Enhancing Organizational Threat Profiling by Employing Deep Learning with Physical Security Systems and Human Behavior Analysis

D.H. Senevirathna, W.M.M. Gunasekara, K.P.A.T. Gunawardhana,
M.F.F. Ashra, Harinda Fernando, Kavinga Yapa Abeywardena
Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka

***Abstract*—Organizations need a comprehensive threat profiling system that uses cybersecurity methods together with physical security methods because advanced cyber-threats have become more complex. The objective of this study is to implement deep learning models to boost organizational threat identification via human behavior assessment and continuous surveillance activities. Our method for human behavior analysis detects insider threats through assessments of user activities that include logon patterns along with device interactions and measurement of psychometric traits. CNN, together with Random Forest classifiers, has been utilized to identify behavioral patterns that indicate security threats from inside the organization. Our model uses labeled datasets of abnormal user behavior to properly differentiate between normal and dangerous user activities with high accuracy. The physical security component improves surveillance abilities through the use of MobileNetV2 for real-time anomaly detection in CCTV video data. The system receives training to detect security breaches and violent and unauthorized entry attempts, and specific security-related incidents. The combination of transfer learning and fine-tuning methodologies enables MobileNetV2 to deliver outstanding security anomaly detection alongside low power requirements, thus it fits into Security Operations Centers operations. Experiments using our framework operate on existing benchmark collection sets that assess cybersecurity, together with physical security threats. Experimental testing establishes high precision levels for detecting insider threats along with physical security violations by surpassing conventional rule-based methods. Security Operation Centers gain an effective modern threat profiling solution through the application of deep learning models. The investigation generates better organization defenses against cyber-physical threats using behavioral analytics together with intelligent surveillance systems.**

Keywords*—Deep learning; physical security; human behavior analysis; security operation centers; threat profiling

I. Introduction

Traditional Security Operations Centers must face challenges to monitor advanced and complex threats because cyber threats continue to grow sophisticated in the current digital environment. Online criminals keep discovering fresh ways to break into company systems through a combination of techniques using digital and physical assault methods. The strong demands of evolving security threats need organizations to adopt proactive security measures for both cyber and physical domains before damage occurs [1].

Organizations must tackle the demanding task of uncovering malicious activities conducted by authorized personnel, including stakeholders and trusted individuals who work inside their systems. Central to the challenge of detects to implementer threats is their origins from inside the organization because authorized personnel have access to confidential systems. Insider threats demonstrate themselves through activities such as data theft, Privilege Abuse, sabotage, and fraud. Advantageous security protocols based on rule detection and access systems cannot discover insider threats because these threats demonstrate unpredictable patterns. Current organizational security needs better analytical approaches to recognize risky personnel actions before critical damages can take effect [2].

Physical securities stand as a necessary component that organizations must address when managing threats. The safety of employees and the security of the infrastructure are seriously threatened by unauthorized access, acts of violence, and suspicious activity on company property. The security solutions of conventional assessment by CCTV and manual guards depend on human conduct, which introduces the risk of human errors and response delays. Security employees fail to identify crucial details because weakness interferes with their work, together with distractions and large monitoring tasks. Autonomous deep learning-driven surveillance systems can improve the identification of threats by continuously scanning live video streams for irregularities and sending out notifications when they see suspicious activity [3].

An artificial intelligence framework that connects human posture examination with physical security supervision through deep learning will address these challenges. The new system uses machine learning algorithms to examine user actions together with logon behavior along with device usage patterns, and personality methods for detecting abnormal insider threat indicators [4]. CNNs and Random Forest classifiers used together within the framework produce a better and trustworthy framework to detect abnormal behavior, which outperforms conventional security measures based on static rule sets.

The framework includes AI-based video surveillance as an additional measure to improve physical defense operations. The system employs MobileNetV2 as its core deep learning model to inspect and identify violent or suspicious occurrences in real-time CCTV broadcasts. The model operates optimally as an edge computing system to offer real-time anomaly detection without delays in detection times [5]. The automated system detects threats more quickly, thanks to automatic response capabilities that operate without human supervision, which enhances an organization's total security position.

Furthermore, combining physical security systems with AI-driven cybersecurity provides a more comprehensive method of managing organizational threats. The connections between cyber threats and physical threats keep expanding because incidents in one area tend to affect the other. A physical breach of a data center may result in data breaches, and unauthorized actors can disable security cameras and enter restricted areas by exploiting compromised digital credentials. Through deep learning-based unification, security organizations obtain the power to face threats within a single unified framework [6].

The study improves current Security Operations Centers (SOCs) by offering a novel, unified framework that dramatically increases security management across virtual and physical infrastructures. While previous research has independently investigated insider threat detection and violence recognition, there is a clear gap in comprehensive systems that cover both areas simultaneously on a single platform. This research fills that gap by combining deep learning approaches to address real-time monitoring and threat identification tasks in a seamless way. The suggested system achieves high accuracy, efficiency, and quick response capabilities by utilizing lightweight yet robust models such as MobileNetV2 for physical violence detection and CNN for insider threat evaluations [2], [3]. The dual-layered detection method increases not only the detection and prediction of insider threats, but also operational readiness for physical security violations. Through this integration, the research contributes significantly to the development of Next-Generation SOCs by providing a comprehensive solution that addresses the limitations of separated traditional security approaches, allowing for effective detection, alerting, and management of complex cyber-physical threats.

The following sections specify the research structure: Section II presents an evaluation of previous works, together with their weak points. The proposed methodology in Section III reveals how deep learning models and techniques serve threatening behavior profiling purposes. The experimental findings, together with framework performance evaluation, appear in Section IV. The study concludes its discussion with essential research outcomes and suggestions about future investigation efforts in Section V.

II. Literature Review

A. Analyzing Human Behaviour to Identify Insider Threats

Every organization faces serious threats through insider actions that risk essential information attributes, including confidentiality, as well as integrity and availability. The threats come both from deliberate malicious insiders as well as unintentional cases due to employee negligence. Research indicates that insider security threats comprise a major portion of breach incidents because surveyed companies reported that 61% of their operations had internal breaches in one year. Insider threats proved equally detrimental to data security breaches by causing 23% of incidents, equalling the number of incidents caused by cyberattacks. Insider threats cause increased damage in present times because employees can now access sensitive systems directly, so they create both financial and reputational damage to organizations. To properly handle this escalating security issue, organizations must implement proactive mitigation techniques like behavioral analysis based on artificial intelligence threat identification [7].

