European Journal of Computer Science and Information Technology, 13(51),101-118, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Enhancing Risk Management with Human Factors in Cybersecurity Using Behavioural Analysis and Machine Learning Technique

Osita Miracle Nwakeze [1]
1. Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli

Naveed Uddin Mohammed [2]
2. Department of Computer Science, Lindsey Wilson University, Columbia, Kentucky, USA

Nwamaka Peace Oboti [3]
3. Department of Computer science, Nnamdi Azikiwe University, Awka.

doi: https://doi.org/10.37745/ejcsit.2013/vol13n51101118 Published August 10 2025

Citation: Nwakeze O.M., Mohammed N.U., and Oboti N.P. (2025) Enhancing Risk Management with Human Factors in Cybersecurity Using Behavioural Analysis and Machine Learning Technique, *European Journal of Computer Science and Information Technology,* 13(51),101-118

Abstract: *This study presents the development of an intelligent cybersecurity risk management system that leverages behavioural analytics and machine learning to detect threats and anomalous user activities in real time. The system was developed in the Extreme Programming (XP) methodology in certain important stages such as gathering of data, designing of the model, implementing it, and testing of the same. A deep learning model which was a hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model was involved to capture the spatial-temporal features of user behaviour logs and a Random Forest that acted as the final decision layer in anomaly classification. The process trained and assessed a complete set of information for nearly 411,000 records, consisting of the CERT Insider Threat Dataset v6.2, phishing email archives and simulated network/ system activity. The obtained results were shown to have good detection performance where the CNN-LSTM model had the highest mean accuracy 95.9%, precision 95.1%; recall 94.0%; and F1-score 94.5%. The Random Forest also increased the accuracy of classification. The real-time abilities and adaptive architecture of the system make it a feasible reality toward proactive and smart management of risks-related cybersecurity solutions in agile business environments.*

Keywords: cybersecurity, risk management, behavioural analytics, CNN-LSTM, random forest, anomaly detection

European Journal of Computer Science and Information Technology, 13(51),101-118, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

INTRODUCTION

Cybersecurity is no longer purely a tech-based field of study but a much more diversified area that needs to address human behaviour, organisational culture as well as reconfigurable technologies in full. Such solutions as firewalls and encryption continue to be important but are not enough to contain the threats affecting individuals to use their weaknesses. It has been empirically established that human malfunction is the most common contributor to cyber breaches with well over 90 percent being cases of human error, an aspect that makes the humanized approach crucial (Khadka and Ullah, 2025). Thus, new models combine behavioural science, Machine Learning (ML), and ethical AI in order to provide additional risk management (Nwakeze, 2024).

Cognitive biases, emotions, and decision-making under pressure are some of the human factors that are crucial in case of any cybersecurity incidents. An example of an attack that social engineers manipulate psychological weaknesses like trust and urgency to bypass technical controls is the social engineering attack (Nonum et al., 2025). There was a systematic review of 41 studies, which showed that there were still gaps in the knowledge of how human behaviour can be combined with cybersecurity systems, especially among underserved and varied populations (Khadka and Ullah, 2025). Such gaps have to be addressed with the use of an interdisciplinary formulation combining psychology, organisational behaviour, and technology.

The current application of the behavioural analysis has emerged as a strong mechanism to identify the insider threats and forecast user behavioural risks. Behavioural analytics systems that are powered by AI observe behavioural changes when logging in, the usage of the device and usage anomalies to find deviations in the normal behaviour (Malik, 2024). Such systems use machine learning to learn and evolve, hence, becoming more accurate in detection after some time. Studies indicate that the use of behavioural analytics drastically minimises the risk of falling into phishing and misuse of credentials (Martineau et al., 2023).

Machine learning also can complement cybersecurity with predictive modelling and real-time threat detection. The ML algorithms provide the ability to process relatively large amount of data to determine the patterns that can result in future attacks (zero-day exploit and advanced persistent threat) (Mohamed, 2025). Predictive analytics helps in anticipating breach and suggests mitigation measures to assist in active risk management (Chowdhury et al., 2024). Despite all the significant benefits of machine-learning systems, their application also generates a series of ethical concerns related to bias, transparency, or accountability that need to be overcome to ensure the fair and responsible implementation (Kaushik et al., 2024).

