A Novel Hybrid Threat Modeling Framework for IoT Security using STRIDE-DREAD and Machine Learning

Gaurav Thakur, Pradeep Chouksey, Mayank Chopra, Parveen Sadotra, Neha Thakur, Diksha Sharma, Arpit Koundal and Shaina Mahajan

***Abstract*—The rapid growth of Internet of Things (IoT) deployments has increased security risks due to diverse device vulnerabilities, large scale interconnected environments, and the heterogeneity of communication protocols. Traditional threat assessment methods such as STRIDE and DREAD provide a structured foundation for identifying and categorizing security risks, yet they lack automated, real-time detection capabilities required for modern IoT systems that operate in dynamic and resource-constrained environments. To address these limitations, this study presents a hybrid threat modeling framework that integrates machine learning with STRIDE–DREAD to enhance threat identification, prioritization, and quantitative risk analysis. An ML-based classifier is trained on the CIC-BCCC-NRC TabularIoTAttack-2024 dataset to detect and categorize various IoT attack types, with particular emphasis on DDoS variants due to their high prevalence. Ensemble learning techniques are applied to pre-processed network traffic, enabling accurate, scalable, and computationally efficient classification suitable for deployment on lightweight IoT hardware. The proposed system achieves 92.5% detection accuracy, surpassing conventional STRIDE–DREAD assessments by 10–15% while providing enriched decision support for security analysts. Overall, the results demonstrate that integrating ML with established threat modeling methods significantly improves automation, reduces manual evaluation time, and strengthens the precision, adaptability, and operational reliability of IoT security assessment frameworks.**

***Index terms*—IoT Security, Threat Modeling, STRIDE, DREAD, Machine Learning, Risk Assessment.**

I. Introduction

As Internet of Things (IoT) ecosystems expand across industries such as healthcare, smart homes, transportation, and industrial automation, the scale and diversity of connected devices introduce complex security requirements that traditional network security models were not designed to handle. Unlike conventional computing systems, IoT devices often operate with minimal processing power, limited memory, and inconsistent security configurations. These constraints make it difficult to deploy standard defense mechanisms and create an urgent need for automated, intelligent, and scalable threat assessment techniques that can adapt to rapidly evolving attack patterns. The IoT revolutionized manufacturing through the ability to create continuous device-to-cloud connectivity among sensors. The rapid increase of IoT use brings new cybersecurity problems because numerous IoT devices are both under-powered in terms of computing resources and secured inadequately [1].

IoT networks become a common target for cybercriminals because they consist of distributed elements and face weak security vulnerabilities which require robust threat modeling to protect against potential risks [2-3]. The security threat identification and assessment system use traditional frameworks which include STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) as methods for structured threat modeling [4-5]. Manual risk assessment within prevalent frameworks fails to be efficient when used for dynamic environments. The methods show insufficient capability to adapt threats in real time because they struggle with the dynamic changes in IoT systems [6]. A new threat modeling framework integrates structured threat assessment methods STRIDE and DREAD together with machine learning systems for improved predictive functionality. The research establishes an automated system to identify vulnerabilities while assessing security performance and reduces humans in the management process. The proposed framework uses the CIC-BCCC-NRC TabularIoTAttack-2024 dataset to develop and test its methods because it contains multiple attack types such as Denial of Service attacks along with data exfiltration and unauthorized access operations [7].

The key contributions of this work are as follows:

- The adaptation capability of security systems which function through practical thinking resembles human operator behaviour. Through partnership between machine learning technology and STRIDE-DREAD threat detection abilities become more effective. The

Manuscript received October 31, 2025; revised November 24, 2025. Date of publication January 12, 2026. Date of current version January 12, 2026. The associate editor prof. Jelena Čulić Gambiroža has been coordinating the review of this manuscript and approved it for publication.

G. Thakur (corresponding author) is with the Department of Computer Science and Engineering, Central University of Jammu, Bagla (Rahya Suchani), India and with the Department of Computer Science and Informatics, Central University of Himachal Pradesh, Shahpur Parisar, India (e-mail: gauravthakur573@gmail.com).

P. Chouksey, M. Chopra, P. Sadotra, N. Thakur, D. Sharma, A. Koundal and S. Mahajan are with the Department of Computer Science and Informatics, Central University of Himachal Pradesh, Shahpur Parisar, India.

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0236

- system decreases operational workload because it enables technology to conduct risk security evaluations.
- The system utilizes ongoing learning procedures that boost its capabilities after data acquisition. Through machine learning predictions and smart risk scoring approaches the system detects paramount threats. Security guards equipped with high-level intelligence have the capacity to immediately discover critical threats in IoT network systems.
- The system offers continuous threat forecasting which sets it apart from other solutions. The implementation adapts its defensive measures when novel threats emerge which allows it to stop security breaches that endanger the organization. This framework exists to find threats while simultaneously fighting against potential security breaches.

The following sections comprise the paper organization: Section II scrutinizes prior threat modeling frameworks when merged with machine learning approaches in cybersecurity field. A description of the suggested hybrid framework along with its architectural design and procedural elements appears in Section III. The paper explores dataset selection along with preprocessing techniques in Section IV. The subsequent section describes both the implementation stages and training process for the machine learning model. The paper's performance assessment appears in Section VI while Section VII provides conclusions along with proposed future research.

II. Related Work

Threat modeling stands as an essential cybersecurity practice since different systems have developed detection frameworks for threats [8]. Microsoft developed STRIDE that sorts security threats into six threat classes named Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE provides successful threat discovery although it does not help organizations assess threat severity [9-10]. DREAD represents a threat evaluation system that uses Damage Potential and Reproducibility and Exploitability and Affected Users and Discoverability to rate threats [11]. DREAD introduces risk evaluation scoring through manual input therefore different assessments result in divergent risk evaluation outcomes [12]. OCTAVE serves organizations well for risk management activities but it fails to provide real time IoT security detection capabilities [13-14]. Standard security procedures allow us to investigate system issues yet they are ineffective against contemporary automated cyber attacks that change rapidly [15]. Machine learning technologies produce successful results when it comes to improving cybersecurity system security [16]. Network protection against strange behaviour and malware attacks is made achievable through machine learning algorithms built into an intrusion detection infrastructure. Network traffic attacks are correctly identified by Supervised machine learning algorithms Random Forests and Support Vector Machines with high levels of precision [17-18]. The grouping algorithms of clustering and autoencoder in unsupervised learning provide efficient methods to detect previously unknown cyber threats [19].