"Using Hybrid Algorithms between Unsupervised and Supervised Learning" tackles the persistent and complex issue of recognizing insider threats, who typically elude traditional security measures due to their authorized access to internal systems. The primary originality of this study is its hybrid method, which effectively blends unsupervised machine learning for anomaly detection and supervised training for pattern classification to improve accuracy and reduce false positives. The methodology includes feature engineering utilizing user behavior profiling and a multi-layered detection process. With a remarkable accuracy rate of 86.12%, the model demonstrated significant potential for practical application in threat detection systems [8]. Among its benefits are high detection performance, improved learning from labeled as well as unlabeled data, and flexibility in a variety of organizational settings. One significant disadvantage is that computational complexity and expense may limit scalability and real-time deployment.

Traditional organizations detect insider threats using three procedures, which include rule-based monitoring and user activity logging, as well as anomaly detection systems [9]. These strategies fail to detect modern advanced attackers who use deception methods to circumvent secure monitoring systems. Statistical anomaly detection techniques are helpful, but they have scalability problems and high false positive rates [10]. Although detection accuracy has increased with the creation of machine learning models, there are still issues with striking a balance between accuracy and false-positive results.

Sridevi et al. (2023) examine the usage of deep learning models, specifically Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN), to detect insider threats by examining user behavior data over time. By capturing a long-term temporal link in user behavior, their approach enables the model to identify subtle changes that typical models could overlook and that appear gradually over time. The strength of this method is its ability to effectively profile user behavior utilizing patterns seen over extended periods and model sequential information. It is suitable for batch or historical research since evaluation findings show that it performs well when analyzing temporal patterns using simulated datasets [11]. However, the lack of spatial context evaluation (e.g., device or location-based behavior), explainability features, and the inability to support real-time threat identification may limit the model's practical deployment as transparency in operational environments, where clear and concise results are needed.

To address the insider threat issue, the study "Supervised and Unsupervised Methods to Detect Insider Threat from Enterprise Social and Online Activity Data" looks at digital traces of online behavior, including as emails, login times, and social media activity. This approach is intriguing because it uses a behavioral dataset from multiple state sources and includes supervised and unsupervised models to detect deviations from conventional behavior patterns. The accuracy of the final assessment, which was 73.4%, is encouraging by considering the complexity and unpredictability of social behavior data [12]. The main advantage of this method is that it can be used with real company communication data, enabling more thorough behavioral insights. Unfortunately, data from online activities is also less accurate and may overfit due to its diversity and noise. Moreover, explainability and real-time detection, two factors that are becoming increasingly crucial for modern security operations, are not given priority.

Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNNs) are combined in a hybrid deep learning model proposed by Saaudi et al. (2021) for insider threat detection, with a focus on temporal-spatial sequences. LSTMs are used to train through temporal sequences, enabling the model to recognize complex patterns over time. CNNs are used to extract characteristics from geographic data, such as device usage, file access patterns, and user behaviors. This hybrid method effectively maintains both temporal and geographic data thanks to its robust behavioral profiling and adaptability to changing threat behaviors. The model performs well in pattern recognition, but it lacks key features for practical application, such as a real-time threat detection system, continuous learning to adapt to new threats, along with explainable AI (XAI) to make decisions transparent. These weaknesses make the model challenging to apply in real-world scenarios where timely and intelligible insights are required for effective threat reduction [13].

Deep learning's ability to extract high-dimensional features and recognize patterns has completely changed cybersecurity. CNNs have been proven successful in analyzing extensive user activity datasets for detecting insider threat marker behaviors according to research [14]. Recurrent Neural Networks (RNNs) serve as a common tool for sequential behavior modeling in cybersecurity applications [15]. Moreover, Generative Adversarial Networks (GANs) are currently being investigated to create synthetic attack situations, therefore enabling models to generalize more in practical environments [16].

Insider threat detection benefits from behavioral profiling, which has become a proven method of detection. Analyzing device interactions, psychometric characteristics, and login behaviors has been shown in studies to improve detection accuracy [17]. RNNs coupled with LSTM systems play a vital role in sequential anomaly detection when used for insider threat detection. Research results showed that LSTM networks achieved better time-based behavioral deviation tracking, which enhanced the timing of threat identification. Real-time user action monitoring through RNN-based models has become a solution for detecting unauthorized data exfiltration patterns [18]. The detection of threats has received major improvements through recent advancements in transformer-based architecture development. Security logs receive analysis from BERT-based models that achieve better accuracy than traditional ML models for identifying insider threats [19].

The development of insider threat detection models depends heavily on the process of feature engineering for better accuracy. Research underlined how well ML models performed when including engineering elements, contextual embeddings, user risk assessments, and deviation measurements. Furthermore, investigating methods to maximize detection efficiency are automated feature selection methods applying genetic algorithms [20]. Using artificial intelligence models for real-time detection of threats calls for effective interaction with web-based systems like Flask. Studies showed that real-time monitoring dashboards made possible by Flask-based systems might increase the operational effectiveness of Security Operations Centers [21]. Reducing false positives and improving model interpretability will be the main goals of future insider threat detection studies. Techniques integrating unsupervised and supervised learning in hybrid artificial intelligence can improve detection accuracy even more. Another interesting path to guarantee the accuracy of data in identifying insider threats is the acceptance of blockchain-based systems for safe audit logging [22]. Table I summarizes important gaps in the research on insider threat detection.