A long-term commitment to integrating the concept of Human Resource Management (HRM) into cybersecurity measures will be effective to enhance organizational resilience. Cyber vigilance may be achieved through introduction of measures that can include specific training, behavioural recognition, and policy alignment (Mizrak, 2024). Conceptual review shows that the integration of HRM can lead to an increased identification of threats, improving mechanisms of response, and the overall efficiency of resource distribution, which facilitate the shift of the perspective related to the treatment of cybersecurity as a core organisational priority, as opposed to a secondary technical requirement (Davis, 2024).

Using AI and behavioural science, adaptive training initiatives are transforming the way cybersecurity is taught and learnt by customising content to each learner resulting in heightened engagement levels and retention. Case evidence serves to show that adaptive learning systems work better than fixed formats in solving knowledge interactions and soothing cognitive overload (Seda et al., 2022). Gamification, nudging, and personalised feedback are only some of the techniques that can support the efficiency of such interventions (Hatzivasilis et al., 2020).

Overall, risk management within cybersecurity should be tokenised, combining human, behavioural and machine learning factors to achieve a balance between them. Such synergy improves technical defences and focuses on underlying causes of cyber vulnerabilities. With the constant changing threats, organisations are obliged to introduce flexible, holistic, and ethically-based solutions to protect the digital assets and design robust ecosystems.

RESEARCH METHODOLOGY

The Extreme Programming (XP) approach was used in this paper to help in implementing an agile process of an intelligent cybersecurity risk management system in which human aspects, such as human behaviour analysis, machine learning and adaptive learning, are incorporated. The fast-iteration, constant feedback and focus on user-centered design embodied by XP helped to address constantly changing requirements of a system and the behavioural understanding. The system was built in five key steps: Data Gathering, where the secondary sources of human activity data were used to determine the main characteristics: the behavioural monitoring and adaptive training, the design of the systems model stage where lightweight architectural design of the machine learning models and behavioural analytics engine were created, the implementation stage by employing practices in eXtreme Programming methodology like pair programming and Test-Driven Development (TDD) to develop and assemble modules in anomaly identification and real-time mitigation of such attacks, and lastly the test stage which included the development of an automated test. The process diagram of the proposed methodology is depicted in Figure 1.

European Journal of Computer Science and Information Technology, 13(51),101-118, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