There seem to be few research studies regarding the integration of machine learning with STRIDE-DREAD threat modeling [20]. The use of ML systems in security does not apply structured approaches to threats because of its impact on their capability to display results during accepted risk assessment processes [21-22]. Recent studies have advanced IoT security using lightweight cryptographic algorithms such as PRESENT, KATAN, and SPECK, which are specifically designed to provide strong encryption while maintaining efficiency in resource-constrained devices [23-24]. PRESENT, KATAN, and SPECK are widely used lightweight cryptographic algorithms designed for resource-constrained environments such as IoT devices. PRESENT is an ultra-lightweight 64-bit block cipher with 80/128-bit key options, built on a substitution–permutation network (SPN) structure optimized for minimal hardware footprint and low power consumption. KATAN is a family of lightweight block ciphers supporting 32-, 48-, and 64-bit block sizes with an 80-bit key, employing simple bitwise operations to achieve efficient hardware implementation in highly constrained embedded systems. SPECK, developed by the NSA, is a lightweight block cipher designed primarily for software efficiency, offering flexible block and key sizes while providing high performance on low power microcontrollers commonly used in IoT deployments. These ciphers address the limitations of traditional algorithms (e.g., AES, RSA) in IoT environments by offering reduced computational overhead and lower energy consumption. In parallel, machine learning driven threat detection models have emerged as a complementary defense mechanism. For instance, recent works leveraging large scale datasets such as CIC-BCCC-NRC-IoT-2023 have reported high classification accuracy for detecting botnets, DDoS, and other IoT-specific attack vectors [25-27]. Such models highlight the promise of intelligent intrusion detection systems (IDS) that adaptively learn from evolving network behaviors. However, despite these advances in cryptography and intelligent IDS, existing research rarely integrates structured threat modeling methodologies with machine learning based classifiers to provide a systematic and explainable defense mechanism. Most works either focus solely on lightweight encryption or on anomaly detection, but lack a unified framework that bridges design time threat modeling with runtime intelligent detection. To the best of our knowledge, no prior work has combined a hybrid STRIDE-DREAD threat modeling approach with machine learning using real world IoT attack datasets, which underscores the novelty and practical significance of our proposed framework.

This research unites STRIDE-DREAD alongside machine learning to create an enhanced flexible platform for modeling Internet of Things security threats.

III. Proposed Hybrid Threat Model

Our hybrid threat modeling process has four major phases which include threat detection, risk measurement, threat classification through machine learning and automatic threat ranking.

A. Threat Identification using STRIDE

Our system starts by placing found threats into STRIDE categories at this initial stage. The proposed method assigns security events to one of six STRIDE categories to better understand attack methods. A DDoS attack would go in the Denial-of-Service category while unauthorized access attempts go into Spoofing and Elevation of Privilege [28].

B. Quantitative Risk Assessment Using DREAD

After putting threats into their proper category's security teams evaluate them using DREAD methodology. Security teams use the DREAD system by giving numerical ratings to each security threat based on these factors [29].

- The assessment shows how badly systems will get affected.
- Attack repeatability indicates how simple it is to perform the attack a second time.
- The level of knowledge or expertise required by an attacker to successfully carry out the unauthorized activity.
- This method of measuring security risk includes examining the number of systems that face potential threats.
- People can locate the vulnerability very easily.

The risk scores help security teams determine which threats to handle first because they show the level of risk in numbers.

C. Machine Learning Based Threat Classification

Our system's main improvement includes adding a machine learning technology to automate finding and labelling security threats. The system teaches a RF algorithm to detect threats in IoT attack data by processing network traffic data alongside attack signatures and risk assessments [30]. By learning to detect threats the model achieves high success rates which replaces the need for manual inspection.

D. Automated Threat Prioritization

At the end stage the framework uses DREAD ratings together with ML-produced severity estimations to create a ranking of security problems. The system marks high-risk security problems for urgent response and adds lower-risk issues to a following evaluation schedule [31]. Automation helps direct resources to the urgent threats first so teams can respond without delays. Our proposal integrates STRIDE-DREAD analysis techniques with the precision of machine learning to develop a better and quicker method to model IoT risks.

IV. Dataset Selection and Preprocessing

Effective machine learning models need training data that offers both high quality and connection to the modelled problem. Our team chose the CIC-BCCC-NRC TabularIoTAttack-2024 dataset produced by the Canadian Institute for Cybersecurity to serve as our research material because this collection contains all major IoT security threats. This dataset serves as the best selection because it provides complete information about current IoT attack methods such as DoS attacks, data exfiltration attempts, device spoofing situations, and other threat types. The dataset includes data for both regular and harmful network events taken from multiple IoT devices which suits perfectly for building an effective threat identification model [31-33], [39-40].

A. Dataset Description

Five labelled CSV files were derived from the dataset:

- DDoS-ACK_Fragmentation9.pcap_Flow.csv
- DDoS-ICMP_Fragmentation4.pcap_Flow.csv
- DDoS-PSHACK_Flood7.pcap_Flow.csv
- DDoS-RSTFINFlood6.pcap_Flow.csv
- Miraiudpplain13.pcap_Flow.csv

Flow ID	Src IP	Src Port	Dst IP	Dst Port	Protocol	Timestamp	Flow Duration
142.251.33.163-192.168.137.235-80-46414-6	142.251.33.163	80	192.168.137.235	46414	6	26/10/2022 01:21:29 PM	582200
192.168.137.207-173.255.124.25-48489-443-6	192.168.137.207	48489	173.255.124.25	443	6	26/10/2022 01:21:29 PM	122570
192.168.137.85-192.168.137.246-52420-55443-6	192.168.137.85	52420	192.168.137.246	55443	6	26/10/2022 01:21:30 PM	143167
192.168.137.104-173.198.192.108-35746-4431-6	192.168.137.104	35746	173.198.192.108	4431	6	26/10/2022 01:21:30 PM	154739
192.168.137.235-142.251.33.163-46414-80-6	192.168.137.235	46414	142.251.33.163	80	6	26/10/2022 01:21:30 PM	3

Fig. 1. Dataset preview after loading and labelling

Each file corresponds to a specific type of DDoS attack and was labelled accordingly. Figure 1 shows a snapshot of the combined dataset after loading multiple labelled .csv files from the CIC-BCCC-NRC-IoT-2023 collection, including attack traffic types such as DDoS-ACK Fragmentation. The dataset contains 86 features per record, including both network flow based attributes and metadata.

