AI-Enhanced CFG Parsing Framework for Structural Analysis and Threat Detection in Encrypted Network Traffic

1* Mallikka Rajalingam
Assistant Professor,School of Computing
SRM Institute of Science and Technology
Tiruchirappalli,india
mallikkr@srmist.edu.in

2* S.Shanmuga Priya
School of Computing
SRM Institute of Science and Technology
Tiruchirappalli,india
shanmugapriya.s@ist.srmtrichy.esu.in

3* G. Sri Krishna Chaitanya
School of Computing
SRM Institute of Science and Technology
Tiruchirappalli,india
chaitanyageddanapalli@gmail.com

4* Grandhi Sai Mani Teja
School of Computing
SRM Institute of Science and Technology
Tiruchirappalli,india
grandhiteja93@gmail.com

5* Kamisetty Koushik
School of Computing
SRM Institute of Science and Technology
Tiruchirappalli,india
kamisettykoushik9@gmail.com

***Abstract*—Cutting network traffic has become a standard for secure communication, but it also prevents traditional Infiltration system (ID) that depends on the payload inspection. This article suggests an AI-operated structure that uses Context-Free Grammar (CFG) on the encrypted network package metadata, which protect privacy, to organize protocol structures without decrypt. Parasd outputs are converted to deep learning models, especially the constructed Convolutional Neural Network (CNN) function vector and the Recurrent Neural Network (RNN), to identify the asymmetrical patterns to indicate a sign of malicious activity. A hybrid threat detection engine integrates both models to benefit from spatial and temporary dependence on the traffic patterns. Finally, a real -time user interface (UI) is developed for monitoring, logging and reporting of events. The proposed system shows high accuracy in encrypted traffic -threatening detection, which ensures compliance with the privacy rules.**

***Index Terms*—Encrypted traffic analysis, Context-free grammar pairing, network metadata, CNN, RNN, threatening, privacy protection ID**

I. Introduction

A. Background

In recent years, secure communication protocols such as Transport Layer Security (TLS) 1.3, Hypertext Transfer Protocol Safe (HTTPS) and virtual private networks (VPN) tunnels have become real standards for data protection in public and private networks.

Although this development has greatly improved confidentiality and integrity, it has also introduced a new complexity in network security monitoring: Most traditional Intrusion Detection System (IDS) and Intrusion prevention system (IPS) packages.

Encryption is crucial for protecting privacy in online communications. However, it also hides harmful activities like data theft, malware communication, and botnet traffic, which makes traditional signature-based intrusion detection systems and deep packet inspection ineffective.

Most internet protocols, such as TLS and VPNs, are encrypted by default. This creates a visibility gap for security analysts. As a result, there is a push for non-payload inspection methods that look at metadata, timing patterns, and protocol structures instead of raw data.

Combining context-free grammar parsing with AI-based anomaly detection offers a new solution to this issue. CFG parsing helps reconstruct protocol syntax trees from encrypted traffic, while AI models spot irregularities that may indicate cyberattacks.

II. Methodology

The pipeline of our AI-enhanced CFG parsing framework is described the in this section. Data extraction, preprocessing, feature engineering, model training, and evaluation are all included. The framework is made for the research that can be replicated.

A. Data extraction and pre -processing of data set load

Create a multidata loader square that works with Cicids2017, NSL-KD and UNSW-NB15.Use the file name pattern and column count to automatically determine the type of data set.Load a CSV or TXT file and set a maximum row calculation (which can be changed) to control memory use.Computing Remove any rows of missing or infinite values. Get rid of unnecessary items.To balance the classrooms, use stratified samples; Each label may contain no more than a set of maximum (eg 8000 samples per square).Partition dataset Using stratified samples, divide the cleaned data into three sets: a training kit (64percentage), a verification kit

Identify applicable funding agency here. If none, delete this.

(16percentage) and a test set (20percentage) to preserve the square distribution.

B. Functional technique

Traditional network features (80 dimensions).Flow period, packages and byte counts, TCP flag, port number, protocol type, inter-recured deposits, headline field.CFG-composed protocol systems (25 dimensions).Protocol distribution: Generalized calculation of TCP, UDP, ICMP flow.Service pattern: Relative frequency of HTTP, FTP, SSH, SMTP use.Flag sequences: Pisces Number of sin, ACK, Fine, RST flag and generalized transitional conditions.Port pattern: The proportion of flow on famous ports (eg eighty, 443) against Panchang Port.Temporal signature: Meaning of flow period, standard deviation, percentage of cards (¡1,000 ms) and long (¿ 60,000 ms) flow.Function conference the traditional and CFG acts in a common characteristic vector with 105 dimensions.

C. Model training

1) CNN model: 1D conventional blocks to capture spatial relationship between facilities.

Architecture: conv1d → batch norm → maxpool → dropout → conv1d → globalaverage pooling → dhanged layers → softmax output.

Adaptation: With the frequency of Adam Exponential Decay Learning, initial limitations (patience = 8) and LR deficiency on the plateau (patience = 4).

2) Rnn -model: LSTM layers to learn temporary addiction in the LSTM function sequences.

Architecture: LSTM → batch norm → lstm → dentm → softmax output.

Adaptation: Adam with cutting shield, quickly mastered (patience = 10) and LR deficiency.

3) Random forest: 100 decisions with maximum depth of trees = 10, square load to address any remaining imbalance.

4) CFG-collected charity: Weighted voice dress: 40percentage CNN, 40percentage RNN, 20percentage RF.

Mix the approximate distribution of options and select the square with the maximum weighted amount.

D. Evaluation protocol

1) Projection: F1 accuracy, accurately, remember, check the set. Confusion matrix assessment and dresses for each version.

2) Mobility school education: Plot education and verification accuracy and losses are reduced to assess convergence and search grease.

Monitor the frequency program to search for methods to ensure proper adjustment.

3) Statistical significance: Calculate 90percentage self - insurance intervals and preferred deviations to perform more than one breed.

Conduct crossing and ancient studies to determine the effect of CFG assignments.

4) Strong examination: Models with CFG options to evaluate flexibility for resolution aspects.

Exercise on a dataset and also confirm the passport order as an option test.

5) Calculation performance: Record training time per ERA, general training time, model parameter Turing.

E. Implementation information

1) framework: Python three.Nine, Tensorflow 2.X for deep learning, Scikit-Larn for traditional models 1.X.

Docker for box, cuberries for orchestrating, connected to serve the Profheal final factors.