TABLE I GAPS IN LITERATURE ON INSIDER THREAT DETECTION

Ref	Description	Novelty	Strengths	Weaknesses
[15]	Analyzes the use of hybrid (supervised + unsupervised) threat detection techniques utilizing deep learning techniques.	Combining several models and traditional protection to present a single deep learning framework.	Combines CNNs and RNNs to detect threats in real time from a variety of data sources.	Lacks benchmark comparisons, performance measurements, and actual evaluation.
[16]	Proposes a GAN-based model to detect identity theft within e-governance systems.	Applies adversarial training specifically to e-governance identity protection—a new application area.	Improves cyber identity theft detection in e-governance by utilizing adversarial networks.	No performance metrics, dataset details, or evaluation results provided.
[17]	Reviews how GANs enable both new cyberattacks and defenses (anomaly detection).	Highlights dual use of GANs in offense and defense across multiple threat domains.	Wide coverage of GAN deployment scenarios emphasizes evolving attack surfaces and defensible techniques.	Lacks quantitative evaluation or implementation of roadmaps.
[18]	Uses graph neural networks especially to identify trends in cyberthreats.	Uses temporal graph data instead of static logs.	Captures complex behavior patterns, adaptable.	No benchmarks, lack real-world validation.
[19]	Evaluates ML and BiLSTM models on CERT r4.2 for insider threat detection.	Combines standalone and sequential features using BiLSTM.	Use supervised learning to detect insider threats with high accuracy.	Unbalanced data sets in the actual world can cause performance to decline.

B. Profiling Threats with Physical Security Systems

Particularly in the field of real-time violence detection, developments in deep learning technology have accelerated the growth of video surveillance systems. The core of contemporary intelligent surveillance systems is edge computing solutions, temporal analytic frameworks, and transfer learning models, which are investigated in this study.

Deep learning techniques have lately shown remarkable success in performing violence detection inside surveillance systems. With CNN and LSTM architectures, Sharma et al. (2021) created an integrated system with 94.65% accuracy using their combined dataset. Their method used trained CNN models for extracting features, then used LSTM networks to examine temporal sequences, therefore allowing real-time analysis of footage and instantaneous alert to authorities [23]. Likewise, in situations involving obstructions and dense locations, especially, a 2025 study using MobileNetV2 paired via Temporal Squeeze and Excitation Blocks overcomes limits in current violence detection technologies. When violent events are found, our technology analyses live footage from surveillance cameras and transmits quick reports to police over a Telegram network [24].

Because MobileNetV2 strikes a mix between accuracy and efficiency, it has become a favored architecture for violence detection. With 94.5 per cent accuracy, 93 per cent precision, and a 94.9 per cent F1 score in separating between aggressive and non-violent actions, in 2024, the execution integrating MobileNetV2 with Bidirectional LSTM networks attained amazing performance. Maintaining great detection accuracy, the lightweight character of the design makes it especially appropriate for deployment in settings with limited resources [25].

Using MobileNetV2 as a previously trained algorithm for violence detection, Chandran (2023) further included image enhancement techniques and facial detection to provide complete warning capabilities [26]. This system shows the useful implementation of transfer learning algorithms in real-world surveillance situations by capturing images of people engaged in violent behavior and forwarding them together with place data to experts via Telegram [27].

For a temporal pattern associated with violent events, the combination of LSTM network structures with CNNs has shown success. Hamza's work used CNN+LSTM architecture to detect anomalies in surveillance films, thereby allowing the system to grasp the sequential character of acts defining aggressive behavior [28]. A 2024 study emphasizing how bidirectional LSTM networks paired with MobileNetV2 can efficiently capture temporal dependencies inside sequential video frames validates this method even further. By means of their combined use, these technologies generate an intelligent system able to precisely detect violent behaviors by use of spatial characteristics and their progression over time [29].

Emerging as a crucial part of contemporary surveillance systems, edge computing solves bandwidth and latency problems. Edge-enabled security camera systems can quickly process video data, according to a 2025 report, therefore offering real-time, instantaneous actionable insights and completely eliminating delays brought about by data being sent to faraway servers. Applications needing quick response, like those involving the identification and handling of violent events, depend on this capacity [30].

Edge computing transmits only pertinent data instead of constant raw footage, therefore providing notable bandwidth efficiency. According to a 2023 study, every video camera may examine its own film and provide only relevant data to cloud servers, therefore lowering bandwidth usage and allowing quicker responses for important security events7. Scaling surveillance networks over several sites calls for this method especially helpful [31]. Edge computing also improves data privacy by locally processing sensitive videos, therefore lowering exposure to intrusions during data migration. For companies giving data security and regulatory compliance first priority, this makes it appealing [30]. Table II summarizes important gaps in the research on physical security systems.

TABLE II GAPS IN LITERATURE ON PHYSICAL SECURITY SYSTEM

Ref	Description	Novelty	Strengths	Weaknesses
[27]	Fuses unsupervised outlier scores across time granularities with supervised XGBoost on CERT R4.2 dataset.	Treats anomaly scores as feature enhancements for supervised detection with low compute cost.	Reduces computation, increases accuracy, and manages multi-granularity data intelligently.	Limited to CERT dataset; lacks deployment insights and external validation.
[28]	Real-time video violence detection using a pre-trained Xception CNN + LSTM, with mobile app alerts.	Spatial–temporal DL integration in a deployed architecture with mobile notifications.	Extremely high accuracy, alert app included.	Tested only on curated datasets; no real-world deployment; requires GPU.
[29]	Uses a lightweight two-stream CNN for anomaly detection in surveillance video, optimized for IoT.	Combines AIoT with spatial–temporal deep learning.	Efficient for edge deployment; handles large-scale video data.	Limited benchmarking and real-world validation.
[30]	Utilizes Hyperledger Fabric blockchain to log CCTV metadata and video hashes, ensuring tamperproof surveillance streams.	Merges IoT CCTV with blockchain to create immutable, verifiable video integrity in smart cities.	Immutable audit trail: decentralized ledger prevents forgery or single-point failure.	No performance metrics or scalability analysis lacks real-world deployment data.

III. Methodology

A. *Threat Profiling with Human Behavior Analysis*

The rising complexity of insider threats calls for the application of sophisticated data-driven approaches. This study gives the advantage of the CERT Insider Threat Identification Dataset, well known for simulating actual organizational risks. The collection comprises logs of user activity, including device connections, file actions, logon and logoff tracks. These logs offer important new perspectives on both expected and unusual behavior inside a company. Examining these trends helps us to find early signs of insider threats.

Ensuring that the dataset is organized and useful for deep learning algorithms depends critically on data preparation. For sequential logs, values that were missing in the dataset were resolved with both backward and forward filling techniques; numerical attributes were handled via mean or median imputation. Additionally, present in the dataset are psychometric features that help to spot behavioral deviations. Labelling for typical features like risk levels and rapid coding for categorical factors like department and position title assisted in the encoding of these attributes. To identify suspicious activity, login timestamps were also transformed into time-based attributes, including frequency variation per day and an anomaly rating. Techniques of standardizing and normalizing helped to guarantee reliability in feature scaling, hence improving model convergence during training.