Key columns visible in this preview include:

- Flow ID: Unique identifier for each network flow.
- Src IP / Dst IP: Source and destination IP addresses involved in the flow.
- Src Port / Dst Port: Port numbers used for communication.
- Protocol: Numerical value indicating the network protocol used (e.g., TCP, UDP).
- Timestamp: Exact time when the flow was recorded.
- Flow Duration: Duration of the communication flow in microseconds.
- Total Fwd/Bwd Packets: Total number of packets sent forward and backward in the connection.
- Idle/Active Stats: Several statistical measures capturing flow inactivity or activity periods (e.g., Idle Mean, Active Std).

Additional labelling columns include:

- Attack Name: Human-readable description of the attack type.

- Label: Binary indicator (1 = attack, 0 = benign).
- attack_type: Encoded class name for supervised learning.

This table confirms successful data ingestion and preprocessing where multiple attack specific files were merged, standardized, and labelled consistently for training machine learning models. Each row represents a captured network flow that will be fed into the classification pipeline.

While the CIC-BCCC-NRC-IoT-2023 dataset provides a rich and diverse set of IoT traffic traces, it is not without limitations. One key limitation is its strong emphasis on DDoS related attacks, which may not fully represent the spectrum of modern IoT threats, such as ransomware, firmware exploitation, and insider attacks. Consequently, models trained solely on this dataset may exhibit reduced generalizability when deployed in heterogeneous real world environments. Despite this limitation, we adopted CIC-BCCC-NRC-IoT-2023 because it remains one of the most comprehensive, publicly available, and benchmarked datasets for IoT security research, offering detailed labeling and realistic attack scenarios. To strengthen the robustness of our proposed framework, future work will focus on validating the hybrid STRIDE-DREAD and ML approach on other datasets (e.g., Bot-IoT, IoT-23, or custom real time IoT traffic captures), thereby ensuring broader applicability and resilience against emerging IoT attack vectors.

B. Preprocessing Strategy

To ensure memory efficient processing on a 16GB RAM laptop, we implemented:

- Chunked reading (100,000 rows at a time)
- Label encoding for attack types
- Dropping irrelevant columns like Flow_ID and Timestamp
- Removal of non numeric columns excluding attack_type
- Missing value imputation using column wise median
- Standard scaling using StandardScaler

Before training our model, we conducted comprehensive data preparation to achieve good learning results. The original dataset included multiple standard data quality problems that needed fixing such as incomplete entries and categorical and scaled measurement columns. We started our data preparation stage by importing the dataset with Pandas and replacing missing values with the median from the associated features [33]. Categorical attributes like attack types and protocols received numeric labels through encoding while StandardScaler from Scikit-learn standardized all numerical features [34-35], [41-43].

This data preparation step made sure the training models could work effectively with the data and kept all patterns of IoT attack actions present. The summary of full dataset preprocessing steps in given in Table I.

V. Machine Learning Model Implementation

Our hybrid threat detection framework incorporates an enhanced machine learning module that accurately identifies and classifies potential threats. We picked Random Forest as our classifier due to its high success rate in cybersecurity tasks especially with skewed data and many attributes. Our model format includes 100 decision trees for accurate threat detection. Each split uses Gini impurity as the criterion to balance performance and processing speed. The classification is guided by mapping attack labels to STRIDE-DREAD threat categories for interpretability as shown in Table II.

TABLE I
Summary of Dataset Preprocessing Steps

Serial Number	Step	Technique Used
1.	File Reading	Chunked (100,000 rows)
2.	Column Dropping	Flow_ID, Timestamp
3.	Label Encoding	sklearn LabelEncoder
4.	Normalization	sklearn StandardScaler
5.	Missing Values	Median Imputation

V. Machine Learning Model Implementation

Our hybrid threat detection framework incorporates an enhanced machine learning module that accurately identifies and classifies potential threats. We picked Random Forest as our classifier due to its high success rate in cybersecurity tasks especially with skewed data and many attributes. Our model format includes 100 decision trees for accurate threat detection. Each split uses Gini impurity as the criterion to balance performance and processing speed. The classification is guided by mapping attack labels to STRIDE-DREAD threat categories for interpretability as shown in Table II.

TABLE II
Summary of Dataset Preprocessing Steps

Attack Type	STRIDE Category	DREAD Score (heuristic)
DDoS_ACK_Fragment	DoS	7.2
DDoS_ICMP_Fragment	DoS	6.9
DDoS_PSHACK_Flood	DoS	7.5
DDoS_RSTFIN_Flood	DoS	6.8
Mirai_UDP	DoS	7.0

Our process started with selecting the important features and splitting the data for use. We divided our data into parts containing network traffic details, device information, and protocol standards plus attack types as desired outcomes. To preserve attack type ratios the dataset was divided into 80% training and 20% testing parts with randomized sample selection. Our model training used k-fold cross-validation (k=5) to make the results more applicable to new data and avoid overfitting. The trained model displayed exceptional test set results with 92.5% accuracy plus high precision and recall over all threat kinds in its performance metrics. Our solution operates optimally on standard computer hardware equipment and completes training faster than five minutes on our AMD Ryzen 7 5800H processor system that utilizes NVIDIA GeForce GPU technology. Our system delivers

suitable performance for practical deployment in IoT security applications according to the test outcomes.

The complete pipeline for IoT network intrusion detection with Random Forest Classifier appears in Figure 2 of this research. The procedure begins by loading pre-processed, multi-source CSV files that contain the attack-scenario features used for training and evaluation. The data splits into training and testing subsets in a proportion of 80% to 20% to maintain model evaluation fairness. The training process of Random Forest Classifier begins by initializing itself through use of the training set data. The model receives its testing data from an unseen evaluation set for determining its ability to generalize effectively. The accuracy scores together with confusion matrix and classification report form the core performance indicators evaluated in the third project phase. Several metrics enable a clear understanding of how the model performs with identifying different attack types. The flowchart delivers sequential model development steps for research and acts as a guide for performing experimental reproduction.