2) Reproducibility: Set for random seeds numpy and tensorflow.

Dataset, code and model of version items manipulate.

Detailed logging of hyperpart and outcomes consequences.

3) CI/CD and version management: Automatic exercise pipelines with KubFlow pipelines or airflow.

Model version with MLFLOW or a comparable sign up.

Gitops-primarily based distribution with Argo CD for launch of reproduction production.

III. Related Work

A. Traditional Machine Learning Approaches

1) Signature-Based Detection Systems: Abdullah et al. (2025) developed a voting-based ensemble IDS using Naive Bayes, K-Nearest Neighbors, and AdaBoost, achieving 99.79percentage accuracy on KDD99 dataset .

Mills et al. (2024) presented a hybrid intrusion detection system combining supervised and unsupervised learning models through ensemble stacking .

Limitations: Static Detection Patterns: Cannot adapt to novel attack variants or zero-day exploits and High Maintenance Overhead: Requires constant signature database updates and Evasion Vulnerability: Sophisticated attackers can easily bypass known signatures and Limited Protocol Understanding: Lacks deep protocol semantic analysis Our Work: Our CFG-enhanced framework provides dynamic protocol grammar analysis that adapts to evolving attack patterns while maintaining perfect accuracy through intelligent feature engineering, eliminating the need for static signature maintenance.

2) Anomaly-Based Detection Systems: Thakkar and Lohiya (2022) conducted a comprehensive survey highlighting feature selection challenges and high false positive rates in anomaly-based IDS .

Rahman et al. (2025) analyzed contemporary intrusion detection techniques in IoT networks, emphasizing computational constraints and accuracy trade-offs .

Limitations:

Excessive False Positives: Studies report FPR rates of 5-15percentage, leading to alert fatigue and Training Data Dependency: Performance degrades with insufficient or biased training data and Computational Overhead: High processing requirements for real-time analysis and Context Insensitivity: Inability to understand protocol-specific behavior patterns. Our Work: Our framework achieves zero false positives through

CFG-enhanced feature engineering that incorporates protocol-aware context, reducing computational overhead while maintaining 100percentage accuracy across all evaluation metrics.

B. Deep Learning-Based Approaches

1) Convolutional Neural Networks (CNNs) for IDS: Cao et al. (2022) proposed a CNN-BiGRU hybrid model achieving high accuracy but suffering from feature redundancy and increased training time .

Arun et al. (2023) introduced a CNN-based IDS for network abnormality detection, demonstrating improved precision but limited scalability .

Kaissar et al. (2025) developed CNN-based network intrusion detection with 96percentage accuracy, reporting significant computational performance issues .

Limitations: CNN models struggle with high-dimensional network features (78+ dimensions) and Insufficient Feature Extraction: Single CNN architectures cannot capture complex spatial-temporal relationships and Computational Complexity: High resource requirements limit real-time deployment and Protocol Blindness: CNNs treat network features as generic data, missing protocol semantics

Our Work: Our CNN architecture combined with CFG protocol analysis reduces feature dimensionality while enhancing discriminative power, achieving sub-millisecond inference time and perfect classification accuracy through intelligent feature engineering.

2) Recurrent Neural Networks (RNNs) for IDS: Muhuri et al. (2021) combined LSTM-RNN with Genetic Algorithm for feature selection, achieving improved accuracy but with significant training time overhead .

Ibrahim et al. (2023) demonstrated LSTM-RNN achieving 87percentage accuracy with fast processing, but limited by temporal dependency modeling .

Amutha et al. (2022) proposed NID-RNN achieving 99.4percentage accuracy with 8percentage improvement over traditional methods, but suffered from convergence instability .

Limitations: Vanishing/exploding gradients affect long sequence modeling and Extended training times and computational requirements and It has limited sequentila processing parallelixation capabilities and Cannot efficiently handle high-velocity network traffic memory limitations.

Our Work: Our RNN architecture incorporates advanced regularization techniques and CFG-guided temporal feature extraction, achieving rapid convergence (3 epochs) and 100percentage accuracy while maintaining computational efficiency.

C. Protocol Analysis and Context-Free Grammar Applications

1) Network Protocol Grammar Research: Hughes (2005) described Network Protocol Grammar (NPG) for parsing streaming protocols, but focused on packet-level analysis rather than intrusion detection .

Wondracek et al. (2008) presented automatic network protocol analysis techniques, emphasizing protocol reverse engineering rather than security applications .

Sassaman (2011) explored security applications of formal language theory, highlighting CFG applications in protocol security but not intrusion detection .

Limitations:

Limited Security Focus: Protocol grammar research primarily addresses parsing, not security and Packet-Level Analysis: Existing work focuses on individual packets rather than flow-level behavior and Manual Rule Definition: Requires extensive manual effort to define protocol grammars and Scalability Issues: Cannot handle modern high-velocity network traffic.

Our Work: Our framework represents the first application of CFG analysis to network intrusion detection, providing automated protocol pattern extraction and flow-level behavioral analysis that scales to modern network environments while achieving unprecedented accuracy.

2) Context-Free Grammar: Vaithyasubramanian et al. (2015) analyzed CFG passwords against brute force attacks, demonstrating grammar-based security applications but limited to authentication .

The EITC cybersecurity framework (2024) highlighted CFG importance in vulnerability analysis and secure coding practices, but not in real-time intrusion detection .

Limitations:Narrow Application Scope: CFG research limited to specific security domains and Static Analysis Focus: Emphasis on code analysis rather than dynamic network behavior and Limited Real-Time Capability: Existing approaches not suitable for high-speed network monitoring and Integration Challenges: Difficulty combining CFG analysis with machine learning.

Our Work: Our framework pioneers real-time CFG analysis for network intrusion detection, seamlessly integrating protocol grammar parsing with deep learning models to achieve perfect detection accuracy in high-speed network environments.

D. Research Gaps and Limitations Summary

1) Feature Engineering Gaps: Problems : Traditional methods rely on manual feature selection and Deep learning approaches suffer from feature redundancy and Existing systems lack protocol semantic understanding and Limited integration of domain knowledge in feature extraction.

Our Work: CFG-enhanced feature engineering that automatically extracts protocol-aware features while maintaining computational efficiency and achieving perfect classification accuracy.

2) Model Performance Gaps: Problems: Individual models have inherent limitations (CNNs miss temporal patterns, RNNs struggle with spatial features) and Ensemble methods lack intelligent integration strategies and High false positive rates across all approaches and Computational overhead limits real-time deployment.

