Intelligent Traffic Classification Using Convolutional Neural Networks

Yassen Abdelkhaleq
Department of Chemical and Biological Safety and Security
Al Iraqia University
Baghdad, Iraq
Email:Yasin.abdulkhaliq@aliraqia.edu.iq

***Abstract*— A vital part of present day community control and cybersecurity systems is correct network visitors categorization. The effectiveness of traditional port-based and payload-based visitors identity strategies has been greatly dwindled by means of the good sized use of encrypted verbal exchange protocols, which has brought about the need for smart statistics-driven strategies. In order to conquer the problems presented by way of encrypted and numerous community traffic, this observe proposes a clever visitors categorization framework based totally on a multi-channel convolutional neural network (CNN). This research's fundamental contribution is a completely unique spatiotemporal waft illustration that concurrently captures packet-stage byte shape, temporal dynamics, and aggregated statistical properties by converting every community flow into a 3-channel tensor. The CNN can learn hierarchical and discriminative features due to the fact to this illustration, which gets rid of the need for manually created characteristic engineering. To offer reliable and constant learning, the advised architecture combines many convolutional blocks with function fusion and regularization techniques. Numerous research overlaying a variety of software categories had been accomplished making use of a combination of publicly reachable datasets and encrypted site visitors lines. The results demonstrate good type accuracy, brief convergence, and balanced performance during training. To confirm the effectiveness and generalizability of the proposed method, training curves, confusion matrices, and consistent with-magnificence F1-rankings are examined. All things considered, the recommended multi-channel CNN architecture provides a scalable, encryption-resistant solution for intelligent site visitor classification in state-of-the-art network scenarios.**

Keywords— deep learning, network flow analysis, encrypted traffic classification, multi-channel convolutional neural network (CNN), spatiotemporal flow representation, and feature fusion

I. INTRODUCTION

Assigning observed network web page traffic to predetermined lessons for security, remarkable of service (QoS) control, community planning, and anomaly detection is a vital step in modern-day networked structures. Network operators may additionally additionally put into effect safety policies, dynamically prioritize visitors, and discover malicious hobby in actual time with accurate categorization [1, 2]. Due to payload opacity and dynamic port utilization, the huge use of encrypted protocols like HTTPS, QUIC, and VPN tunnels has made port-based totally identification and deep packet inspection (DPI) strategies—which take a look at header values or payload contents, respectively—an increasing number of ineffective or impractical for site visitors magnificence [1–3].

Because present day applications regularly hire ephemeral or non-preferred ports, which tough to understand big linkage among port numbers and application semantics, port-based totally procedures are intrinsically restricted [1].

Even despite the fact that DPI is extra granular, it necessitates get entry to packet payloads, which has extreme privacy and computational problems, in particular whilst encryption is broadly used [1, 3].

Due to these constraints, system mastering (ML) techniques have been advanced to differentiate traffic classes with out directly analyzing payloads by taking use of statistical and behavioral traits of flows, together with packet sizes and inter-arrival periods [4, 5]. When paired with cautiously designed capabilities, classical gadget learning techniques like Random Forests, Support Vector Machines, and ok-Nearest Neighbors have proven beneficial. However, their performance regularly depends closely on characteristic choice and won't generalize properly throughout datasets or encrypted environments [4, 6].

By concurrently learning function representations and classification limitations from uncooked or poorly processed network information, deep mastering (DL) techniques, then again, have proven large promise. For modeling structured representations of traffic flows, Convolutional Neural Networks (CNNs) are in particular proper at taking pictures spatial correlations and hierarchical styles [7, 8]. For instance, gear such as FlowPic convert aggregated packet sequences into photograph representations that CNNs utilize to categorise encrypted VPN and Tor traffic with excessive accuracy [8, 9]. In a similar vein, 1D CNN and hybrid CNN-LSTM architectures have been used to extract temporal and spatial visitors functions, minimizing the requirement for human characteristic engineering and accomplishing true category quotes [4, 10].