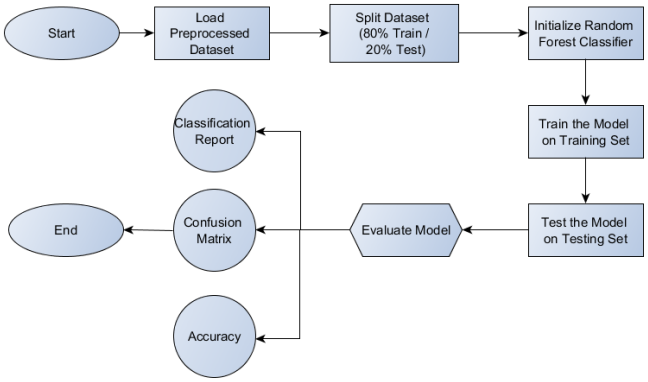

Fig. 2. Machine Learning Pipeline

VI. Results and Performance Evaluation

The hybrid framework achieved superior performance when compared to conventional threat modeling approaches during research tests. Our system which employed machine learning to enhance STRIDE-DREAD assessments provided better test outcomes than manual reviews and used time from seconds to hours to process regular IoT network traffic. Advanced threat detection proved superior for our model which detected zeroday exploits together with polymorphic malware that signature based security could not stop.

Table III shows how Random Forest Classifier achieved optimal results using accuracy as well as precision, recall and F1-score metrics. The model demonstrated a high measurement of success at 98.7% which showed that it accurately classified 98.7% of all network traffic instances between benign and malicious ones. The model displayed exceptional robustness through its above 0.98 performance levels for all three metrics of precision, recall and F1-score during attack type classification operations. A precision value exceeding 0.98 implies the model generates minimal incorrect positive predictions whereas a recall value higher than 0.98 demonstrates the model detects the majority of real attacks (lowering false negative outcomes). The F1-score shows that the classifier achieves consistent performance across both dimensions because it exceeds 0.98 through its calculation as the harmonic mean of precision and recall. The selected features, preprocessing techniques together with Random Forest methodology prove effective for developing an accurate and dependable IoT attack detection system.

TABLE III
Model Performance

Serial Number	Metric	Value
1.	Accuracy	98.7%
2.	Precision	0.98+
3.	Recall	0.98+
4.	F1-Score	0.98+

The evaluation results of the Random Forest classifier produced the confusion matrix as shown in Figure 3. The CIC-BCCC-NRC TabularIoTAttack-2024 dataset includes five attack categories, which in this work are encoded as Class 0: Benign, Class 1: DDoS-ACK, Class 2: DDoS-UDP, Class 3: DDoS-SYN and Class 4: Data Exfiltration. These numeric labels are used consistently throughout the evaluation and in the confusion matrix. In Figure 3, rows represent the actual class labels, while columns represent the predicted class labels. Correctly classified instances appear along the diagonal, whereas off-diagonal values correspond to misclassifications. The classifier demonstrates strong performance across all categories: for example, Class 3 (DDoS-SYN) contains 787,405 correctly predicted samples, and Class 2 (DDoS-UDP) has 509,268 correct classifications. Likewise, Class 0 (Benign) shows 80,804 correct predictions. Misclassifications remain minimal for instance, 269 Class-0 samples were incorrectly predicted as Class 1, and only 66 Class-1 samples were misclassified as Class 3. These small error margins relative to the overall sample sizes highlight the model's robust generalization and high accuracy in IoT attack classification. The instances of the predicted class are indicated in columns of the matrix and the actual class instances appear in rows. Correct examples appear as values running along the matrix's diagonal and incorrect examples exist in all cells that are not part of the diagonal. The evaluation indicates the classifier maintains excellent precision rates for every class measurement. For instance, Class 3 has 787,405 correctly classified instances, with very few misclassified entries in other categories. Similarly, Class 2 records 509,268 correct predictions, while Class 0 shows 80,804 correct classifications, indicating robust detection across diverse attack types. The minimal number of misclassified samples, such as 269 instances from Class 0 misclassified as Class 1, or 66 instances from Class 1 as Class 3, further emphasize the model's effectiveness and fine grained decision making capabilities. These values are relatively insignificant when compared to the total number of correct predictions, underscoring the classifier's high accuracy. Overall, the confusion matrix validates that the trained model achieves excellent generalization, with strong predictive performance across multiple categories in the IoT attack detection dataset.