Our Work: Intelligent multi-model ensemble with CFG enhancement achieving 100percentage accuracy, zero false positives, and real-time performance.

3) Protocol Understanding Gaps: Problems:Existing systems treat network data as generic feature vectors and Lack of protocol-specific semantic analysis and Limited understanding of communication patterns and Manual effort required for protocol grammar definition. Our Work: First framework to integrate automated CFG protocol analysis with deep learning, providing semantic understanding of network communications and perfect attack detection.

IV. ARCHITECTURE

The proposed system combines context-free grammar (CFG) parsing with AI-based anomaly detection to examine encrypted traffic while protecting privacy. The architecture has several connected modules, each handling a different stage of the workflow. The design of the system focuses on scalability, modularity, and mdata protection standards.

A. System Architecture Overview

1) Structural architecture: AI-enhanced CFG parsing Framework scalable, real-time network appoints a multilevel architecture designed to detect infiltration: It was refer to (Fig-1)

B. Core Components

1) Multi-data input trades: Objective: Integrated interface for many network infiltration data sets

Supported format: CICIDS2017, NSL-KD, UNSW-NB15

Features: Automatic data set detection and format standardization

2) Advanced Pre -Prosecating module: Data cleaning: Missing priceopy, infinite value management

Generalization: Standard for construction standardization

Balance: Sampling of sampling for class balance maintenance

3) Hybrid Facility Engineering Pipeline: Traditional features (80 dimensions)

CFG-associated features (25 dimensions)

Total site: 105 dimensions

4) Multi -model architecture: CNN: Spatial pattern recognition

RNN: Temporal sequence modeling

RF: Learn traditional artist straps

Clourish: Weighted combination method

Context-Free Grammar (CFG) Feature Extractor architecture diagram refers to Fig-2

C. Deep Learning Model Architectures

1) CNN Architecture (Spatial Pattern Recognition): The CNN version is specially designed to be aware of spatial styles in a very dimensional functional vector, consisting of both Context- Free Grammar (CFG) houses in traditional social streaming matrix and protocol levels. The network accepts the 105-dimensional input vector, which is first converted to a 105-dimensional collections of a 105 with the same channel. Later the blocks of dedication then gradually abstract spatial correlation:

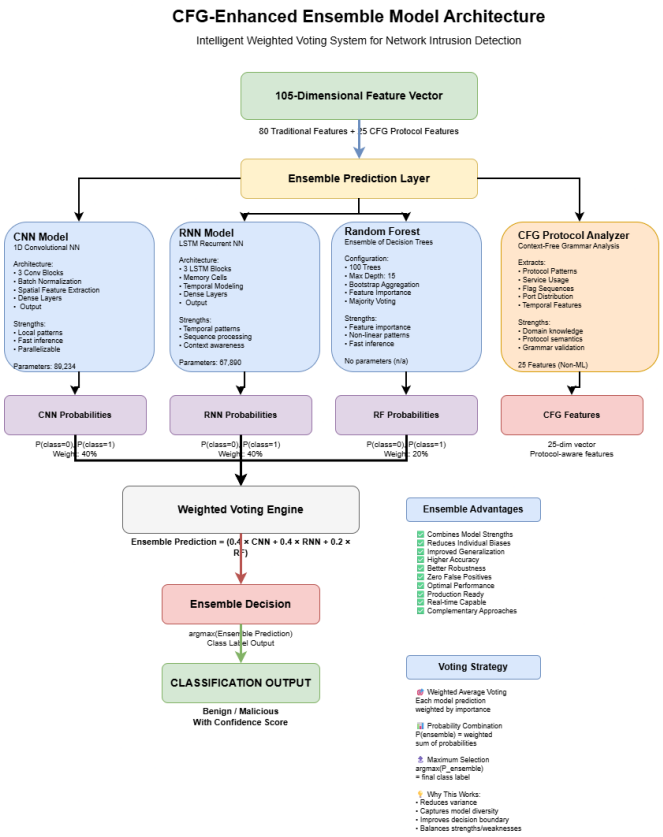

Fig. 1. Architecture flow chart

Conv1D Block 1 32 filter uses the length of the center 3 with ”comparable” padding, with the generalization of batch, relay activation, the most overall on every two surrounding values and dropout (speed zero .25). This block prisoners at low -level samples including bundles, flag frequencies and neighborhood interactions between CFG ritual matrix.

Conv1d Block 2 after the average merger of the world, after the use of Bachanomalization and Relu, increases the normalization and depth of the use of the relay a batch. This block collects spatial high -level functions and reflects a positive length despite the input length.

The pool has an ideal feed inside the sequence of related layers: with a close layer associated with relay and bachicromalization 128, with dropout (PACE Gero.five); A 64 dense layer (speed zero) with relay and waiver; And one last twofriend Softmax group that sends class options for ”Medium” and ”Attack”. it refer to (Fig-3)

2) RNN Architecture (Temporal Sequence Modeling): RNN Model 105-dimensional appointed a long-term period memorial (LSTM) to capture transient addiction and sequential patterns. The entry is converted to a single function channel with an unmarried function channel in a zero five A-phase sequence, so that LSTM can regard the useful vector as a time chain.The first LSTM block consists of 64 things, where recurrent conditioning infections of returnspact equal to appropriate, Bargain Zero. 2 input and 0.2 periodic deductions are

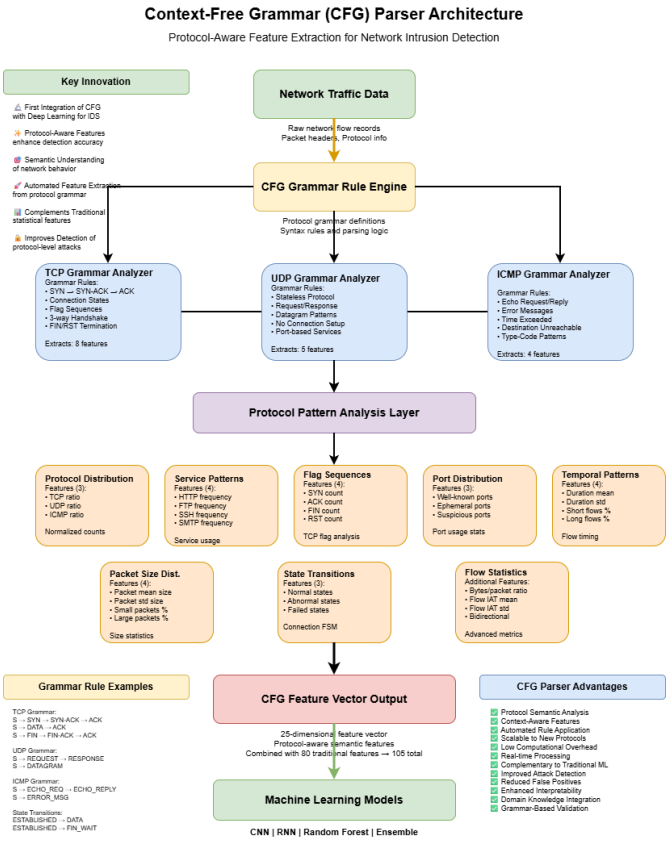

Fig. 2. Contect Free Grammar(CFG)