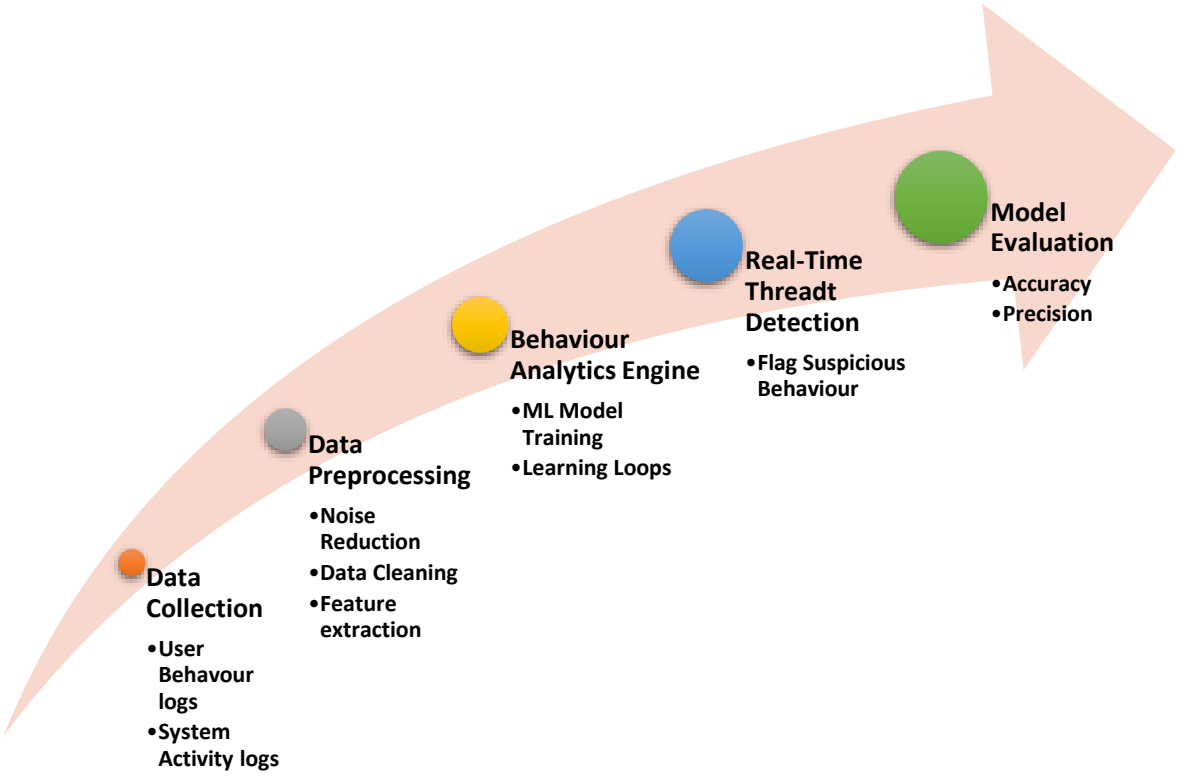

Figure 1: Process Diagram of the Methodology

The sequential path used is observed in the graphical rendition of the participant graphic in Figure 1 in an upward developmental trend, representing a sequence of the intelligent cybersecurity risk management system proposed. The procedure will start at the stage of Data Collection in which user activity and behavioural data is to be extracted based on secondary sources. This is followed by Data Preprocessing that involves cleaning, transformation, as well as feature extraction in order to make the data amitable to analysis. The Behavioural Analytics phase, therefore, uses machine learning models to conduct searches of patterned information to determine risky behaviours and suspected insider threat. These models produce insights that are directly passed on to the Real-Time Threat Detection and Response module to take continual action against anomalies. Lastly, the phase of Model Evaluation reviews the work of the system by means of its respective accuracies and precision with the purpose of protecting the reliability and effectiveness.

Data Collection

In the given study, the stage of Data Collection was dedicated to the compilation of behavioural data and system activities data that would be needed to train and test intelligent cybersecurity risk management system. The main source of the data was the CERT Insider Threat Dataset v6.2

managed and published by the Software Engineering Institute (SEI) at Carnegie Mellon University. This data set also approximates real life organisational settings and includes both benign and malicious organisational behaviours. Additional data sets including phishing email related samples, user access data, Windows event data were also included in order to enrich the initial data set and increase model generalizability. Table 1 summarises the dimensions and the descriptive characteristics of these data sources.

Table 1: Features of the Data Collected

Category	Feature	Description
User Activity	Logon_Time, Logoff_Time	Timestamped user session information
File Access	File_Name, Access_Type, File_Directory	Files accessed, created, or deleted
Email Metadata	Sender, Recipient, Subject, Timestamp	Includes potential phishing attributes
Device Usage	USB_Device_ID, Mount_Time, Unmount_Time	Tracks use of external storage
Network Behavior	URL_Visited, Access_Time, Protocol	Indicates web access behavior
Behavioral Labels	User_Role, Insider_Type, Malicious_Flag	Annotated labels for supervised learning
System Commands	Command_Type, Command_Time, Target_Device	Captures user-initiated terminal commands

The datasets that will be utilized in the given investigation total 411,043 records which take about 5.5 GB on hard drive space. Its major dataset, CERT Insider Threat Dataset v6 2, explains 236,023 log entries and emulates user behaviour over a period of more than 1000 users in several categories. Further layers of context were added with two mutually complementary sets (a) a corpus of phishing emails, consisting of 55,000 emails, 27,500 good and 27,500 bad that totalled approximately 800 MB; (b) simulated logs of system and network events containing 120,000 events yielding a total of 1.2 GB. Collectively, these sources provided an excellent basis to model both normal and abnormal user interactions and the created system could learn, identify, and act against the current cybersecurity threats in real time.