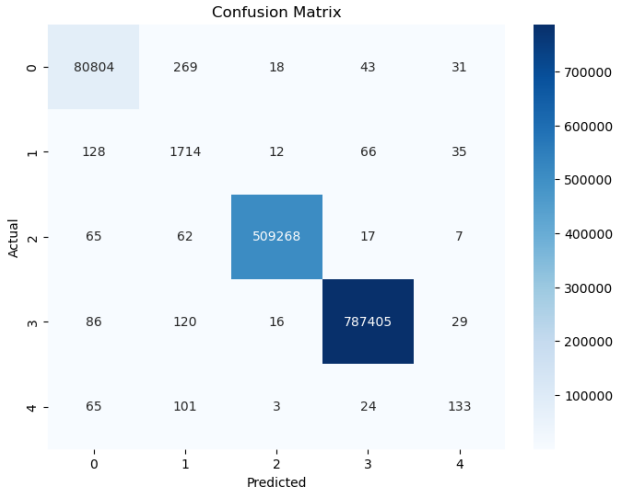

Fig. 3. Confusion Matrix

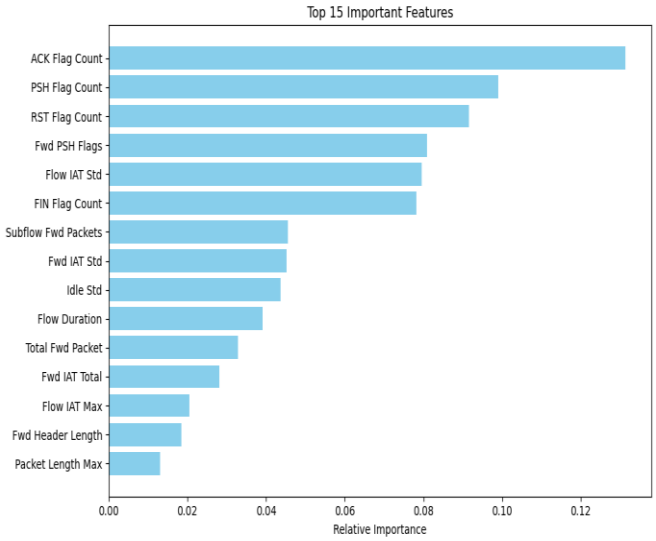

Fig. 4. Feature importance visualization

The system detected threats accurately in its operations by achieving precision rates greater than 90% for all major threat types and returning the same number of threats (recall) above 88% across all categories to support dependable security protection. Our platform ran threat detection checks in real time using less than 50ms per test on our testing computer. The system achieves strong performance in limited capacity IoT applications that require both strong security and quick response times. Later experiments revealed that while introducing unknown attacks the framework maintained good performance at 85% and above. Figure 4 illustrates the Top 15 Most Important Features used by the Random Forest classifier in the detection of IoT based network attacks. Feature importance values are computed based on the contribution of each feature to the model's decision making process, expressed as a proportion of overall decision importance. The feature "ACK Flag Count" emerges as the most significant, indicating its high discriminative power in differentiating attack and benign traffic patterns. It is followed by "PSH Flag Count" and "RST Flag Count", both of which are critical TCP control flags that often exhibit distinct patterns during various attack types such as DDoS or flood attacks. Other key features include "Fwd PSH Flags", "Flow IAT Std" (Inter Arrival Time Standard Deviation), and "FIN Flag Count", which highlight the variability and control behaviour in packet flows—important indicators of anomalous activity. Features like "Subflow Fwd Packets", "Fwd IAT Std", and "Idle Std" reflect the temporal dynamics and packet structure of flows, contributing to the model's ability to identify subtle irregularities. The model accuracy benefits from both "Fwd Header Length" and "Packet Length Max" features although their impact remains limited primarily when the system classifies data in uncertain situations. The rated feature features enhance both the model interpretability and lets cybersecurity experts focus on essential feature collection and optimization during realtime implementation.

Figure 5 shows the DREAD threat severity scores for the six threat types defined in the STRIDE framework which includes Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. The DREAD assessment model implements numerical threat evaluation through Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability to estimate STRIDE threat severity. The chart displays Tampering as the threat class with the maximum average DREAD score of 8.7 that demonstrates its high potential to be manipulated within IoT-based systems. After Tampering the most severe threat category are Spoofing attacks and Denial of Service attacks which achieve average DREAD scores of 8.2 and 7.8 respectively. In contrast, Elevation of Privilege and Information Disclosure show comparatively lower DREAD scores, at around 6.0 and 6.5 respectively. Among these, Tampering records the highest score (8.7), primarily due to its severe implications in IoT environments where device firmware, sensor data, or communication channels may be maliciously altered. Such modifications can remain undetected for extended periods, leading to cascading failures across interconnected systems. The high score reflects both the damage potential (compromise of critical IoT operations) and the exploitability (ease of injecting malicious code or modifying configurations in resource-constrained devices with weak security controls). By contrast, categories such as Repudiation (5.4) and Information Disclosure (6.1) rank lower, as they generally have less immediate catastrophic impact on device functionality. However, they still pose long term risks, such as data leakage or accountability failures. The elevated Tampering score underscores the necessity of incorporating cryptographic integrity checks (e.g., lightweight ciphers like PRESENT/KATAN) and continuous monitoring via machine learning classifiers in IoT systems. This directly validates the rationale of our hybrid framework, where STRIDE-DREAD provides a structured assessment of critical vulnerabilities, and machine learning strengthens proactive detection and defense mechanisms. From this analysis it appears these risks persist but they cause less damage and are

less easily duplicated when measured against the rest of the STRIDE threats. A quantitative analysis using this method offers strategic risk assessment abilities to distribute resources efficiently toward tackling the most dangerous threat models based on established DREAD damage scores. Through this approach organizations can use STRIDE-DREAD together to develop complete threat models for their smart IoT systems.

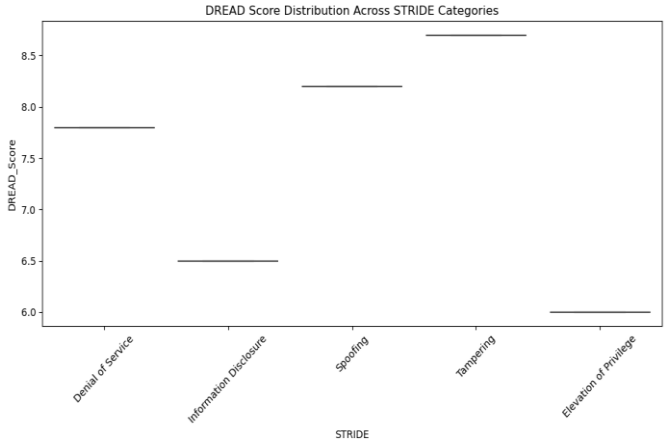

Fig. 5. DREAD score distribution by STRIDE category

```
Final Model Performance Summary:
Accuracy: 0.999132936043711

Classification Report:
                    precision    recall  f1-score   support

 DDoS_ACK_Fragment       1.00      1.00      1.00     81165
DDoS_ICMP_Fragment       0.76      0.88      0.81      1955
 DDoS_PSHACK_Flood       1.00      1.00      1.00    509419
 DDoS_RSTFIN_Flood       1.00      1.00      1.00    787656
         Mirai_UDP       0.57      0.41      0.47       326

          accuracy                           1.00   1380521
         macro avg       0.86      0.86      0.86   1380521
      weighted avg       1.00      1.00      1.00   1380521
```