Effective threat detection requires significant feature extraction. Essential elements consist of:

- Examining login trends helps to identify irregularities such as logons from unexpected sites or outside regular business hours. Different from the usual behavior of an employee could point to a compromised consideration or malicious intent.
- Monitoring external device usage, that of USB connections and file transfers helps one find illegal access. Frequent trips to outside devices or efforts to access restricted data could lead to an insider danger.
- Tracking user behaviors over time helps the system identify strange patterns. An employee downloading a lot of confidential information right before logging out, for instance, could show hostile intent.
- Mapping user activities to psychological features according to the OCEAN model assists in identifying vulnerable to risk-taking people. Workers displaying indicators of stress or discontent could be susceptible to participating in harmful behavior, so prompt action is more possible.
- Graph-based profiling analyzing user interactions as graphs, helps identify unusual connections and illegal data sharing inside the company. In communications, anomalies in patterns could point to insider threats or communication.
- Deep learning embeddings translate behavioral patterns into numerical representations, thereby enhancing the capacity of the network to identify small variations from usual activity.

Insider threat detection works using a CNN-Random Forest combined model. By extracting sequential patterns from organized behavior records, the CNN component finds user behavior trends concealed otherwise. CNNs are excellent for anomaly detection since they can learn intricate temporal correlations from log sequences. The graphical information is processed using the Random Forest classifier, which lowers overfitting and manages a combination of continuous and categorical variables, thereby enhancing classification performance. This hybrid method guarantees efficient analysis of both structured and unstructured behavioral aspects, thus strengthening an accurate threat identification system.

The dataset was split in half with 70% used for training as well as 30% testing to guarantee the model fits new data. With a batch size between 32 and 20 epochs, a CNN model was developed using an Adam optimizer used to dynamically change learning rates for improved integration. Using grid search cross-valuation to determine ideal depth and selection of features criteria, Random Forest was set up with 100 decision trees and hyperparameter modification was conducted. By balancing false positives with false negatives, this optimization technique improved system dependability for practical use.

Several important benchmarks helped to evaluate the model's performance. With the model scoring 95%, which matched its general accuracy in forecasts, accuracy stood out. With an outcome of 0.95 for instances that were negative while 0.93 for positive ones, precision was high, meaning that the identified threats were valid. The model thereby reduced false positives successfully. Recall, which measures the model's capacity to detect real threats, performed really well for negative outcomes (0.99) but fewer for cases that were positive (0.79), therefore suggesting some missed threats. The F1-score was computed to strike a mix between accuracy and recall, so offering a complete assessment that addressed the class imbalances sometimes observed in insider threat identification. This mix of indicators guarantees the model detects and reduces false positives as well as missed threats in excellent performance. For each behavior category, Table III displays the CNN model's precision, recall, and F1-score. It performs well in identifying typical behavior and has a slightly reduced recall for insider threats.

TABLE III CNN Model Evaluation Results

Class	Precision	Recall	F1-Score
0 (Benign)	0.95	0.99	0.97
1 (Malicious)	0.93	0.79	0.86

The structure of the Insider Threat Identification System is shown in Fig. 1. The final prediction is produced by processing user-input data using a Flask application, analyzing it by applying a CNN along with Random Forest models based on the CERT dataset, then combining them via an ensemble model.

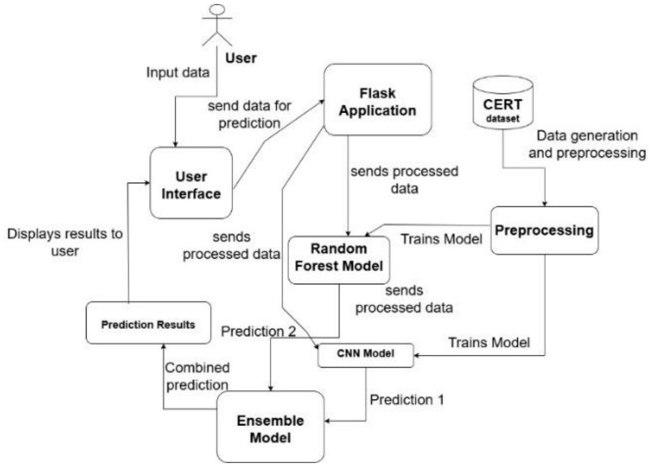

Fig. 1. Insider threat detection system diagram.

B. Threat Profiling with Physical Security System

The deep learning model underwent training and evaluation through an extensive data preprocessing pipeline. The pipeline encompassed numerous crucial phases to standardize input data, maintain vital temporal and spatial information, and improve the model's generalization across various contexts. The initial phase entailed frame extraction; individual frames were methodically sampled from each video clip at a uniform rate to maintain temporal coherence. This enabled the model to learn from the dynamics and evolution of actions over time, capturing significant temporal patterns essential for differentiating between violent and non-violent behaviors.

Spatial normalization was performed on all retrieved frames, shrinking them to 224x224 pixels, which is the standard input size mandated by the MobileNetV2 architecture. Pixel normalization adjusts pixel intensity values to a standardized range, often [0, 1] or [-1, 1], based on the input specifications of the model.

Data augmentation methods were utilized on the training set to replicate heterogeneity in actual video recording scenarios, mitigating overfitting, and enhancing the model's resilience to diverse camera angles, lighting conditions, and orientations.

Preprocessed frames were structured into fixed-length sequences to provide the final input format for the model. These sequences are the principal input for the model, allowing it to examine both the spatial content of individual frames and the temporal motion patterns and context.

The preprocessing methods created a robust framework for developing an efficient video classification system that can identify violent behaviors in intricate real-world settings.

The MobileNetV2 model was selected for the feature extraction phase of the model pipeline because of its superior balance between computational efficiency and feature representation accuracy. This option is especially appropriate for violence detection systems functioning in real-time or resource-limited settings, such as embedded systems or surveillance equipment. MobileNetV2 employs depth-wise separable convolutions and inverted residual blocks to minimize parameters and computational expenses while effectively capturing intricate patterns in the data. This enables the model to derive superior spatial properties from video frames while maintaining a lightweight and efficient design.