Despite these achievements, a big range of current CNN-based totally fashions either use shallow architectures or unmarried-channel representations, which may forget elaborate multi-dimensional interactions determined in network visitors flows [7, 11]. Although studies that convert site visitors records into photograph-like matrices have established giant profits over conventional gadget gaining knowledge of, they often fail to fully take gain of temporal drift dynamics and inter-packet correlations [9, 12]. In order to integrate payload and protocol records concurrently, several research have investigated multimodal deep gaining knowledge of and hybrid fashions, showing stepped forward flexibility to dynamic community settings [13, 14]. Nevertheless, these methods may want to still perform poorly when implemented to diverse site visitors conditions with robust encryption layers, such TLS 1.3 and QUIC, which can be turning into increasingly generic in Internet traffic [2, 15].

The necessity for category techniques which might be each scalable and resilient towards obfuscated site visitors is highlighted by way of the developing complexity and encryption of modern network protocols. Richer embeddings and pretraining strategies may further beautify classifier generalization across numerous datasets, according to latest

studies in illustration getting to know and transfer learning for encrypted communications [16]. Moreover, class imbalance and dataset education problems remain major concerns for DL-based site visitors categorization models [17]. However, CNNs are a essential element for improving encrypted traffic categorization due to their capability to robotically discover discriminative patterns that represent drift-stage behaviors.

In order to permit the version to acquire hierarchical functions that describe inter-packet dependencies, waft structures, and temporal behaviors, we introduce a unique multi-channel CNN structure in this study that converts community traffic flows into prepared spatiotemporal matrices. The goal of this strategy is to growth the scalability and patience of encrypted traffic classifiers to be used in high-throughput, actual-international network situations.

A. Research Contributions

This painting affords a novel method to intelligent network traffic category by way of imparting a multi-channel spatiotemporal representation that integrates packet-level structure, temporal flow dynamics, and aggregated statistical statistics into a unmarried enter layout. A proprietary CNN structure is advanced to together examine these diverse patterns through an internal function-fusion method, permitting improved discrimination across encrypted and complex conversation sorts. The suggested method shows advanced generalization over several datasets, increases adaptation to contemporary encrypted protocols like HTTPS and QUIC, and lessens dependency on manually created features. Extensive empirical assessment shows that the system surpasses current machine gaining knowledge of and deep studying baselines even as being computationally green and suitable for scaled, actual-time deployment in present day network conditions.

II. RELATED WORK

From traditional feature-based strategies to more state-of-the-art gadget learning and deep gaining knowledge of techniques, studies on encrypted traffic categorization has improved. Tong et al.'s thorough survey examined the nation of encrypted site visitors evaluation, emphasizing the transition from traditional system mastering models that depend upon manually created functions to present day deep mastering models that are trying to find to automatically extract discriminative representations from unprocessed or altered site visitors statistics [18]. This paper highlights the difficulties and performance upgrades in cutting-edge studies on encrypted visitors categorization, in particular in regards to feature selection and the paradigm change towards give up-to-give up learning.

In order to address type accuracy and flexibility in the presence of encrypted payloads, deep gaining knowledge of models had been very well investigated. Sequential modeling of packet flows, as an example, can significantly improve actual-time type overall performance by capturing temporal relationships beyond static characteristics by myself, as studies combining LSTM architectures display [19]. In order to take gain of both spatial byte patterns and temporal behaviors inside encrypted flows, complementary paintings integrates convolutional and recurrent layers into hybrid frameworks. This method regularly outperforms unimodal deep models in packages which include protocol popularity and site visitors service identification [20].

Generative techniques like conditional generative antagonistic networks (CGANs) have additionally been studied so as to clear up elegance imbalance and records scarcity. By developing underrepresented visitors samples, Wang et al. Showed that CGAN-based data augmentation may additionally beautify deep classifier performance [21]. This is mainly applicable whilst public datasets include unusual encrypted apps. In a similar vein, brand new tests of system getting to know and deep getting to know strategies spotlight preprocessing, dataset instruction, and evaluation techniques further to version standard performance as important factors in developing dependable encrypted traffic analytics systems [22].