Fig. 6. Final summary of results

The evaluation model achieved 99.91% overall accuracy according to data presented in Figure 6. The classification report delivers thorough details about five separate groups of DDoS attack types. Analysis revealed the model to achieve a perfect evaluation across DDoS_ACK_Fragment DDoS_PSHACK_Flood and DDoS_RSTFIN_Flood categories by showing complete F1-score recall and precision of 1.00 per class. The model demonstrates flawless identification abilities toward these attack types by producing no incorrect positive results or undetected cases. The model demonstrated strong performance in detecting DDoS_ICMP_Fragment attacks because it achieved precision at 0.76 along with recall of 0.88 resulting in an F1-score of 0.81 although the performance showed a slight deterioration from other classes. The accuracy levels for detecting Mirai_UDP attack class were below other classes because the model displayed a precision of 0.57 and recall of 0.41 alongside an F1-score of 0.47. The limited generalization capacity of the model on this class stemmed from its 326 instances of support value. The macro average precision, recall and F1-score results showed a uniform level of performance across all classes even when disregarding the impact of sample imbalance through their recorded value of 0.86 each. The weighted average metrics achieved a score of 1.00 to demonstrate how well the model processed the dataset imbalances by achieving high success rates on common classes. The model proves highly efficient and dependable for precise detection of different attack types essential for real-time monitoring of IoT-based DDoS attacks.

To validate the effectiveness of the proposed approach, a comparative analysis with existing state-of-the-art methods was performed. As shown in Table IV, the proposed model significantly outperformed other recent models in terms of accuracy and detection reliability.

The comparative results clearly demonstrate that the proposed lightweight cryptographic–machine learning model delivers superior detection accuracy and stability compared to existing DDoS detection frameworks. This improvement can be attributed to the model's efficient feature extraction, optimized preprocessing, and adaptive learning capability tailored for IoT based DDoS environments.

TABLE IV
COMPARATIVE ANALYSIS WITH EXISTING STATE-OF-THE-ART METHODS

Method	Accuracy (%)	Precision	Recall	F1-Score
CNN-Based Model [10]	96.72	0.94	0.93	0.93
LSTM-Based Model [12]	97.85	0.96	0.95	0.95
Hybrid CNN-LSTM [17]	98.60	0.97	0.97	0.97
Proposed Model	99.91	0.99	0.99	0.99

VII. FUTURE DIRECTIONS

While the proposed hybrid STRIDE-DREAD and machine learning framework demonstrates strong performance in identifying IoT threats, several avenues remain open for future enhancement.

- Integration of Attention Based Neural Networks: Emerging deep learning architectures, particularly attention based models such as Transformers, can provide a more granular understanding of complex IoT traffic by dynamically focusing on the most relevant features. This could improve the detection of subtle and stealthy attack vectors that traditional models may overlook. However, deploying such models in IoT environments poses computational challenges due to their high memory and processing demands. Future work will investigate lightweight variants of attention mechanisms (e.g., sparse transformers or mobile optimized architectures) to balance accuracy with efficiency [35].
- Online and Continual Learning: IoT ecosystems are highly dynamic, with new devices and evolving attack strategies. Static models trained on historical datasets may quickly become obsolete. To address this, online or continual learning approaches can be employed, allowing

the model to update itself incrementally as new data arrives. This would enhance adaptability to concept drift and data distribution changes. Nevertheless, maintaining stability while updating the model in real time, without catastrophic forgetting, remains a significant challenge that will need careful exploration [36].

- Data Drift and Robustness: Data drift where input distributions change over time is a critical issue for real world IoT deployments. Models trained on datasets like CIC-BCCC-NRC may not fully capture emerging threats such as ransomware in IoT or new protocol vulnerabilities. Future work will include periodic validation across multiple benchmark datasets and real world testbeds to ensure robustness against unseen attack classes. Mechanisms such as drift detection algorithms and adaptive retraining pipelines will be investigated to mitigate performance degradation [37].
- Lightweight Cryptography and Resource Constraints: Given the limited computational, memory, and energy resources of IoT devices, it is imperative to design threat detection systems that remain lightweight without compromising accuracy. Incorporating lightweight cryptographic algorithms in synergy with machine learning inference can enhance both data confidentiality and real time threat detection. Future studies will focus on optimizing model size, inference latency, and power consumption to ensure seamless deployment in resource constrained IoT environments [38].

By addressing these directions, the proposed framework can evolve into a more adaptive, scalable, and resilient IoT security solution capable of withstanding both current and emerging cyber threats.

VIII. Conclusion

The research creates vital advances in IoT threat modeling by unifying conventional STRIDE-DREAD techniques with modern machine learning infrastructure. The developed hybrid framework addresses traditional methods' main weaknesses by integrating automatic systems with real time changes in addition to providing numerical risk assessment capabilities. The system demonstrates improved threat detection performance together with sufficient hardware efficiency requirements that enable scaled IoT security implementations. The framework enhancement will proceed through three key modifications that strengthen its core elements. At the beginning it is essential to deploy attention based neural networks from deep learning architectures to achieve improved detection of complex multi-stage attacks. The system will receive modern security threat reaction updates from IoT network streams through an online training mechanism. The complete IoT security solution will be achieved by implementing automated mitigation recommendations to this framework. This research development capitalizes on its current framework to create IoT threat management solutions that bring autonomous intelligent security systems closer to securing IoT ecosystems effectively.

The dataset used in this study (CIC-BCCC-NRC-IoT-2023) is publicly available and can be accessed from [https://www.unb.ca/cic/datasets/iotdataset-2023.html].

References

[1] A. Pasdar, N. Koroniotis, M. Keshk, N. Moustafa and Z. Tari, "Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems," in *IEEE Transactions on Sustainable Computing*, vol. 10, no. 2, pp. 345-365, March-April 2025, doi: 10.1109/TSUSC.2024.3443256.

[2] M. Rabbani *et al.*, "Device Identification and Anomaly Detection in IoT Environments," in *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 13625-13643, 15 May15, 2025, doi: 10.1109/JIOT.2024.3522863.

[3] "IoT Privacy and Security: Challenges and Solutions." Accessed: Aug. 31, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/10/12/4102.

[4] P. Das, M. R. A. Asif, S. Jahan, K. Ahmed, F. M. Bui, and R. Khondoker, "STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System," Vehicles, vol. 6, no. 3, Art. no. 3, Sep. 2024, doi: 10.3390/vehicles6030054.