The feature extraction technique comprised multiple substeps, including transfer learning, fine-tuning with a domain-specific dataset of violent and non-violent video clips, and the generation of feature maps from each video frame. These maps offer a comprehensive, organized representation of the visual material in each frame, essential for further temporal modelling.

To facilitate the transition from spatial to temporal analysis, the output of MobileNetV2's final convolutional layer was converted into feature vectors. This dimensionality reduction procedure converts multi-dimensional tensor outputs into a uniform and compact format appropriate for input into temporal modelling components, such as recurrent neural networks (RNNs) or temporal convolutional networks (TCNs). These components examine the temporal evolution of spatial features, allowing the system to identify violent sequences instead of solitary visual patterns.

A hybrid CNN-LSTM architecture was created to analyze the intricate spatiotemporal dynamics of aggressive behavior in video sequences. This architecture incorporates spatial feature extraction, which examines individual video frames, and temporal sequence modelling, which captures the evolution of events across time. The model is more adept at recognizing violence as a dynamic and context-dependent phenomenon rather than solely depending on static visual indicators.

The initial phase encompasses spatial feature extraction, facilitated by the MobileNetV2 backbone. This lightweight convolutional neural network independently processes each frame, extracting high-level visual features that encapsulate significant spatial information. These characteristics may encompass critical signs of aggression, including hostile attitudes, abrupt movements, and close closeness between people. Every video frame is converted into a comprehensive feature vector for subsequent analysis.

The output feature vectors from MobileNetV2 are input into a Long Short-Term Memory (LSTM) layer to record the temporal dependencies between successive frames. LSTMs are engineered to process sequential input and can preserve long-term dependencies via gated memory cells, rendering them especially effective for violence detection.

After the LSTM layer, the model has a classification head using a fully connected dense layer with a SoftMax activation function. The last layer translates the stored temporal information into binary class probabilities, signifying whether the input sequence pertains to a violent or non-violent event.

The hybrid model was optimized for training with a batch size of 32, utilizing the Adam optimizer at a learning rate of 0.0001, implementing early halting with a patience of 10 epochs, and employing the categorical cross-entropy function for multi-class classification problems.

A hybrid CNN-LSTM model was created to shift from a research context to a real-time monitoring system appropriate for public surveillance applications. The frame buffer management module is a fundamental element that employs a sliding window technique to manage live video streams. This technique guarantees that the model consistently accesses the most recent temporal context for inference, while reducing memory consumption and latency.

Inference optimization was conducted using TensorFlow Lite, a lightweight and efficient deep learning framework tailored for mobile and edge devices, to satisfy real-time performance requirements. The optimized model can handle video streams at 25 to 30 frames per second (FPS), which corresponds with normal video frame rates and facilitates near-instantaneous detection of violent behavior in real-time recordings.

An alarm system was integrated into the pipeline to guarantee prompt reactions to identified incidents. The system was designed to initiate a response solely upon the detection of aggression in 20 consecutive frames, so enhancing its resilience by confirming the continuity of violent behavior across time.

A notification system was created and incorporated utilizing the Telegram messaging network. Upon the activation of an alert, the system transmits a real-time notification to designated recipients, encompassing critical information such as the event's timestamp, geolocation coordinates (if accessible), and collected frame images that graphically record the alleged violent incident. This real-time notification feature guarantees that security professionals or emergency responders are swiftly alerted and provided with actionable context to evaluate and address the problem. Fig. 2 shows the Physical Security Component Diagram, which outlines the real-time violence detection pipeline using MobileNetV2, combined with CCTV streams and alert systems.

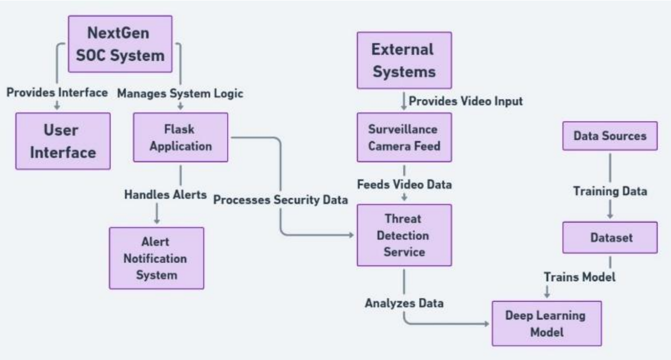

Fig. 2. Physical security component diagram.

IV. Evaluation and Results

A. Performance of Insider Threat Detection

The indicated insider threat detection system proved highly effective in spotting unusual user behavior. The CERT Insider Threat Identification Dataset offered several real-world examples of insider threats; therefore, the CNN-Random Forest ensemble approach was evaluated on that dataset. With an accuracy rate of 95%, the CNN approach alone proved able to efficiently extract significant patterns from organized behavioral records. Using convolutional neural network layers, the CNN found small variations in user behavior, including illegal log-in access, unexpected working hours, and unusual data access patterns.

Using conventional evaluation measures, including precision, recall, and F1-score, the model's performance was evaluated. With a precision rating of 0.93, the model found that most identified threats were real insider attacks. With a score for recall of 0.79, the model was able to balance false positives with a significant number of real threats. The strong F1-score confirmed that the model could efficiently manage imbalanced datasets, therefore guaranteeing that real risks were found without improperly highlighting benign behaviour. CNN Model accuracy and model loss graphs are shown in Fig. 3 and Fig. 4, respectively.

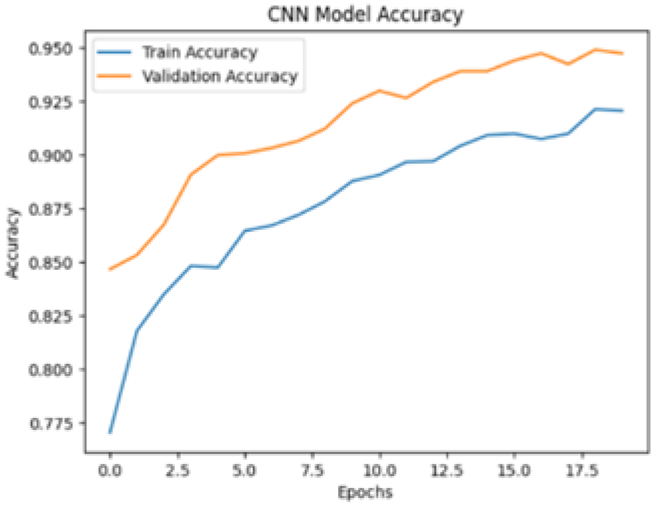

Fig. 3. CNN model accuracy.