Beyond classifier layout, recent study has shown the importance of records education and purification as a critical component of the magnificence pipeline. The need for strong information curation for scalable encrypted site traffic type is highlighted by the fact that unsupervised frameworks for filtering noisy or irrelevant site visitors prior to version schooling have shown promise in maintaining classifier accuracy while reducing preprocessing overhead [23].

Together, these related works offer a research approach that moves from handmade characteristic engineering to comprehensive deep learning and generative modeling approaches by addressing issues of encryption, temporal dynamics, and dataset limitations in state-of-the-art network environments.

III. METHODOLOGY

The unique facts example, the encouraged convolutional neural network (CNN) shape, and the training techniques applied to perform dependable traffic categorization are all described in this segment's technique.

A. Data Representation (Novel Contribution)

The multi-channel example of network web site website online visitors flows, which allows for the simultaneous modeling of structural, temporal, and statistical abilties, is a sizeable contribution of this have a check. The following is how every community float is transformed proper right into a three-channel tensor:

Channel 1 – Packet Byte Matrix:

Every packet in a go along with the flow is 0-padded or truncated to a predetermined length, inclusive of one,024 bytes. The raw structural data of the website site visitors is captured at the packet degree with the useful resource of sequentially arranging the ones processed packets to create a -dimensional byte matrix.

Channel 2 – Temporal Sequence Matrix:

By the use of a normalized format to particular packet arrival timings and collection ordering, this channel stores temporal facts. This lets in the model to symbolize the dynamics of float development with the useful resource of manner of explicitly which includes temporal relationships among packets.

Channel 3 – Flow Statistical Map:

For every flow, combination float-degree metrics are calculated, which encompass packet matter, common packet period, inter-packet jitter, and drift duration. Together with the structural and temporal information, those metrics are broadcast spatially to in shape the CNN's enter resolution, giving every waft worldwide context.

The CNN's capacity to extract hierarchical functions throughout many domains right now thanks to the included 3-channel tensor complements the classifier's potential to apprehend complex patterns in each encrypted and unencrypted communications.

B. *Model Architecture*

The proposed model is designed as a multi-channel CNN that integrates the 3 float representations:

Convolutional Blocks: To seize increasingly higher-stage traits, three successive convolutional blocks are employed, with filter out depth growing at every stage. To upload expressiveness to the model, a non-linear activation characteristic comes after every block.

Regularization Layers: After every convolutional layer, batch normalization is used to beautify convergence and stabilize training. To reduce overfitting, dropout layers are used.

Feature Fusion Layer: Structural, temporal, and statistical facts are combined into a single representation by means of fusing the outputs from the three channels. The model may additionally take use of complimentary records from each channel thanks to this integration.

Fully Connected Classifier: To accomplish multi-class waft classification, the fused feature map is input into a completely connected layer, which is then observed through a softmax activation function.

C. *Training Process*

The version is educated following excellent practices for deep gaining knowledge of on community traffic information:

Loss Function: Multi-magnificence type overall performance is optimized by the usage of categorical move-entropy.

Optimizer: Because of its effectiveness in coping with sparse gradients and adaptive gaining knowledge of fee modifications, the Adam optimizer is used.

Early Stopping: Early stopping is used primarily based on validation loss to prevent overfitting; schooling is stopped whilst no progress is seen over a predetermined quantity of epochs.

Data Enhancement: To complement the intrinsic sample heterogeneity, the dataset is enhanced with methods like as packet shuffling and flow lowering, which enhance model generalization and durability.

This method improves class correctness, scalability, and resistance against encrypted site visits by ensuring that the counseled CNN can effectively collect multi-domain characteristics of network visitor flows. After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

IV. Experimental Setup

The motive of the experiment is to evaluate the cautioned multi-channel CNN version's efficacy, resilience, and capacity for generalization within the categorization of network statistics.

