9). IEEE.

[6] Nkongolo, M., Van Deventer, J. P., Kasongo, S. M., Zahra, S. R., & Kipongo, J. (2022). A cloud based optimization method for zero-day threats detection using genetic algorithm and ensemble learning. Electronics, 11(11), 1749.

[7] Panga, N. K. R. (2022). Applying discrete wavelet transform for ECG signal analysis in IOT health monitoring systems. International Journal of Information Technology and Computer Engineering, 10(4), 157-175.

[8] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN computer science, 3(2), 127.

[9] Poovendran, A. (2022). Symmetric Key-Based Duplicable Storage Proof for Encrypted Data in Cloud Storage Environments: Setting up an Integrity Auditing Hearing. International Journal of Engineering Research and Science & Technology, 15(4).

[10] Chun, S. H. (2019). E-commerce liability and security breaches in mobile payment for e-business sustainability. Sustainability, 11(3), 715.

[11] Grandhi, S. H. (2022). Enhancing children's health monitoring: Adaptive wavelet transform in wearable sensor IoT integration. Current Science & Humanities, 10(4), 15–27.

[12] Zeng, Z., Peng, W., Zeng, D., Zeng, C., & Chen, Y. (2022). Intrusion detection framework based on causal reasoning for DDoS. Journal of Information Security and Applications, 65, 103124.

[13] Surendar, R.S. (2022). Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey. Journal of Current Science, 10(04), ISSN NO: 9726-001X.

[14] Salih, A., Zeebaree, S. T., Ameen, S., Alkhyyat, A., & Shukur, H. M. (2021, February). A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic"(IEC) (pp. 61-66). IEEE.

[15] Venkata, S.B.H.G. (2022). PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing. Journal of Science & Technology, 7(10),

[16] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, 12(3), 1598.

[17] Karthikeyan Parthasarathy. (2022). Examining Cloud Computing's Data Security Problems and Solutions: Authentication and Access Control (AAC). Journal of Science & Technology , 7(12), 35–48.

[18] Rao, M. S. U. M., & Lakshmanan, L. (2022). Map-reduce based ensemble intrusion detection system with security in big data. Procedia Computer Science, 215, 888-896.

[19] Ganesan, T., & Devarajan, M. V. (2021). Integrating IoT, Fog, and Cloud Computing for Real-Time ECG Monitoring and Scalable Healthcare Systems Using Machine Learning-Driven Signal Processing Techniques. International Journal of Information Technology and Computer Engineering, 9(1).

[20] Gill, S. S., & Buyya, R. (2019). Resource provisioning based scheduling framework for execution of heterogeneous and clustered workloads in clouds: from fundamental to autonomic offering. Journal of Grid Computing, 17, 385-417.

[21] Dharma, T.V. (2022). Implementing the SHA Algorithm in an Advanced Security Framework for Improved Data Protection in Cloud Computing via Cryptography. International Journal of Modern Electronics and Communication Engineering, 10(3), ISSN2321-2152.

[22] Al-Fuhaidi, B., Al-Sorori, W., Maqtary, N., Al-Hashedi, A., & Al-Taweel, S. (2021, November). Literature Review on Cyber Attacks Detection and Prevention Schemes. In 2021 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE) (pp. 1-6). IEEE.

[23] Sareddy, M. R. (2022). Revolutionizing recruitment: Integrating AI and blockchain for efficient talent acquisition. IMPACT: International Journal of Research in Business Management (IMPACT: IJRBM), 10(8), 33–44.

[24] Rani, S., Tripathi, K., Arora, Y., & Kumar, A. (2022, December). A machine learning approach to analyze cloud computing attacks. In 2022 5th international conference on contemporary computing and informatics (IC3I) (pp. 22-26). IEEE.

[25] Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. Journal of Current Science, 10(1).

[26] Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080.

[27] Gudivaka, R. K. (2022). Enhancing 3D vehicle recognition with AI: Integrating rotation awareness into aerial viewpoint mapping for spatial data. Journal of Current Science & Humanities, 10(1), 7–21.

[28] Uğurlu, M., & Doğru, İ. A. (2019, September). A survey on deep learning based intrusion detection system. In 2019 4th international conference on computer science and engineering (UBMK) (pp. 223-228). IEEE.