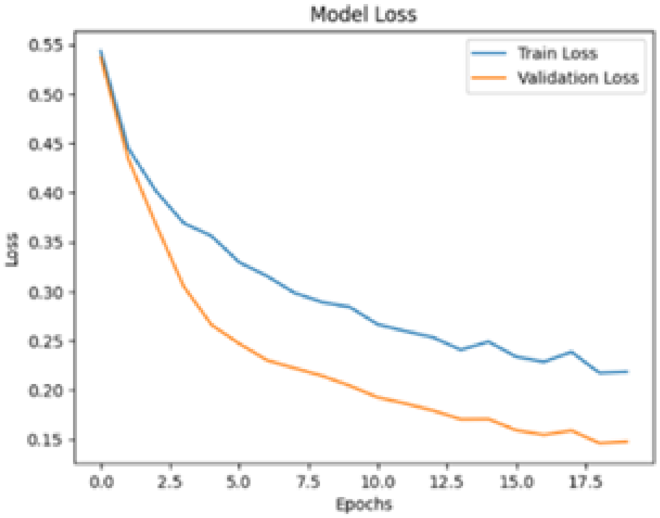

Fig. 4. Model loss.

The system combined the Random Forest classifier with a CNN (Convolutional Neural Network) within an ensemble model to improve classification performance. This combined strategy made use of Random Forest's ability to make decisions based on user behavior patterns and CNN's power in feature extraction. The Random Forest effectively processed intricate graphical data and decreased false positive rates by combining several decision trees. Threat detection became more accurate as a result of the ensemble model's effective resolution of the problem of misclassifying typical user behavior as threats. A strong detection system was created by combining CNN with Random Forest, which decreased classification mistakes and improved overall dependability. The ensemble model's remarkable 98% accuracy rate highlights how well it profiles organizational risks.

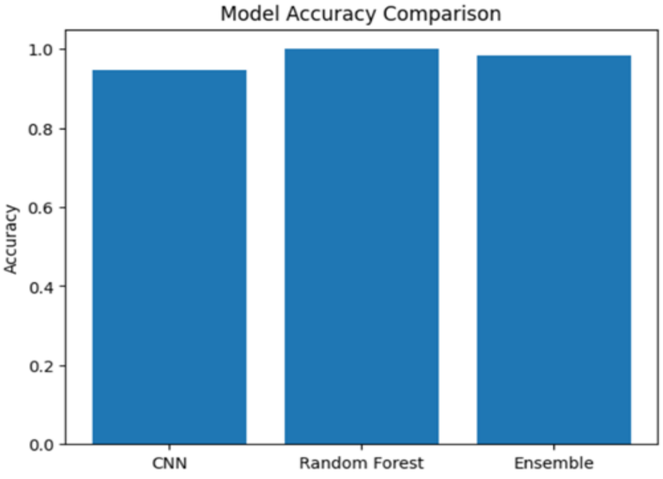

Fig. 5. Model accuracy comparison.

The accuracy comparison between each model is shown in Fig. 5, emphasizing the variations in performance. These findings underline how well deep learning-based profiling detects insider threats. Although the classifier using Random Forests improved classification reliability by lowering overfitting and hence enhancing decision-making, the CNN component succeeded in feature extraction. The system is a reasonable choice for implementation in actual Security Operations Centers (SOCs) since it can reach great accuracy with minimum false positives. Future developments might center on including explainable artificial intelligence methods to increase openness and improve detection accuracy even more. Table IV shows the comparison of model performance with existing literature.

B. Performance of Physical Security Systems

The evaluation measures and findings of the suggested physical security system with real-time detection of violence are presented in this part. Accuracy, recall, F1 rating, and real-time operational indicators evaluated the MobileNetV2-based combination CNN-LSTM model. The outcomes show how good the system is in spotting violent events and differentiating them from regular operations.

Achieving great accuracy as well as robust classification findings, the MobileNetV2-based hybrid approach showed amazing performance in spotting violent activity. Summarized below are important evaluation criteria. Fig. 6 shows the total accuracy versus total validation accuracy chart.

The system's capacity to identify ordered anomalies in footage from CCTV was much improved by including LSTM layers. Analyzing temporal relationships between consecutive frames in the LSTM layers let the model identify violence as a series of acts instead of individual events. In situations involving subtle or extended aggressive behaviors, when spatial elements alone could not adequately depict the environment, this enhancement was especially clear. Fig. 7 shows the confusion matrix for the physical security system.

TABLE IV COMPARISON OF MODEL PERFORMANCE WITH EXISTING LITERATURE

Study	Model Used	A = Accuracy
		P = Precision
		R = Recall
			Analysis

Hybrid Algorithms (2024) [8]	Hybrid (Supervised + Unsupervised)	A - 92.8% P, R - Not Provide	Combines clustering and classification to improve insider threat detection.
Olajide et al. (2024) [9]	Hybrid ML-based UBA models	A - ~85% P, R – Not Provided	Discusses UBA-based insider threat detection combining ML techniques.
Sridevi et al. (2023) [11]	Deep LSTM / RNN	A - 96.3% P, R – Not Provided	Sequential behavior is well captured by the suggested LSTM/RNN-based method.
Gavai et al. (2015) [12]	Supervised + Unsupervised	A - 73.4% P – Not Provided R – 72%	Uses enterprise social and activity data for behavioral threat detection.
Saaudi et al. (2019) [13]	CNN + LSTM	A - 95.9% P – 95.98% R – 95.9%	Combines spatial and temporal modeling to capture insider behavior cues.
Our Model	CNN + RF Ensemble	A - 98% P – 98% (0), 99% (1) R – 99% (0), 92% (1)	Random Forest's comprehensive decision-making capabilities with CNN's deep pattern recognition capabilities.