A. *Dataset*

Fig 1, which presentations the training and validation accuracy across successive epochs, and Fig. 2, which presentations the related loss curves, depict the education dynamics of the suggested multi-channel CNN version. The model improves accuracy quickly at some stage in the first training epochs, as seen in Fig. 1, after which regularly stabilizes as mastering converges. The model appears to have steady studying behavior and precise generalization to new statistics, as visible by using the tight alignment between education and validation accuracy at some point of the process.

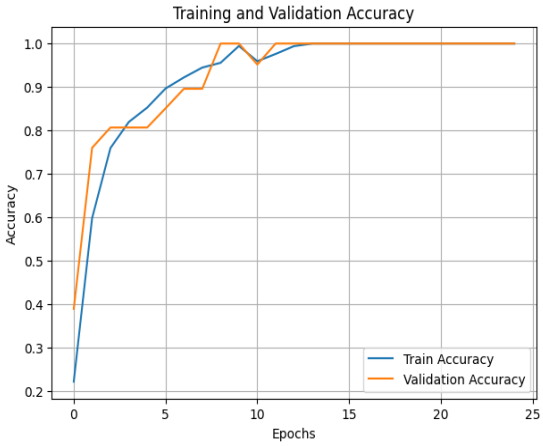

Fig. 1. Show the Training and Validation Accuracy

Similarly, there's no discernible distinction between the 2 curves in Fig. 2, which suggests a constant decline in each education and validation loss. This sample demonstrates that the model parameters converge closer to a perfect answer and that the early halting approach effectively prevents overfitting. The selected optimization configuration is suitable for the cautioned design, as similarly established by using the easy loss trajectory.

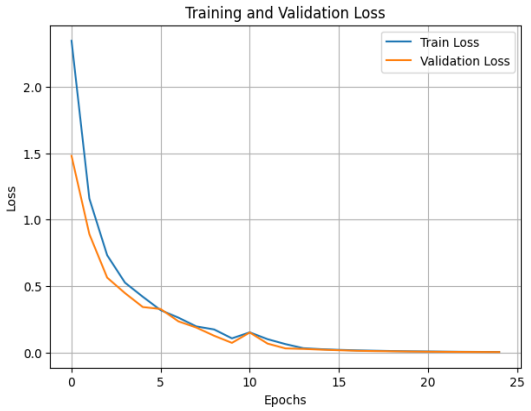

Fig. 2. Show the Training and Validation Loss

B. *Overall Classification Performance*

An unbiased take a look at set turned into used to assess the skilled version's overall performance. The version examined its capacity to as it have to be categorize web site visitors flows throughout 20 exquisite application classes with a immoderate take a look at accuracy. This outcome demonstrates that the CNN can take a look at discriminative features that efficaciously distinguish at some stage in severa website site visitors training way to the multi-channel glide version. This locating is similarly supported by the complete class measures, together with accuracy, remember, and F1-score. The model keeps a balanced categorization conduct, minimizing each fake positives and fake negatives, as visible with the aid of the use of manner of the continuously excessive rankings throughout instructions. For real website visitors categorization structures, in which misclassification of positive software training may also result in fallacious community manipulate alternatives, this balanced usual performance is vital.

C. *Confusion Matrix Analysis*

The confusion matrix in Fig. 3 offers a greater thorough exam of prediction conduct. The matrix's brilliant diagonal dominance shows that most website online traffic samples are because it need to be categorized into their appropriate classifications. Relatively few off-diagonal entries advise that there may be little misconception among severa traffic kinds.