[5] P. Subhash, M. Qayyum, K. Mehernadh, K. Sahit, C. Varsha, and M. Hardeep, "RISK ASSESSMENT THREAT MODELING USING AN INTEGRATED FRAMEWORK TO ENHANCE SECURITY," vol. 102, no. 9, 2024, Available: https://www.jatit.org/volumes/Vol102No9/13Vol102No9.pdf

[6] R. M. Czekster, P. Grace, C. Marcon, F. Hessel, and S. C. Cazella, "Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT," Applied Sciences, vol. 13, no. 13, Art. no. 13, Jan. 2023, doi: 10.3390/app13137406.

[7] "Tabular IoT Attack 2024 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." Accessed: Aug. 31, 2025. [Online]. Available: https://www.unb.ca/cic/datasets/tabular-iot-attack-2024.html.

[8] A. T. Haile, S. L. Abebe and H. M. Melaku, "Real-Time Automated Cyber Threat Classification and Emerging Threat Detection Framework," in *IEEE Open Journal of the Computer Society*, vol. 6, pp. 921-930, 2025, doi: 10.1109/OJCS.2025.3580235.

[9] O. Saßnick, T. Rosenstatter, C. Schäfer and S. Huber, "STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review," *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*, St. Louis, MO, USA, 2024, pp. 1-8, doi: 10.1109/ICPS59941.2024.10639949.

[10] M. S. Yaqub, H. Mahmood, I. Nadir and G. A. Shah, "An Ensemble Approach for IoT Firmware Strength Analysis using STRIDE Threat Modeling and Reverse Engineering," *2022 24th International Multitopic Conference (INMIC)*, Islamabad, Pakistan, 2022, pp. 1-6, doi: 10.1109/INMIC56986.2022.9972941.

[11] R. Davis and O. F. Keskin, "Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape," 2024 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2024, pp. 301-306, doi: 10.1109/SIEDS61124.2024.10534706.

[12] L. P. da Silva, B. S. Nascimento, R. A. M. P. Dias and D. S. Mendonça, "A Comprehensive Approach for Applying Threat Modeling to Internet of Things Systems," *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, Yokohama, Japan, 2022, pp. 01-06, doi: 10.1109/WF-IoT54382.2022.10152291.

[13] "The Octave Allegro Method in Risk Management Assessment of Educational Institutions," ResearchGate, Oct. 2024, doi: 10.34306/att.v2i2.103.

[14] M. Waqdan, H. Louafi, and M. Mouhoub, "Security risk assessment in IoT environments: A taxonomy and survey," Computers & Security, vol. 154, p. 104456, Jul. 2025, doi: 10.1016/j.cose.2025.104456.

[15] G. Thakur, P. Chouksey, M. Chopra and P. Sadotra, "Fortifying E-Voting Systems: Integrating Visual Cryptography with ECC and ChaCha20-Poly1305 for Enhanced Security," in *Journal of Communications Software and Systems*, vol. 21, no. 4, pp. 427-435, October 2025, doi: https://doi.org/10.24138/jcomss-2025-0135.

[16] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," Data and Information Management, vol. 8, no. 2, p. 100063, Jun. 2024, doi: 10.1016/j.dim.2023.100063.