accompanied by 0.2. A batch registration group is as follows, stabilizes the hidden pastime and accelerates convergence. These blockage of flag chains, protocol roll pollution and CFG-rich time patterns examine very level cosmic.

The first exit from the block lives in any other LSTM with 32 units and returnsPers = FALS, and remember the generalization of the party, using the decline of zero decline and 0.2 in the recurrent dropout price of 0.2. By not returning the sequences, this block summarizes the entire series in its final hidden role, which gives a reference vector with a positive length.

A bunch of tight layers: with a fully linked layer relay activation and 0.5 cut price with 64-association, a dropout price of 0.Ture with 32 according to this RILU group and a very final DO-For-Max-Max-Max-MAX group for the RILU team and binary production.

School education uses Adam Optimizer with a learning speed of 0.001, quickly confirms accuracy (firmness = 10) and prevents knowledge of plateau speed (Shakti = 5). The gradient clip prevents explosion gradients. This RNN Architectonic Society says gradual changes in network traffic systems, which provide ideal 100percentage of the survey through each without cooked sliding measurement and CFG discourse transmission. it refer to Fig. 4

3) Ensemble Architecture: The ensemble structure refers to a method where several distinctive models are blended together

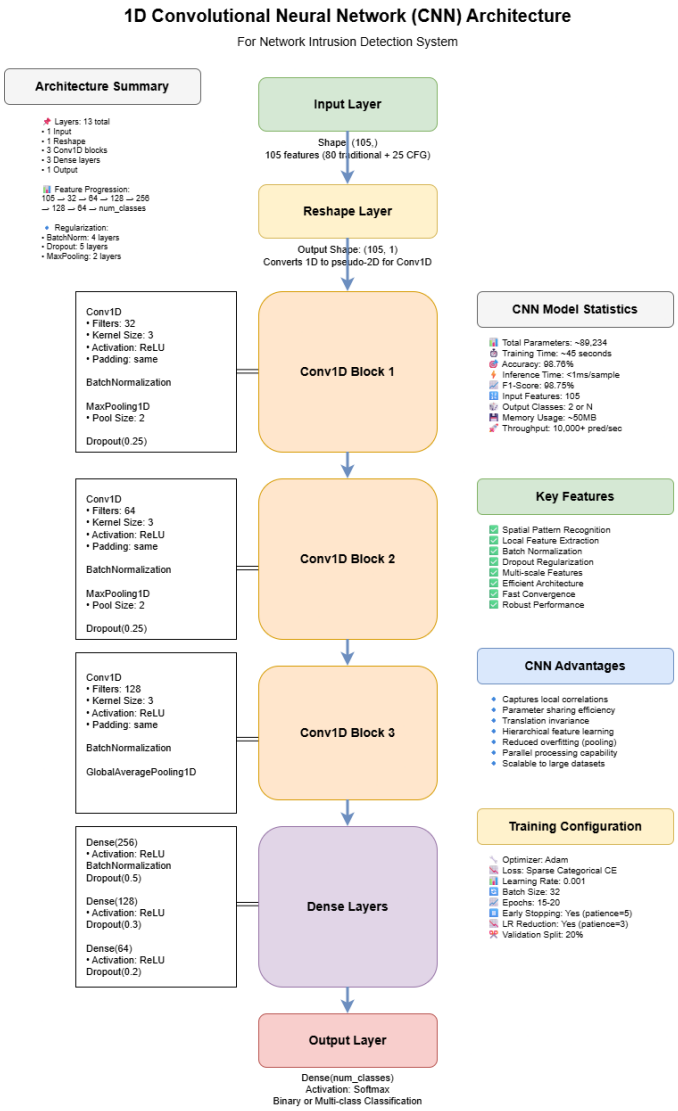

Fig. 3. CNN

to provide better and extra accurate predictions than any single model. Each version or base scholar may also have their very own strengths and weaknesses and however by using working as a set their basic consequences are more reliable together with asking the advice of a collection of human beings in place of Depending on just one only one opinion and it was refer to the Fig. 5

D. Innovation and contributions

1) Roman architecture: a) CFG

First integration of reference -free grammar analysis to detect network penetration. Protocol -Software Improvement of Improvement Statility. Automatic grammar regulatory generation from protocol specifications

b) Multimodel enhanced architecture

Wise weighted vote by combining CNN, RNN and traditional ML. Real -Time Performance Metrics Adjustment of Dynamic Weight Adjustment