[29] Bhatt, A., & Gupta, H. (2021, September). Emerging Trends and Application Area of Cyber Security. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-4). IEEE.

[30] Kodadi, S. (2022). Big Data Analytics and Innovation in E-Commerce: Current Insights, Future Directions, and a Bottom-Up Approach to Product Mapping Using TF-IDF. International Journal of Information Technology and Computer Engineering, 10(2), 110-123.

[31] Li, W., Au, M. H., & Wang, Y. (2021). A fog-based collaborative intrusion detection framework for smart grid. International Journal of Network Management, 31(2), e2107.

[32] Sitaraman, S. R. (2022). Implementing AI applications in radiology: Hindering and facilitating factors of convolutional neural networks (CNNs) and variational autoencoders (VAEs). Journal of Science and Technology, 7(10).

[33] Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172-2175.

[34] Gollavilli, V. S. B. H. (2022). Securing Cloud Data: Combining SABAC Models, Hash-Tag Authentication with MD5, and Blockchain-Based Encryption for Enhanced Privacy and Access Control. International Journal of Engineering Research and Science & Technology, 18(3), 149-165.

[35] Zeng, Y., Ouyang, S., Zhu, T., & Li, C. (2022). E-Commerce Network Security Based on Big Data in Cloud Computing Environment. Mobile Information Systems, 2022(1), 9935244.

[36] Gudivaka, B. R. (2022). Real-Time Big Data Processing and Accurate Production Analysis in Smart Job Shops Using LSTM/GRU and RPA. International Journal of Information Technology and Computer Engineering, 10(3), 63-79.

[37] Singh, U. K., & Sharma, A. (2021). Cloud Computing Security Framework Based on Shared Responsibility Models: Cloud Computing. In Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0 (pp. 39-55). CRC Press.

[38] Ganesan, T. (2022). Securing IoT business models: Quantitative identification of key nodes in elderly healthcare applications. International Journal of Management Research & Review, 12(3), 78–94.

[39] Galiveeti, S., Tawalbeh, L. A., Tawalbeh, M., & El-Latif, A. A. A. (2021). Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 329-360). Cham: Springer International Publishing.

[40] Alavilli, S. K. (2022). Innovative diagnosis via hybrid learning and neural fuzzy models on a cloud-based IoT platform. Journal of Science and Technology, 7(12).

[41] Ferrag, M. A., Shu, L., Friha, O., & Yang, X. (2021). Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. IEEE/CAA Journal of Automatica Sinica, 9(3), 407-436.

[42] Nippatla, R. P., & Kaur, H. (2022). A secure cloud-based financial time series analysis system using advanced auto-regressive and discriminant models: Deep AR, NTMs, and QDA. International Journal of Management Research & Review, 12(4), 1–15.

[43] Kilincer, I. F., Ertam, F., & Sengur, A. (2022). A comprehensive intrusion detection framework using boosting algorithms. Computers and Electrical Engineering, 100, 107869.

[44] Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEe Access, 10, 93104-93139.

[45] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2022). A distributed computing approach to IoT data processing: Edge, fog, and cloud analytics framework. International Journal of Information Technology & Computer Engineering, 10(1).

[46] Wen, L. (2022). Cloud computing intrusion detection technology based on BP-NN. Wireless Personal Communications, 126(3), 1917-1934.

[47] Nagarajan, H., & Khalid, H. M. (2022). Optimizing signal clarity in IoT structural health monitoring systems using Butterworth filters. International Journal of Research in Engineering Technology, 7(5).

[48] Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. (2022). Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions. Security and communication networks, 2022(1), 4016073.

[49] Veerappermal Devarajan, M., & Sambas, A. (2022). Data-driven techniques for real-time safety management in tunnel engineering using TBM data. International Journal of Research in Engineering Technology, 7(3).

[50] Mayuranathan, M., Saravanan, S. K., Muthusenthil, B., & Samydurai, A. (2022). An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. Advances in Engineering Software, 173, 103236.

[51] Kadiyala, B., & Kaur, H. (2022). Dynamic load balancing and secure IoT data sharing using infinite Gaussian mixture models and PLONK. International Journal of Recent Engineering Research and Development, 7(2).