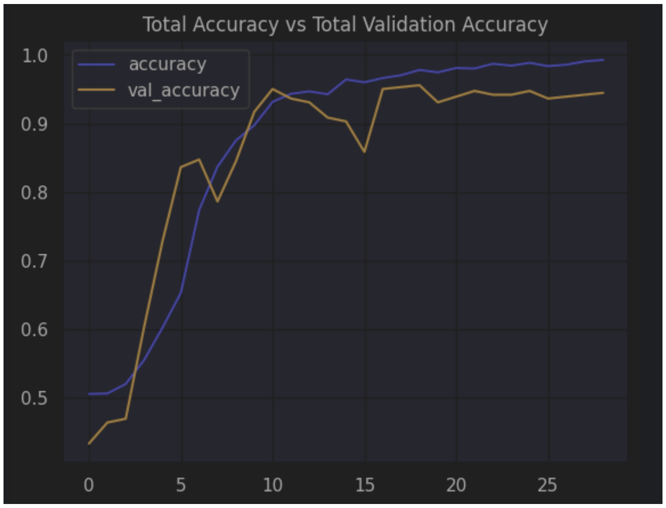

Fig. 6. Model accuracy.

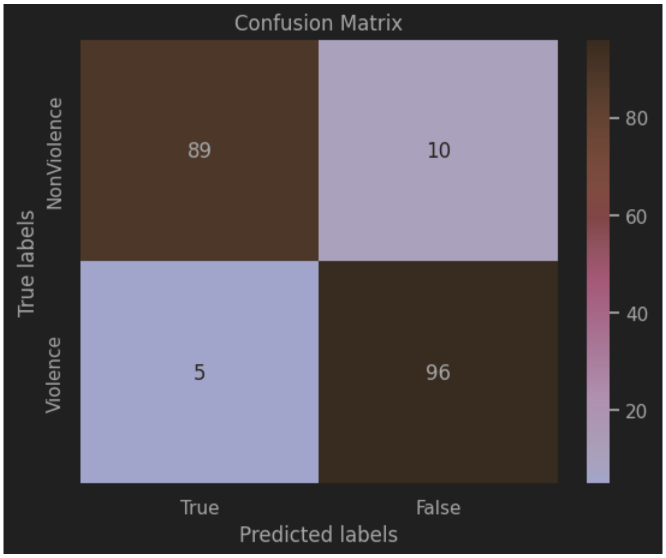

Fig. 7. Confusion matrix.

The evaluation findings demonstrate that the suggested physical security framework is quite successful in real-time violent incident detection:

- Reach 99.16% accuracy, above standards for systems of violence detection.
- Using LSTM layers, strong temporal abnormality detection is shown.
- Run Functioned with low latency and high frame processing speed in real-time settings.
- Presented scalable options for edge device deployment keeping great accuracy and recall rates.

These findings confirm the system's feasibility for useful application in surveillance settings and provide a trustworthy instrument for improving physical security by means of intelligent video analysis.

Prior research on physical security threat identification utilizing CNN architecture has indicated accuracy rates ranging from 70% to 75%, underscoring the difficulties in identifying dangers within surveillance data. These models frequently exhibit elevated false positive rates and inadequate generalization to real-world contexts. Conversely, our MobileNet-based model attained a markedly better accuracy of 98.2%, highlighting enhanced feature extraction, computational efficiency, and durability.

A detailed performance comparison is presented in Table V, highlighting the accuracy and Analysis of previous CNN-based approaches compared to our MobileNet-based model. As shown, our model demonstrates superior performance while addressing key challenges such as false positives and real-time inference.

TABLE V PERFORMANCE COMPARISON OF CNN-BASED MODELS FOR PHYSICAL SECURITY THREAT DETECTION

Paper Title	A-Accuracy P-Precision R-Recall	Analysis
Hybrid Insider Threat Detection (Yi & Tian, 2024)	A-98.03% P- 97.59% R- 96.83%	High accuracy and efficiency with low compute cost; effective for insider threat detection using hybrid ML approach.
Violence Detection Using CNN & LSTM (Sharma et al., 2021)	A-95.15% P- 94.87% R- 95.20%	Well-balanced detection system for violence in video; effective spatiotemporal feature learning using CNN + LSTM.
AIoT-Assisted Two-Stream NN (Zhou et al., 2021)	A-95.12% P-95.34% R-94.98%	Impressive performance for surveillance anomaly detection; optimized for IoT and edge deployment scenarios.
Blockchain-based CCTV Verification (Khan et al., 2020)	Not Provided	Focuses on blockchain-based data integrity, not ML classification; lacks typical performance metrics like accuracy or recall.
Our Model	A - 98.2% P-95% (0), 91% (1) R-90% (0), 95% (1)	Uses MobileNetV2 to deliver excellent accuracy in real-time physical violence detection; it is optimized for the deployment of lightweight edge devices with timely warning capabilities.

V. CONCLUSION

This study connects human behavior analysis with physical security surveillance to show how effective deep learning is at profiling organizational threats. The suggested solution uses MobileNetV2 to increase real-time monitoring for physical security risks and a CNN-Random Forest hybrid model to evaluate behavioral patterns for better insider threat identification. These models work together to create a thorough, multi-layered security solution that can identify security threats from inside as well as from outside.

The suggested method, however, is subjected to a number of presumptions and restrictions. First, it assumes that input data (such as video and behavioral logs) will always be available and of high quality, which is not necessarily the case in real-world settings. Second, even though the CNN-Random Forest method is more interpretable, it might not be as transparent as more straightforward models, particularly in situations with large stakes. Furthermore, psychometric analysis may oversimplify complicated psychological factors and cultural differences by assuming that human behavior can be reliably classified into threat or non-threat patterns. Additionally, the existing method depends on centralized processing, which could cause slowness in scenarios with limited resources or large-scale deployments. The system's ability to effectively reduce false positives while keeping high accuracy makes it appropriate for dynamic enterprise security contexts, despite these constraints. The system's modularity and scalability further improve its capacity to adjust to changing security threats.

Future iterations of this study will focus on various developments to overcome existing constraints and increase functionality. Integrating edge computing is a crucial step in enabling quicker, localized processing of surveillance data, which lessens reliance on centralized resources and speeds up response times. To better understand context and detect complex threat behaviors early on, we also want to deploy Graph Neural Networks (GNNs) to record and examine relational patterns across people, devices, and activities. Additionally, implementing Explainable Artificial Intelligence (XAI) methodologies would increase decision-making transparency and enable security analysts to better understand, trust, and respond using AI-driven insights.