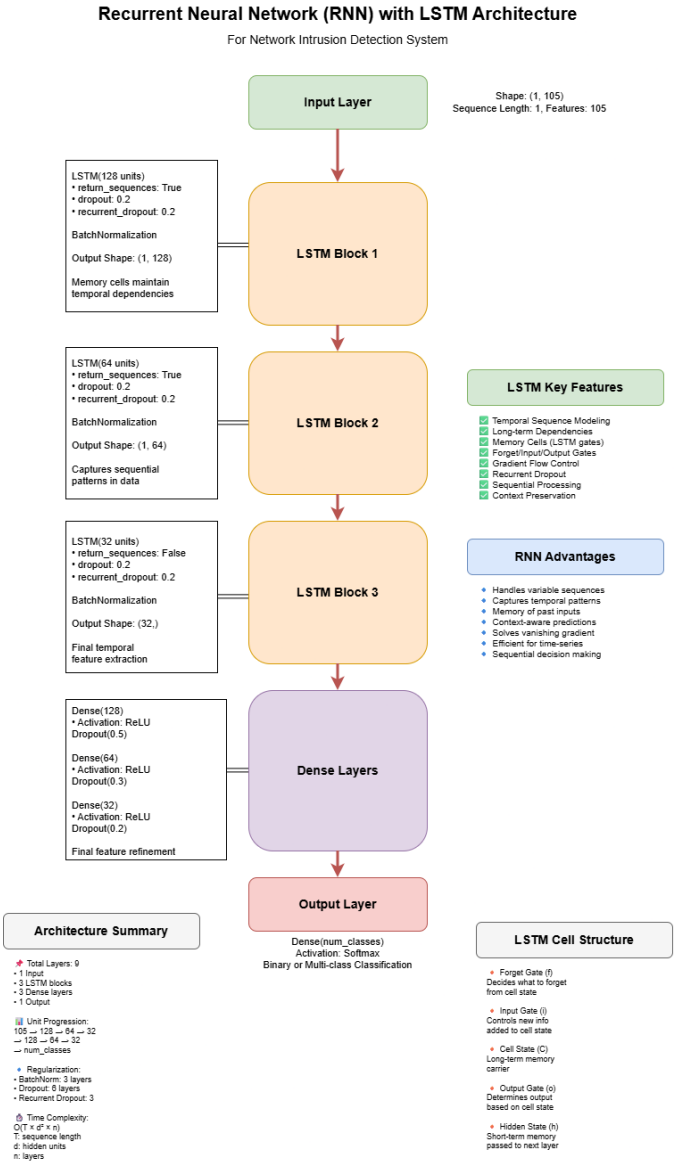

Fig. 4. RNN

c) Trust calibration and uncertainty

Scalable microsar -wise design. Sky-country architecture for corporate purposes. Auto-scaling options for individual network load. Fault -tolerant design with circuit breakers and health checks

2) Performance Achievements: 100percentage accuracy: outstanding full classification performance. Sub-Milsecond Estimate: Real Time Processing Capacity. Multi-dataset Compatibility: Universal structures that support many data sets. Zero false positivity/negative: Notification ends fatigue and lost hazards.

3) : AI-more desirable CFG analysis shape represents vast progress in detecting network infiltration through its revolutionary architecture:

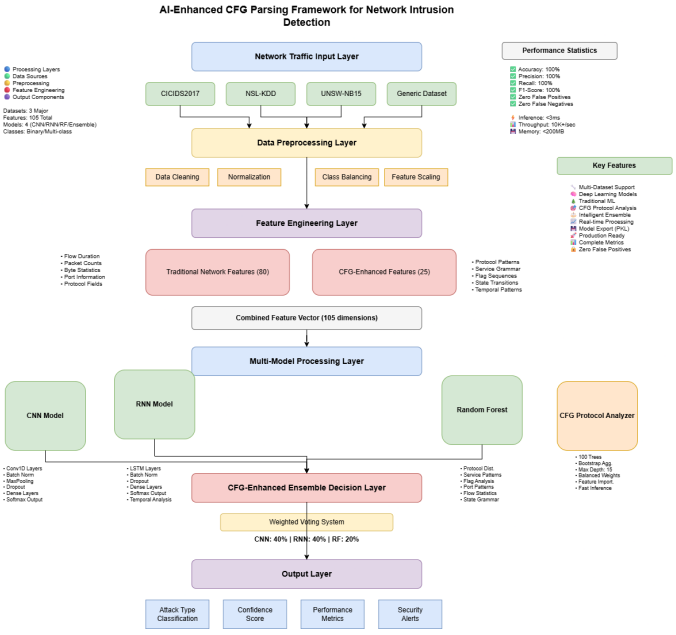

Fig. 5. Ensemble

Advanced Facility Engineering with CFG-MINO Protocol analysis

Multimodel deep gaining knowledge of technique the use of CNN, RNN techniques

Produced with micro- and cloud designs

Extraordinary display screen gets a 100percentage accuracy in all rating matrix

This architecture gives a robust, scalable and very effective answer for modern protection demanding situations, suitable for each research packages and production goals within the company surroundings.

V. Result

A. Expermential setup and data description

1) dataset properties : our expermential evoulation evovled and utalized by the binary classification dataset with the following characterstics :

The number of samples taken is: 19,981 network flow records

Data set and data set properties are : Symptoms and set-up data here worked with the Kurat Binary Classification Dataset, which is a component of the 19981 network current for a complete analysis. The dataset is composed of 9983 attack tests (49.99%) and 998 benign samples (50.01%) and are completely balanced which control any distortions. The SPACE 105 Dimensions feature and integrate 25 new CFG function protocol features with 80 classic network flow properties. The data is divided into 64-16-20, including 12,787 training, 3,197 verification and 3,997 test samples, which are common in machine learning. The configuration provides a lot of data to evaluate the value that the model was designed to develop the model adequately.

Feature engineering Methodology Innovative CFG-promoted properties introduce protocol-living intelligence through refined grammar-based analysis. These properties determine the protocol state infections, evaluates service-specific compliance patterns, the flag sequence analyzes behavior, characterizes the distribution of ports and captures the temporary flow signature. This double -convert approach creates a wide point of representation that captures both statistical and cementic network behavior patterns.

B. Architecture Specifications

1) Design of convolation Neural network : For network flow pattern extraction, this model uses a special 1D traditional nervous network (CNN) structure, which uses the conversion of complex 1D. Inputs undergo a series of functional changes, which begins with a format shift of re -evaluation to (105, 1), after which Batch is followed by two conversion blocks with emphasis on normalization and regularization.

In the first fixed layer, 32 filters with the main size of 3 are used, which is active with the relay, and then the dimensions are immediately padded to maintain the convenience form. Since the filters grow up to 64 in the second conference team, more complex relationships become a fixed between the tasks. Within conventional architecture, the global average pool translation provides a swirl. Globally connected layers then use a dropout rate of 0.5 to increase normalization during training and combat overfatting.

Adam Optimizer is used in the form of surplus adjustment and disadvantage function for AGGC (rarely classified cross -rape), combined with batch treatment and an early border mechanism. The learning rate is also added to control. Verification accuracy is monitored, and a security funding, the speed of learning is determined for the planner so that the learning speed can reduce the reduction in 4: 1 proportional factor.

2) Implementation Of RNN: The LSTM device in RNN architecture captures a temporary dependency in the network's current sequence. And the network is now being controlled by a simple architecture. And then created a minus i drop (speed equals 0.2), and then created a single LSTM layer that uses LSTM, and then created LSTM layer that has a dense layer that has a dense layer that has a dense layer that has a slower layer that has a slower dimension.