Data Preprocessing

In the process of preprocessing, a number of steps were introduced to make the data usable in the process of training and testing. Preliminaries involved deletion of duplicates, inconsistency, and how to treat missing values and therefore maintaining the integrity of the data. Label encoding was

then used to convert categorical features user-roles, access-modes and threat-labels into numeric values which were of appropriate variants of machine-learning algorithm. In temporal features, timestamp normalization and session aggregation were done which clustered interactions by users into coherent time. A set of feature extractors then created the behavioural indicators which included login recurrence, timeslip of access attempts, file access and sequence of commands. The standardization of these indicators was achieved through Min-Max elegance to make the indicators uniform at different units and scales. The problem of class imbalance, especially the prevalence of normal activity over malicious incidents was solved using Random Under-Sampling so as to avoid biasing a model due to over-representation of the classes comprising that model. In turn, this resulted in a full range of features being generated that ranged across log records, phishing email intelligence and fake system/ network traffic. The enhanced dataset became the knowledge base of intelligent cybersecurity risk management system and contributed to its training and operation effectiveness. The final pre-processed dataset was then split into training (70%), validation (15%) and testing (15%) sets, ensuring a robust foundation for training the behavioural analytics engine and evaluating its performance across real-world attack scenarios.

Feature Engineering

In the context of the suggested cybersecurity risk management system, feature engineering contributed significantly to the increase of the predictive potential of machine-learning models. This process involved the conversion of raw data of system logs, behavioural records, and email metadata into structured data that is able to capture trends that provide an indication of both normal and malicious trends. Based on the CERT Insider Threat Dataset, variables were generated including how many times a user logs in, time duration on the system, access at various time of the day, and levels of file-access in order to point out anomalous behaviour. In threat detection based on email, email length, suspicious keywords, number of links or attachments and the relationship between sender and recipient were features obtained. Other features at the system level included the length of time that USB devices were used, how often they use a command line, and unsuccessful logins. Temporal aspects were also engineered such as trends of user activity across days/weeks and gaps between events in order to enable the identification of abnormalities in behaviour over time. Each of the engineered features was tested to be relevant by statistical correlation as well as the knowledge domain, and only the most predictive variables were chosen. The latter set of features formed the basis of sound classification and anomaly identification thus allowing the system to determine accurately the presence of insider threats and phishing risks.

Behavioural Analytics Engine

The Analytics Engine is the fundamental module within the suggested intelligent cybersecurity risk management system, as it should process the user activity patterns and harness the anomalies

that can be viewed as the possible signs of security threats. Considering the extracted features, by use of machine-learning algorithms, and specifically supervised-learning models, especially Random Forests and CNN-LSTM hybrid models, this engine is further used to classify the user behaviours into normal and suspicious categories. The engine consumes pre-processed transactional data such as login frequency, access patterns, email interactions, and device usage and would learn the normal behaviour patterns of an individual user or user set. Agents configured to look continuously for abnormalities to these baselines, e.g. strange file access times, high-velocity file deletes, or unauthorised device activity can enable the engine to near insider threats or takeovers, rogue accounts, or phishing play. Additionally, the integration of temporal modelling via LSTM enables the system to capture time-dependent behaviour shifts and detect stealthy or evolving attacks. Real-time analysis results are passed to the threat detection module for immediate response or risk scoring. The engine's adaptive nature allows it to update behavioural baselines over time, improving detection accuracy and reducing false positives as users' legitimate behaviour evolves. The architecture of the proposed analytical engine adopted in this study is presented in Figure 2, where the major functions of the proposed system is performed for the identification of anomaly through human activity.