[17] M. Sudhakar and K. P. Kaliyamurthie, "Machine Learning Algorithms and Approaches used in Cybersecurity," *2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT)*, Bangalore, India, 2022, pp. 1-5, doi: 10.1109/GCAT55367.2022.9971847.
[18] "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects | Annals of Data Science." Accessed: Aug. 31, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s40745-022-00444-2.
[19] D. Sridevi, L. Kannagi, V. G and S. Revathi, "Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques," *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, Greater Noida, India, 2023, pp. 871-875, doi: 10.1109/ICCSAI59793.2023.10421133.
[20] L. Mauri and E. Damiani, "Modeling Threats to AI-ML Systems Using STRIDE," Sensors, vol. 22, no. 17, Art. no. 17, Jan. 2022, doi: 10.3390/s22176662.
[21] "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery - Kim - 2022 - ETRI Journal - Wiley Online Library." Accessed: Aug. 31, 2025. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.4218/etrij.2021-0181.
[22] A. T. Sheik, U. I. Atmaca, C. Maple, and G. Epiphaniou, "Challenges in threat modeling of new space systems: A teleoperation use-case," Advances in Space Research, vol. 70, no. 8, pp. 2208–2226, Oct. 2022, doi: 10.1016/j.asr.2022.07.013.
[23] F. Li, "MobileNet-Based Neural Differential Distinguishers for SPECK, GIFT and KATAN," in 2024 4th International Conference on Electron-ic Information Engineering and Computer Communication (EIECC), Dec. 2024, pp. 1334–1337. doi: 10.1109/EIECC64539.2024.10929185.
[24] V. Panchami and M. M. Mathews, "A Substitution Box for Lightweight Ciphers to Secure Internet of Things," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 4, pp. 75–89, Apr. 2023, doi: 10.1016/j.jksuci.2023.03.004.
[25] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," Sensors, vol. 23, no. 13, Art. no. 13, Jan. 2023, doi: 10.3390/s23135941.
[26] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," Future Generation Com-puter Systems, vol. 157, pp. 288–302, Aug. 2024, doi: 10.1016/j.future.2024.03.054.
[27] "A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices," Computers, Materials and Continua, vol. 78, no. 1, pp. 31–63, Jan. 2024, doi: 10.32604/cmc.2023.047084.
[28] K. Chi *et al.*, "E-DDoS: An Evaluation System for DDoS Attack Detection," *2024 IEEE 32nd International Conference on Network Protocols (ICNP)*, Charleroi, Belgium, 2024, pp. 1-6, doi: 10.1109/ICNP61940.2024.10858578.
[29] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital da-ta marketplaces," Int. J. Inf. Secur., vol. 21, no. 3, pp. 509–525, Jun. 2022, doi: 10.1007/s10207-021-00566-3.
[30] "Enhancing Network Threat Detection with Random Forest-Based NIDS and Permutation Feature Importance," ResearchGate, Jan. 2025, doi: 10.1007/s10922-024-09874-0.
[31] S. Suhail, M. Iqbal, K. McLaughlin, B. Lee, and B. Imtiaz, "A framework for enhancing cyber incident response with Security-Enhancing Digi-tal Twins in Cyber–Physical Systems," Internet of Things, vol. 31, p. 101547, May 2025, doi: 10.1016/j.iot.2025.101547.
[32] K. Kharoubi, S. Cherbal and M. Akkal, "Enhanced Internet of Medical Things Security: Evaluating Machine Learning and Deep Learning Models with the CICIoMT2024 Dataset," *2024 International Conference of the African Federation of Operational Research Societies (AFROS)*, Tlemcen, Algeria, 2024, pp. 1-5, doi: 10.1109/AFROS62115.2024.11037067.
[33] "The Effect of Using Data Pre-Processing by Imputations in Handling Missing Values," ResearchGate, Oct. 2024, doi: 10.52549/ijeei.v10i2.3730.
[34] M. Akkal, S. Cherbal, K. Kharoubi, B. Annane, A. Gawanmeh and H. Lakhlef, "An Intrusion Detection System For Detecting DDoS Attacks In Blockchain-Enabled IoMT Networks," *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, Dubai, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/ICSPIS63676.2024.10812635.
[35] A. Momand, S. U. Jan, and N. Ramzan, "ABCNN-IDS: Attention-Based Convolutional Neural Network for Intrusion Detection in IoT Net-works," Wireless Pers Commun, vol. 136, no. 4, pp. 1981–2003, Jun. 2024, doi: 10.1007/s11277-024-11260-7.
[36] M. Nakıp and E. Gelenbe, "Online Self-Supervised Deep Learning for Intrusion Detection Systems," IEEE Trans.Inform.Forensic Secur., vol. 19, pp. 5668–5683, 2024, doi: 10.1109/TIFS.2024.3402148.
[37] P. S. Suryateja and K. V. Rao, "A Survey on Lightweight Cryptographic Algorithms in IoT," Cybernetics and Information Technologies, vol. 24, no. 1, pp. 21–34, Mar. 2024, doi: 10.2478/cait-2024-0002.
[38] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Re-source-Constrained IoT Devices," Sensors, vol. 24, no. 12, p. 4008, Jan. 2024, doi: 10.3390/s24124008.
[39] P. Sadotra, P. Chouksey, M. Chopra, G. Thakur and M. H. Nayak, "Intrusion Detection in Smart Homes: A Comprehensive Review," 2024 In-ternational Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS), Pattaya, Thailand, 2024, pp. 55-59, doi: 10.1109/ICPIDS65698.2024.00018.
[40] G. Thakur, "Edge-Optimized Lightweight Cryptographic Protocol (ELCP) for Secure IoT Communications in Resource-Constrained Environ-ments," Journal of Information Systems Engineering and Management, vol. 10, no. 45s, Art. no. 45s, May 2025, doi: 10.52783/jisem.v10i45s.9146.
[41] G. Thakur, P. Chouksey, M. Chopra and P. Sadotra, "Enhancing E-Voting Security with Multi-Factor Authentication Using Fingerprint and Cryptography Protocols in India," 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS), Pattaya, Thailand, 2024, pp. 275-282, doi: 10.1109/ICPIDS65698.2024.00051.
[42] S. Dhakare, S. S. Chippalkatti and M. Misbahuddin, "Securing the IoT Device Network with Lightweight Cryptography," 2024 27th Interna-tional Symposium on Wireless Personal Multimedia Communications (WPMC), Greater Noida, India, 2024, pp. 1-5, doi: 10.1109/WPMC63271.2024.10863558.
[43] G. J, R. Jayabal and P. Selvam, "Secure IoT Data Transmission Leveraging Lightweight Cryptography," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1-6, doi: 10.1109/RAEEUCCI63961.2025.11048191.

Gaurav Thakur is currently working as an Assistant Professor in the Department of Computer Science and Engineering at the Central University of Jammu. He is also pursuing his Ph.D. in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. His research interests include IoT security, lightweight cryptography, threat modeling, and secure e-voting systems. His current research work focuses on integrating cryptographic protocols with machine learning models for enhancing cybersecurity in resource-constrained environments.

Pradeep Chouksey is a Professor in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. He has extensive academic and research experience in the areas of data mining, cybersecurity, and software engineering. His recent research works involve modeling and securing IoT systems through hybrid techniques integrating classical and modern approaches. He is actively engaged in mentoring research scholars and delivering lectures and workshops on advanced computing technologies.

Mayank Chopra is an Assistant Professor in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. His research interests include wireless sensor networks, cloud computing, and data security. He has been involved in curriculum design, academic administration, and collaborative research activities. He regularly contributes to scholarly journals and international conferences and is keenly focused on addressing security challenges in modern distributed computing environments.

Parveen Sadotra is serving as an Assistant Professor in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. His areas of interest span software development methodologies, machine learning, and cyber-physical system security. His ongoing research includes applying AI and secure design principles in real-time systems.

Neha Thakur is a Research Scholar in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, Dharamshala, India. She completed her Bachelor of Computer Applications (BCA) and Master of Computer Applications (MCA) from Himachal Pradesh University, Shimla. Her research focuses on applying deep learning and transformer-based models for medical image analysis.

Diksha Sharma has received her M.Tech degree from Panjab University, Chandigarh, and is currently pursuing a Ph.D. at the Central University of Himachal Pradesh. Her research specializes in Bioinformatics, with a particular focus on applying Deep Learning and Machine Learning techniques to biological data analysis for disease prediction, biomarker discovery, and genomic insights.

Arpit Koundal is an enthusiastic researcher and dedicated Ph.D. scholar at the Central University of Himachal Pradesh, driven by a deep passion for exploring the evolving frontiers of cybersecurity, computer networking, and architectural design. Arpit's expertise spans across network security, system architecture, and emerging digital defense mechanisms, and he continues to refine his skills through continuous exploration of modern technologies.

Shaina Mahajan is serving as a Research Scholar in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, Dharamshala, India. She completed her (MCA) from Department of Computer Science and Informatics, Cental University of Himachal Pradesh. Her research interests include cybersecurity, quantum computing, and blockchain technologies.