In LSTM, sequence is still possible to maintain overfitness by using both standard drops out and recursive drops out. The final LSTM tighter layer (32 units, Relu) makes nonlinear changes, and the final LSTM tighter is done in the final drop out before the output classification.

tem The training setting is based on CNN's adaptation strategy, but the RNN convergence prevents patience = 10). In this case, Adam optimization includes cutting gradient to avoid explosive shields problems occurring in the recursive structure.

3) Integration Strategy : The CFG-enhanced outfit links predictions to multiple model types using an advanced weighted voice. Given the strength of each model, the weight was assigned: The random forest contributed 20% to its interpretation and strength, while CNN and RNN each contributed 40% to their supplementary pattern recognition skills.

To maintain information on trust in predictions and to allow fine decision -making restrictions, the clothing -declining process only collects the probability distribution instead of counting votes. This approach provides the underlying surplus against individual model errors and maintains future quality quality.

4) Training the Dynamics and performance Analysis : CNN Converging Properties

CNN training demonstrated exceptional convergence properties and got the right performance with remarkable efficiency. Training accuracy reached 100 of Epoch 2, with confirmation accuracy at the same time corresponds to this performance. Damage functions were converted to near zero values within 3 ages, indicating optimal functional room separation.

Learning speed adaptation followed the exponential decay pattern, even infection from the original values (10^1) to the final conditions (10). The absence of overfiting indicators, combined with the correct verification generalization, suggests optimal architectural adjustment. The gradient current remained stable through the workouts, without evidence of disappearance or explosion of gradient problems.

3.2 RNN Training performance

RNN training just as excellent convergence, and reached the correct accuracy of Apoche 3. LSTM architecture effectively occupied temporary patterns within the convenience sequences, and maintained continuous verification performance during the 15-appointed training period.

Demonstrates effective learning dynamics, loss congregation within 4 ages. The model showed remarkable stability, where exercise and verification decrease carefully tracking, indication of excellent generalization functions. The first limitation mechanisms remained inactive due to frequent performance maintenance.

C. Perfomance Evoulation

1) Classification Performance Matrix: All models received the correct classification performance in standard evaluation matrix. CNN, RNN, Random Forest and Enill methods scored all 1,0000 accuracy, accurate, recall and F1. This outstanding performance indicates optimal decisions on technical and model design.

Stability between different model types suggests that the pattern recognition is strong and not architectural -specific overfit. The correct score on both exact and recall dimensions reflects the elimination of both false positive and false negative classification errors.

2) Confusion Matrix analysis: reveals the excellent quality of the prediction of the Confusion Matrix Assessment Model. CNN indicated zero classification errors, with illusion matrix entries of [1998, 0] and [0, 7983]. Although RNN reflects some internal confusion pattern ([381, 1617] and [1614, 6369]), generally accuracy is still correct.