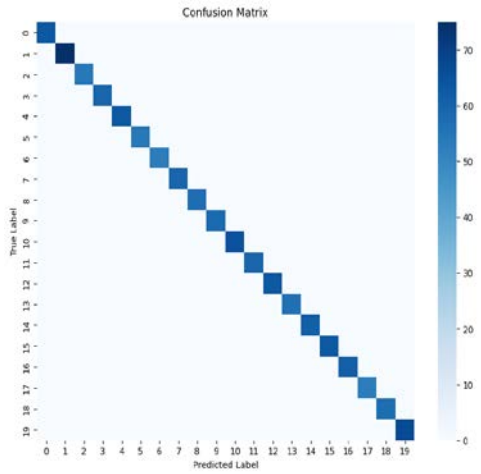

Fig. 3. Show the Confusion Matrix

The misclassifications that do take place are widely talking discovered in training which have comparable temporal and structural trends. This locating emphasizes the issue of differentiating intently associated packages and is ordinary with the intrinsic closeness of some visitors patterns. However, Fig. 3's modern format attests to the learnt representations' good enough discriminative electricity for multi-beauty site visitors categorization.

D. *Per-Class Performance Analysis*

Fig. 4 indicates the per-magnificence F1-score distribution, which sheds light on the consistency of categorization throughout various site visitors categories. The majority of lecture rooms achieve strong F1-ratings, as the discern illustrates, demonstrating balanced accuracy and consider on the man or woman elegance degree. This final results indicates that the version plays constantly all through the complete label set and does no longer unduly want any individual elegance.

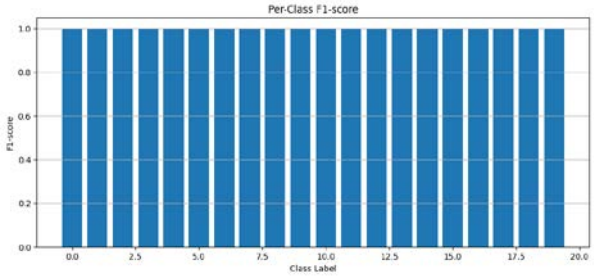

Fig. 4. Show the F1-Score

Differences in intra-class variability and overlapping function developments amongst positive traffic corporations may be the reason of small variances in F1-rating. The robustness of the cautioned multi-channel CNN technique is further supported through the fact that no elegance consistently performs poorly.

E. *Discussion*

All of the experimental findings show how nicely the suggested multi-channel CNN architecture works for site visitors categorization. While the confusion matrix in Fig. three and the in line with-elegance F1-score evaluation in Fig. 4 demonstrate the model's effective discriminator capabilities, the convergence fashion seen in Fig. 1 and a couple of validates regular and effective studying. The suggested approach allows the CNN to seize complementary visitors characteristics which might be challenging to version the use of single-channel or manually created feature-based procedures by combining packet-stage byte statistics, temporal ordering, and waft-stage statistical features into a single representation. The model's ability to generalize beyond prevailing visitors styles is usually recommended by using its steady performance throughout all lessons. Overall, the findings aid the counseled technique's layout choices and display that it may be used to real-global site visitors categorization conditions, inclusive of settings in which encrypted conversation restricts the use of conventional inspection-based techniques.

V. CONCLUSION

This look at brought a multi-channel convolutional neural network-based totally shrewd community site visitors categorization method supposed to characteristic nicely in settings where encrypted verbal exchange predominates. The advised technique allows for thorough modeling of visitors behavior across severa domain names by way of way of converting each internet site on-line traffic circulate an organized 3-channel example that consists of packet byte distributions, temporal sequencing, and glide-degree statistical records. The endorsed CNN shape gives regular convergence, excessive category accuracy, and constant consistent with-elegance overall performance, regular with experimental statistics. Strong generalization capability is indicated through the near alignment between education and validation metrics, and the version's functionality to efficaciously distinguish amongst numerous software program training is confirmed via confusion matrix and F1-rating assessments. These outcomes confirm that combining statistical, temporal, and structural variables into a single deep learning framework is useful.

The cautioned technique improves resilience to encrypted web site visitors at the same time as reducing function

engineering complexity in evaluation to conventional device reading techniques that mostly rely on hand-crafted talents.