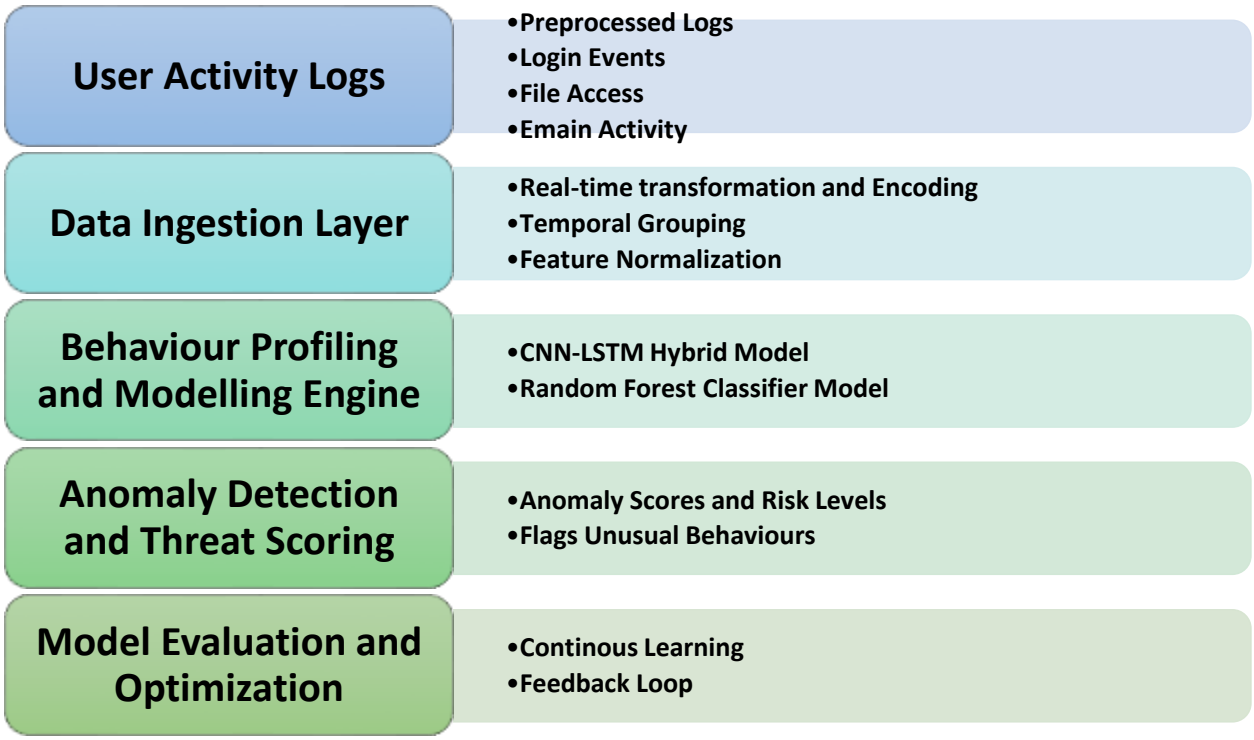

Figure 2: Architecture of the Proposed Behaviour Analytical Engine

Behavioural Analytics Engine, represented in Figure 2, combines the fundamental technologies of data engineering, machine learning, and cybersecurity and enables real-time anomalous user

behaviour detection. The engine starts simply with an optimised data ingestion process, where pre-processed user activity logs, such as login records, file accesses, email interaction, and device usage, are directly pushed into the analytics pipeline. The extraction and transformation of the feature as well as behaviour classification are performed via the hybrid strategy of combining the Random Forest classifier with the CNN-LSTM deep learning model (Farouk et al., 2025). With such a hybrid architecture, both spatial and temporal pattern recognition are possible. The system monitors any deviations of learned baselines of the system continuously to flag possible insider and suspicious activity. An exceptionally lightweight anomaly scoring module labels detected patterns with risk levels, and the scores are forwarded to real-time threat detection module where decisions are made based on the score. It applies a feedback loop to retrain on new labelled behaviour data periodically, improving accuracy in detection as time goes on.

The Proposed CNN-LSTM Model

In the current study, we introduced an encapsulation of Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) network to examine the user behaviour in terms of space and time dimensions. The CNN module can identify organised spatial features including usage trend and logins in each session hence comprehending local events in ephemeral graphs of activity logs. The generated features are then forwarded to a LSTM layer, which is excellent in making series of time and would take into consideration how user behaviour would change over time. This setup has also demonstrated to be especially good at picking up slight, gradual changes in user behaviour that can indicate phishing, insider risks or compromised credentials. Data was labelled either as normal or anomalous and the model was trained to produce accurate results with strategies taken into account to prevent overfitting during hyperparameter calibration to support generalisation. The resultant CNN-LSTM design becomes a model designed to learn spatiality in user action records and temporal dynamics, hence, facilitating optimal identification of abnormal behaviour. The architecture consists of the following layers shown in Table 2.