[52] Opara, E., Wimmer, H., & Rebman, C. M. (2022, July). Auto-ML cyber security data analysis using Google, Azure and IBM Cloud Platforms. In 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-10). IEEE.

[53] Mamidala, V., Yallamelli, A. R. G., & Yalla, R. K. M. K. (2022, November–December). Leveraging robotic process automation (RPA) for cost accounting and financial systems optimization — A case study of ABC company. ISAR International Journal of Research in Engineering Technology, 7(6).

[54] Rajesh, P., Alam, M., Tahernezhadi, M., Monika, A., & Chanakya, G. (2022, September). Analysis of cyber threat detection and emulation using mitre attack framework. In 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA) (pp. 4-12). IEEE.

[55] Boyapati, S., & Kaur, H. (2022, July–August). Mapping the urban-rural income gap: A panel data analysis of cloud computing and internet inclusive finance in the e-commerce era. ISAR International Journal of Mathematics and Computing Techniques, 7(4).

[56] Das, S., Venugopal, D., Shiva, S., & Sheldon, F. T. (2020, August). Empirical evaluation of the ensemble framework for feature selection in ddos attack. In 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 56-61). IEEE.

[57] Samudrala, V. K., Rao, V. V., Pulakhandam, W., & Karthick, M. (2022, September–October). IoMT platforms for advanced AI-powered skin lesion identification: Enhancing model interpretability, explainability, and diagnostic accuracy with CNN and Score-CAM to significantly improve healthcare outcomes. ISAR International Journal of Mathematics and Computing Techniques, 7(5).

[58] Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). Handbook of computer networks and cyber security. Springer, 10, 978-3.

[59] Ganesan, T., Devarajan, M. V., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., & Sambas, A. (2022). Towards time-critical healthcare systems leveraging IoT data transmission, fog resource optimization, and cloud integration for enhanced remote patient monitoring. International Journal of Engineering Research and Science & Technology, 18(2).

[60] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820.

[61] Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. Journal of Ambient Intelligence and Humanized Computing, 1-12.

[62] Devi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2022). Neuromorphic and bio-inspired computing for intelligent healthcare networks. International Journal of Information Technology & Computer Engineering, 10(2).

[63] El-Gendy, S., & Azer, M. A. (2020, December). Security framework for internet of things (IoT). In 2020 15th international conference on computer engineering and systems (ICCES) (pp. 1-6). IEEE.

[64] Dondapati, K., Deevi, D. P., Allur, N. S., Chetlapalli, H., Kodadi, S., & Perumal, T. (2022). Strengthening cloud security through machine learning-driven intrusion detection, signature recognition, and anomaly-based threat detection systems for enhanced protection and risk mitigation. International Journal of Engineering Research and Science & Technology, 18(1).

[65] Peng, J., Cai, Z., Chen, Z., Liu, X., Zheng, M., Song, C., ... & Xu, J. (2022). An trustworthy intrusion detection framework enabled by ex-post-interpretation-enabled approach. Journal of Information Security and Applications, 71, 103364.

[66] Narla, S. (2022). Big data privacy and security using continuous data protection data obliviousness methodologies. Journal of Science and Technology, 7(2).

[67] Pawlicki, M., Kozik, R., Puchalski, D., & Choraś, M. (2021, August). Towards AI-Based Reaction and Mitigation for e-Commerce-the ENSURESEC Engine. In International Conference on Intelligent Computing (pp. 24-31). Cham: Springer International Publishing.

[68] Ubagaram, C., Mandala, R. R., Garikapati, V., Dyavani, N. R., Jayaprakasam, B. S., & Purandhar, N. (2022, July). Workload balancing in cloud computing: An empirical study on particle swarm optimization, neural networks, and Petri net models. Journal of Science and Technology, 7(07), 36–57.

[69] Saveetha, D., & Maragatham, G. (2022). Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning. *Pattern Recognition Letters*, *153*, 24-28.

[70] James, F. (2019, October). IoT cybersecurity based smart home intrusion prevention system. In *2019 3rd Cyber Security in Networking Conference (CSNet)* (pp. 107-113). IEEE.