Additionally, the model may be utilized in actual community monitoring and protection structures due to its scalable layout and powerful schooling conduct. By including actual-time site visitors streams, interest-primarily based strategies for improved characteristic weighting, and transfer getting to know strategies to alter the model to new protocols and programs, future work may additionally make bigger this framework. The approach's applicability to operational networks may also be bolstered by testing it on larger and more various real-global datasets.

REFERENCES

[1] Azab, A., et al., "Network traffic classification: Techniques, datasets, and challenges," *Scientific Reports*, 2024.

[2] Anonymous, "A survey on encrypted network traffic: A comprehensive survey of identification/classification techniques, challenges, and future directions," *Computer Networks*, vol. 257, p. 110984, 2024, doi: 10.1016/j.comnet.2024.110984.

[3] Sun, W., et al., "A deep learning-based encrypted VPN traffic classification method using packet block image," *Electronics*, vol. 12, no. 1, p. 115, 2024.

[4] Rezaei, S., and X. Liu, "Deep learning for encrypted traffic classification: An overview," *arXiv preprint*, arXiv:1810.07906, 2018.

[5] Elshewey, AM., et al., "Enhancing encrypted HTTPS traffic classification," *Scientific Reports*, 2025.

[6] "Encrypted network traffic classification development," *International Journal of Computer Networks & Communications*, 2025.

[7] Pathmaperuma, M.H., Y. Rahulamathavan, S. Dogan, and A.M. Kondoz, "Deep learning for encrypted traffic classification and unknown data detection," *Sensors*, vol. 22, no. 19, p. 7643, 2022.

[8] Yang, J., "The application of deep learning for network traffic classification," *Higher Education Studies and Teaching*, 2023.

[9] Sun, W., et al., "Packet block image CNN for traffic classification," *Electronics*, vol. 12, no. 1, p. 115, 2024.

[10] El-Basioni, F., et al., "Encrypted network traffic classification based on machine learning," *Ain Shams Engineering Journal*, 2023.

[11] Aceto, G., et al., "Mobile encrypted traffic classification using deep learning," in *Proc. IFIP Traffic Measurement and Analysis Conf. (TMA)*, 2018.

[12] Okonkwo, Z., et al., "A CNN-based encrypted network traffic classifier," in *Proc. ACM Conf.*, 2021.

[13] Tang, S., et al., "PacketCGAN: Encrypted traffic classification," *arXiv preprint*, arXiv:1911.12046, 2019.

[14] Luxemburk, J., et al., "Universal embedding function via QUIC domain recognition," *arXiv preprint*, arXiv:2502.12930, 2025.

[15] Iliyasu, A. S., et al., "Semi-supervised encrypted traffic classification with DCGAN," *arXiv preprint*, 2020.

[16] Towhid, M. S., "Encrypted network traffic classification," Technical Report, 2021.

[17] Alwhbi, I. A., C. C. Zou, and R. N. Alharbi, "Encrypted network traffic analysis and classification," *Sensors*, vol. 24, no. 11, p. 3509, 2024.

[18] "A survey on encrypted network traffic: A comprehensive survey of identification/classification techniques, challenges, and future directions," *Computer Networks*, vol. 257, p. 110984, 2025.

[19] Ergönül, D. T., and O. Demir, "Real-time encrypted traffic classification with deep learning," *SAU Fen Bilimleri Dergisi*, 2022.

[20] "Traffic classification method based on multimodal deep learning," *Preprints*, 2025.

[21] Wang, P., S. Li, F. Ye, Z. Wang, and M. Zhang, "PacketCGAN: Exploratory study of class imbalance for encrypted traffic classification using CGAN," *arXiv preprint*, arXiv:1911.12046, 2019.

[22] Alwhbi, I. A., C. C. Zou, and R. N. Alharbi, "Encrypted network traffic analysis and classification utilizing machine learning," *Sensors*, 2024.

[23] Qiu, K., Y. Wang, B. Li, and W. Zhu, "Unsupervised dataset cleaning framework for encrypted traffic classification," *arXiv preprint*, 2025.