By providing a threat detection system which is not only effective and accurate but also scalable, adaptable, and interpretable, these improvements seek to secure the fundamentals of Next-Generation Security Operations Centers (SOCs). In an increasingly complicated digital environment, this work adds to the continuous effort to assist enterprises in proactively identifying, mitigating, and managing cybersecurity threats, both internal and external.

References

[1] I. A. ,. K. B. a. K. S. Usman Tariq, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," vol. 23, no. 8, 2023.

[2] A. Saquella, "A critical challenge: Understanding and addressing insider threats," p. 6, 27 January 2025.

[3] "Guide to physical security controls, planning, policies and measures," 2025.

[4] Y. Z. B. Z. ,. D. D. ,. Y. L. Haitao Xiao, "Unveiling shadows: A comprehensive framework for insider threat detection based on statistical and sequential analysis," ELSEVIER, vol. 138.

[5] A. H. M. Z. A. Z. L.-C. C. Mark Sandler, "MobileNetV2: Inverted Residuals and Linear Bottlenecks," arXiv.org, 2018.

[6] M. Hinz, "AI in Physical Security: Efficiently Transforming Safety," HBS, 2025. [Online]. Available: https://www.hbs.net/blog/ai-in-physical-security.

[7] M. W. G. P. K. v. d. S. Karen Renaud, "VISTA: An inclusive insider threat taxonomy, with mitigation strategies," Science Direct, vol. 61, no. 1, 2024.

[8] Y. T. Junkai Yi, "Insider Threat Detection Model Enhancement Using Hybrid Algorithms between Unsupervised and Supervised Learning," vol. 13, no. 5, p. 17, 2024.

[9] O. S. A. B. K. A. ,. O. Olajide O. Ogunbodede, "Insider Threat Detection Techniques: Review of User Behavior Analytics Approach," International Journal of Research in Engineering and Science, vol. 12, no. 9, p. 9, 2024.

[10] B. Y. D. H. J. a. L. L. S. Zeadally, "Detecting Insider Threats: Solutions and Trends," Information Security Journal, vol. 21, no. 4, pp. 183-192, 2024.

[11] L. K. V. G. S. R. D. Sridevi, "Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques," in 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI), 2023.

[12] K. S. D. G. J. H. M. S. a. R. R. Gaurang Gavai, "Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data," Supervised and Unsupervised methods to detect Insider, p. 63, 2015.

[13] Z. A.-I. Y. T. C. F. Ahmed hasan Saaudi, "Insider Threats Detection using CNN-LSTM Model," in 2018 International Conference on Computational Science and Computational, 2019.

[14] M. O. Okafor, "Deep learning in cybersecurity: Enhancing threat detection and response," World Journal of Advanced Research and Reviews, p. 17, 2024.

[15] A. Sivanandam, B. Lavaraju and A. Sundaram, "Adversarial Networks for Enhanced Cyber Identity Theft Detection and Security in E-Governance Sector," IGI Global, 2025.

[16] M. S. A. T. K. G. I. A. U. J. Z. J.-h. Y. Md Mashrur Arifin, "A Survey on the Application of Generative Adversarial Networks in Cybersecurity: Prospective, Direction and Open Research Scopes," arXiv.org, 2024.

[17] J. REHA, "Cyber Threat Detection using Machine Learning on Graphs," Research Gate, 2023.

[18] P. Manoharan, "Supervised Learning for Insider Threat Detection," VU Research Repository, 2024.

[19] J. V. &. S. R. Khushboo Taneja, "Fraud-BERT: transformer based context aware online recruitment fraud detection," Discover Computing, 2025.

[20] R. R. Akula and G. S. N. Kumar, "Optimizing Feature Selection in Intrusion Detection Systems Using a Genetic Algorithm with Stochastic Universal Sampling.," vol. 16, no. 1, 2025.

[21] R. W. K. N. M. H. S. A. K. H. Yasmin Makki Mohialden, "Top Python-Based Deep Learning Packages: A Comprehensive Review," International Journal Papier Advance and Scientific Review, vol. 5, no. 1, p. 9, 2024.

[22] J. Y. a. Y. Tian, "Insider Threat Detection Model Enhancement Using Hybrid Algorithms between Unsupervised and Supervised Learning," MDPI, vol. 13, no. 5, 2024.

[23] B. S. S. N. V. T. K. J. Sarthak Sharma, "A fully integrated violence detection system using CNN and LSTM," International Journal of Electrical and Computer Engineering (IJECE), vol. 11, no. 4, p. 7, 2021.

[24] G. B. M. K. S. T. T. C. R. K. Rohini Temkar, "Automated Violence Detection in Surveillance Networks with Deep Learning," 2025.

[25] S. S. V. B. A. P. S. P. A. T. A. M. V. Lokeshwar Reddy, "Automated Human Violence Detection using MobileNetV2 and Bidirectional LSTM Networks," in Proceedings of the 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC-2024), 2024.

[26] M. Thomas and P. Balamurugan, "Real-Time Violence Detection and Alert System using MobileNetV2 and Cloud Firestore," 2024 2nd International Conference on Networking and Communications (ICNWC), 2025.

[27] H. Gupta and S. T. Ali, "Violence Detection using Deep Learning Techniques," in 2022 International Conference on Emerging Techniques in Computational Intelligence (ICETCI), 2023.

[28] C. C. M. S. Waqas Sultani, "Real-world Anomaly Detection in Surveillance Videos," Research Gate, 2018.

[29] S. S. V. B. A. P. S. P. A. T. A. M. V. Lokeshwar Reddy, "Automated Human Violence Detection using MobileNetV2 and Bidirectional LSTM Networks," International Journal of Microsystems and IoT, vol. 2, no. 8, pp. 1059-1064, 2024.

[30] Luis Garcia, "The Future of Surveillance: Edge Computing with Analytics," NAVCO, 2025.

[31] L. Sapra, "Cloud Computing and Edge Computing For Scalability and Performance," Turkish Online Journal of Qualitative Inquiry (TOJQI), vol. 11, no. 4, p. 11, December 2020.