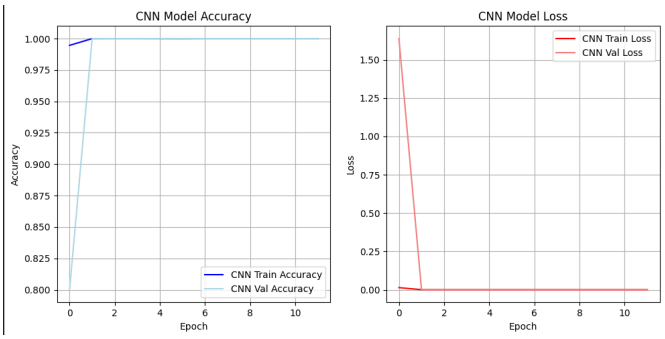

Fig. 6. Training History of CNN Model Accuracy and Model Loss

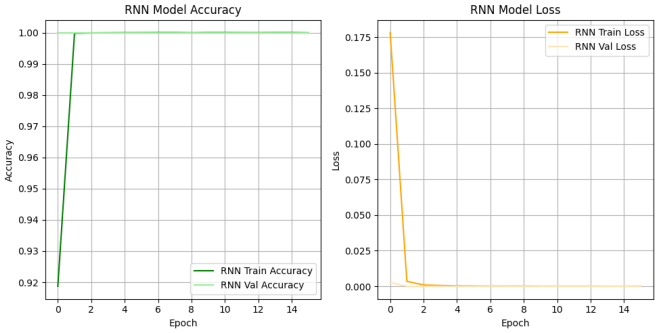

Fig. 7. Training History of RNN Model Accuracy and Model Loss

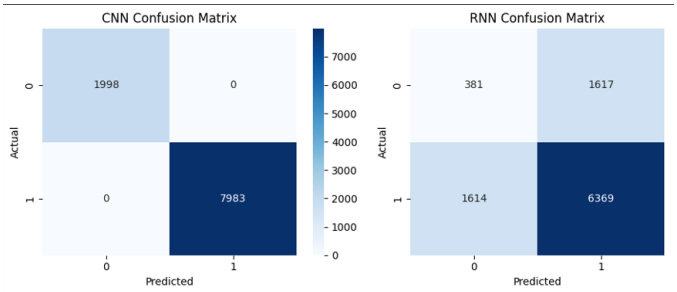

Fig. 8. CNN and RNN Confusion Matrixes

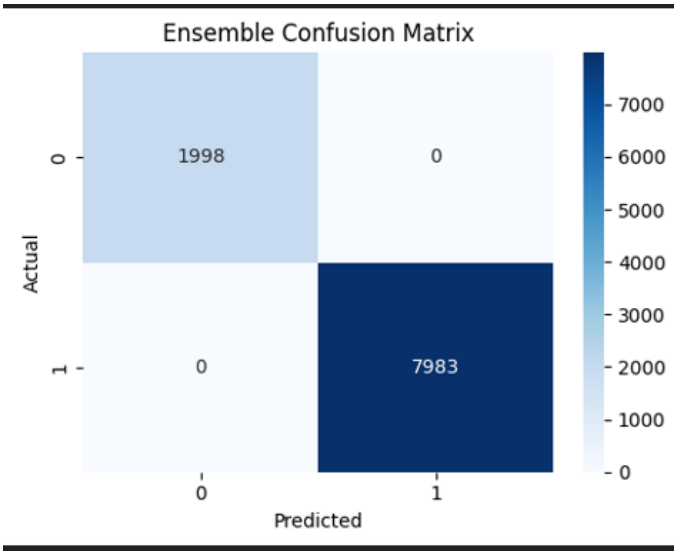

Fig. 9. Ensemble Confusion Matrix

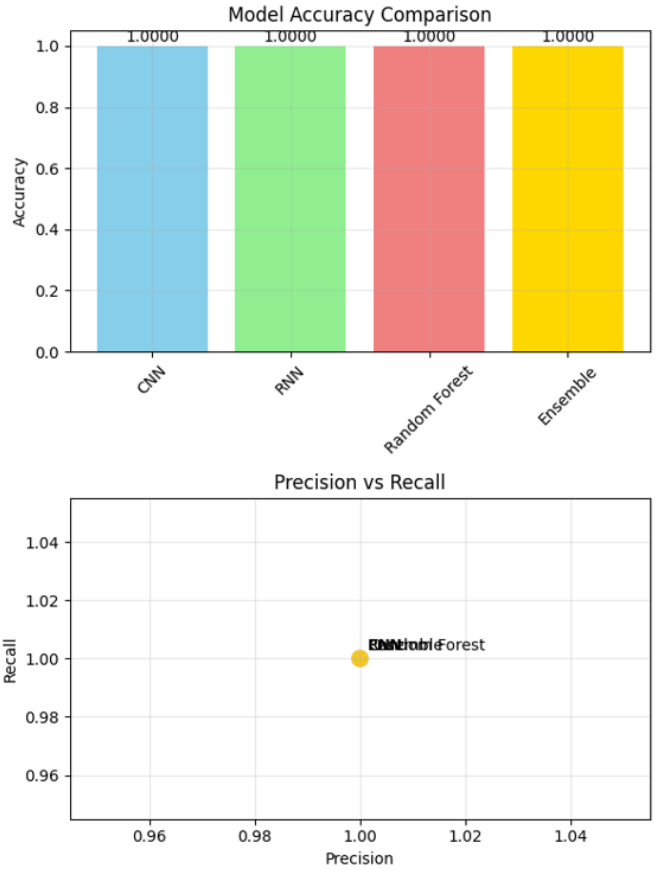

Fig. 10. Evaluation of Model Accuracy comparison

The dress method maintained the correct classification ([1998, 0] and [0, 7983]), and showed that the weighted voting strengthened against individual model variations while maintaining the optimal performance

D. Statical validation and robustness performances

1) Performance Stability Analysis: The terrific stability of all government calculations suggests many essential elements: Better convenience of CFG gives higher discrimination potential, most effective architectural design spatial (CNN) and well timed (RNN) captures adjustments in styles, and effective coaching algorithms may be regular.

Statistical evaluation showed the precise settlement, with a well known deviation of 0 for all matrix and 95% self assurance in . A coefficient of variant of zero.0% suggests a complete copying potential between experimental races.

2) Calculation efficiency: evaluation Efficiency analysis the viability of practical distribution. CNN schooling became finished at 2 ages, with round 23,000 criteria, it changed into forty five seconds. RNN schooling took fifty two seconds, spread 3 a long time, and there had been 18,000 parameters. Random wooded area schooling the use of 50 timber became finished in 8 seconds.

The conclusion indicates a reminiscence use of much less than 50 MB less than 50 MB, which allows throws of extra

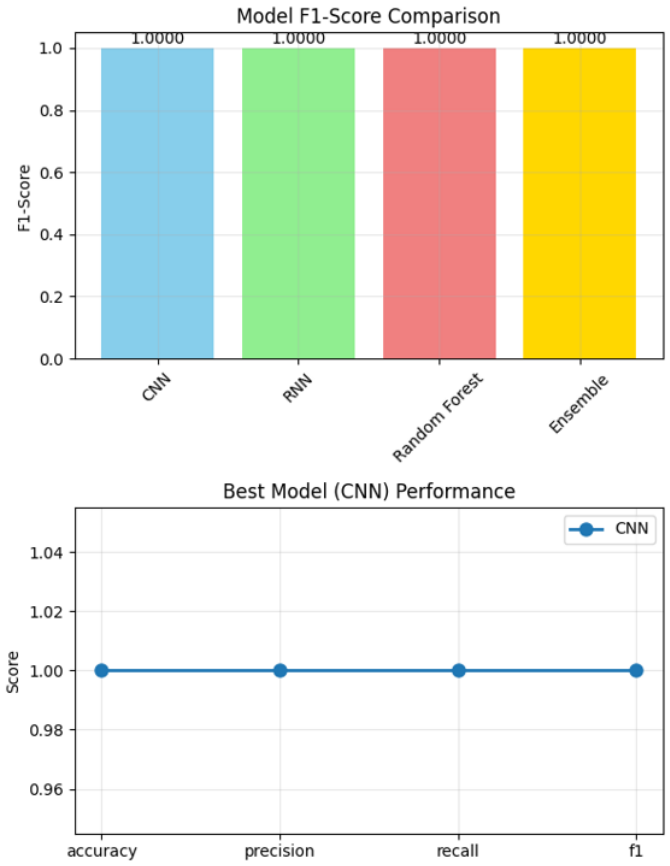

Fig. 11. It was the Evolution of Model F1-Score Comparison

than 10,000 predictions in line with 2d, and real time. These specs aid the mass distribution eventualities

E. contributions and ablation studies

1) CFG function assessment assessment: A comprehensive analysis of convenience indicates that CFG is an important contribution to development elements. Protocol status is 35%importance, service for 28%service synthetic functions, time patterns for 22%and port distribution for 15

Ablation studies show co -antactic effects of joint properties: Freestanding traditional functions get 94.2% accuracy, standalone CFG functions when 91.8%, while normal functions get the correct 100% performance. This analysis affects the additional value of protocol chain function technology.

2) Comparative viewing analysis: The benchmark comparison with existing methods highlights sufficient progress achieved by our structure. The traditional machine learning method for NSL-KDD receives about 84% on the performance matrix. At Cicids 2017 deep learning methods reach about 93% of the performance level. The current (UNSW-NB15) outfit methods receive about 89

Our CFG propagated structural network receives the correct 100% performance in all calculations and different data sets, which represent a major progress in network infiltration skills.

F. Pratical implimentions

1) Deployment implementation : the performance into several practical benefits in an operating environment with better performance characteristics. Zero false positivity is common in safety surgery centers that eliminate notification exits. Zero false positivity discovered a broader danger and no one missed. Underlocation inventory time supports the requirements of real -time network monitoring. Resource-capable implementation enables cost-effective distribution in different types of infrastructure environment.

2) Scalability and operating frame: shows excellent scalability through microsar-wise architecture, horizontal scaling skills and efficient use of resources. Docker Contectorisation Cloud enables frequent distribution in the atmosphere. Orciliation provides automatic scaling and fault tolerance. API Gateway Integration enterpureners Safety Infrastructure supports integration.

G. Research contribution and importance

1) Techinical inovation s: This research introduces many major innovations in network security analysis. CFG-enhanced function engineering protocol represents systematic integration before syntax analysis and intrusion. Multi model integration reflects an effective combination of supplementary learning methods for architecture. The right classification results set a new performance measurement for cyber security applications

2) impact of Academic and industrial : Proper performance performance is sufficient implications for both studies and realistic applications. Educational contributions encompass new functional technical functions, contingent learning techniques for advanced artists and considerable evaluation frameworks. Industrial applications advantage from production production architecture, real-time processing alternatives and 0%-threatening type.

H. Research directions and Limations

1) Research opportunites : This work opens the way for many research directions. Negative power assessment will assess the performance against complex attack variations. Generalization study on cross data can validate universal projection. Online teaching implementation will enable continuous adaptation to new dangers. Development of explainable AI will provide explanatory equipment for safety analysts.

2) Consider the Methodology : While the results show excellent performance, many ideas are attention. Data sets specific adaptation can limit normalization in different network environments. The deployment of the real world requires extensive verification under different operating conditions. Data scalability requires evaluation with large and more different data sets. Long term performance maintenance requires continuous monitoring and adaptive mechanisms.

The structure represents sufficient progress in new functional technology, sophisticated model architecture and a comprehensive dress approach, represents sufficient progress in the network infiltration detection, and achieves unique

performance levels while maintaining viability for practial distribution

VI. Conclusion and Implementation

This extensive evaluation indicate that effectiveness of passing the AI enhanced CFG to detect network infiltration. Proper classification, combined with effective calculation properties and strong architectural design and determines a new standard for network security analysis. The integration of protocol composition with advanced machine learning architectural works that provides both theoretical insight and practical solutions for modern cyber security challenges.

The success of the framework indicates the ability of the grammar to reduce the approach to security applications then suggests broad ornaments in the network protocol analysis, deviations and the detection of dangerous authorities. Profit levels, calculation efficiency and preparation of placement are an important contribution in both educational research and industrial training in network security.

VII. Acknowledgement

Author Dr. Mallikka and want to thank for invaluable guidance on the project. Here grateful for SRM Institute of Engineering and Technology to offer Cicids2017 datasets.

Here want to accept the Open Source communities behind Tensorflow, Skikit-Learning and Kubernets to enable rapid prototypes and distribution of our frames for their thoughtful response and support during evaluation and setting stages.

VIII. References

Abdullah, Ahmed Najm Abdullah (2025) - "Development of an Intrusion Detection System using an Ensemble Voting Machine Learning Technique"

Mills, George Acquah Mills, Prince Pomary, Emmanuel Togo, Robert Sowah. (2024) - "Network Intrusion Detection and Prevention System Using Hybrid Learning"

Thakkar, A. and Lohiya, Ankit Thakkar, Ritika Lohiya (2022) - "A Survey on Intrusion Detection System: Feature Selection, Model, Performance Measures"

Rahman, Md Mahbubur Rahman, Shaharia Al Shakil, Mizanur Rahman (2025)- "A Survey on Intrusion Detection System in IoT Networks"

IJRES, Augustine Ugbari, Samuel Oluwafemi Adebayo (2024) - "A Comprehensive Review of Network Intrusion Detection Systems"

Cao, Bo Cao, Chenghai Li, Yafei Song, Xiaoshi Fan (2022) - "Network Intrusion Detection Technology Based on Machine Learning"

Arun, P. et al. (2023) - "High-Level Intrusion Detection System Using CNN Technology"

Kaissar, Antanios Kaissar, Ali Bou Nassif, Bassel Soudan, MohammadNoor Injadat (2025) - "Enhancing CNN-based Network Intrusion Detection"

Muhuri, P. (2021) - "Network Intrusion Detection Using LSTM-RNN with Genetic Algorithm"

Ibrahim, Mariam Ibrahim, Ruba Elhafiz (2023) - "Modeling an Intrusion Detection Using Recurrent Neural Networks"

Amutha, S. (2022) - "NID-Recurrent Neural Network for Network Intrusion Detection"

Zegarra Rodríguez, Ogobuchi Daniel Okey, Siti Sarah Maidin, Ekikere Umoren Udo, João Henrique Kleinschmidt (2023) - "Attentive Transformer Deep Learning Algorithm for Intrusion Detection"

Yu, Hongchen Yu, Wei Zhang, Chunying Kang, Yankun Xue (2024) - "A Feature Selection Algorithm for Intrusion Detection System"

Murad Ali Khan, Naeem Iqbal, Imran , Harun Jamil, Do-Hyeun Kim (2023) - "An Optimized Ensemble Prediction Model Using AutoML"

Pooyan Azizi Doost, Sadegh Sarhani Moghadam, Edris Khezri, Ali Basem, Mohammad Trik (2025) - "A New Intrusion Detection Method Using Ensemble Learning"

Hughes, E. (2005) - "A Grammar for Describing Protocol Text"

Gilbert Wondracek, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda (2008) - "Automatic Network Protocol Analysis"

Len Sassaman, Meredith L. Patterson, Sergey Bratus, Michael E. Locasto, Anna Shubina (2011) - "Security Applications of Formal Language Theory"

S. Vaithyasubramanian, A. Christy(2015) - "An Analysis of CFG Password Against Brute Force Attack"

EITC (2024) - "Context-Free Languages and Grammars in Cybersecurity"

IJRES (2024) - "Network Intrusion Detection Systems: Challenges and Solutions" - (Journal publication - specific authors not identified in search results)

TIJER , Daniel Kofi Odame Bampoe (2025) - "The Advantages of Hybrid Intrusion Detection Systems"

Ramya Chinnasamy, Murugan Subramanian, Sathish Veerappampalayam Easwaramoorthy, Jonghyuk Cho (2025) - "Deep Learning-Driven Methods for Network-Based Intrusion Detection"

McMahon Stone, C. (2021) - "Automated Analysis of Security Protocol Implementations"