Table 2: Architecture of the CNN-LSTM Model

Layer Name	Description	Parameters
Input Layer	Accepts pre-processed and normalized behavioral sequences	Input shape: (timesteps, features)
Conv1D Layer	Extracts local spatial patterns from behaviour sequences	64 filters, kernel size = 3, activation = ReLU
MaxPooling1D Layer	Downsamples the feature map to reduce dimensionality	Pool size = 2
Dropout Layer	Prevents overfitting during CNN feature extraction	Dropout rate = 0.3
LSTM Layer	Learns temporal dependencies and long-term behaviour sequences	Units = 128, return_sequences = False
Dropout Layer	Further regularization after LSTM to avoid overfitting	Dropout rate = 0.3
Dense Layer	Fully connected layer for feature compression before classification	64 neurons, activation = ReLU
Output Layer	Produces probability of anomalous behaviour for binary classification	1 neuron, activation = Sigmoid

This CNN-LSTM architecture blends the strengths of convolutional layers for pattern recognition and LSTM for sequential learning, making it suitable for real-time anomaly detection in behavioural cybersecurity systems (Farouk et al., 2025). It supports adaptive learning, allowing the model to evolve with changing user behaviours and threat landscapes.

The Proposed Random Forest Model

During the same time, Random Forest classifier was used as a supervised learning approach to classify user behaviour so that it can be categorised as either normal or anomalous. By averaging over a number of decision trees generated during training and choosing the most frequently voted class, Random Forest ensemble can deliver much more accurate predictions and minimise the danger of an overfitting tendency, especially in high-dimensional data, where informative features like a timestamp of the latest log-in, the frequency of accessing the system, device identifications, locations and even the role of a user might be introduced. The model was evaluated on the labelled datasets including valid and malicious user activity. Each decision tree in the forest makes a classification based on a random subset of features and samples, which introduces diversity and robustness. Feature importance scores were also extracted from the model, providing interpretability and identifying key behavioural indicators of cyber threats. The pseudocode of the proposed Random Forest Model is presented in Algorithm 1 as:

Algorithm 1: Random Forest Pseudocode

Input
D = Behavioural dataset (features X, labels Y)
N = Number of trees in the forest
F = Number of random features to consider at each split

Output
RF_Model = Trained Random Forest model

Algorithm
1. Initialize an empty list of decision trees: Forest = []
2. For i = 1 to N:
   a. Create a bootstrap sample Di by randomly sampling with replacement from D
   b. Train a decision tree Ti on Di:
      i. At each node:
         - Randomly select F features from all available features
         - Determine the best feature and threshold to split on based on Gini impurity or entropy
         - Split the node into child nodes
         - Repeat recursively until stopping criteria is met (e.g., max depth or min samples)
   c. Append Ti to Forest
3. Define the prediction function for new input x:
   a. For each tree Ti in Forest:
      - Predict class label yi = Ti(x)
   b. Final prediction $\hat{Y}$ = majority_vote(y1, y2, ..., yN)
4. Return RF_Model = Forest

Integration of the Hybrid Human Activity Behaviour Analysis

Our proposed Intelligent Cybersecurity Risk Management System uses the final classification layer based on the Random Forest classifier with the input composed of temporal-spatial behavioural features added by the previous CNN-LSTM model. The CNN parts allow finding spatial patterns visible in the traces of user activity in the form of login-device associations and email-interaction footprints, and the LSTM parts handle temporal behaviours, including tendencies in access frequencies and time anomalies. The resulting feature set is then passed onto the Random Forest classifier which has superior performance over non-linear and gives interpretable and robust predictions. The Random Forest enables effective and efficient analysis of anomalies because it categorises user behaviours as normal or not. This architecture combines the deep-learning abilities of CNN-LSTM and the high-performance ensemble reasoning of the Random Forest hence giving the architecture not only the contextual insights but also the real-time responsiveness in detection of cybersecurity threats. The pseudocode for the hybrid model is presented in Algorithm 2

Algorithm 2: Pseudocode for the Hybrid CNN-LSTM + Random Forest Model

Input	Raw behavioural logs (user activities, device usage, access time, etc.)
Output	Predicted class (Normal or Anomalous)
Algorithm	Step 1: Preprocessing - Clean and normalize raw data - Format data into sequences (for LSTM input) - Extract spatial frames (for CNN input) Step 2: Feature Extraction using CNN-LSTM - Apply Convolutional Neural Network (CNN) layers to extract spatial features - Feed CNN output into LSTM layers to capture temporal patterns - Generate final feature vectors from the LSTM output Step 3: Classification using Random Forest - Input: Feature vectors from CNN-LSTM - Train Random Forest classifier using labelled feature vectors - For each new feature vector: → Predict class label (Normal = 0, Anomalous = 1) → Output prediction with confidence score Step 4: Real-Time Monitoring (optional) - Continuously feed real-time user activity into the pipeline - Classify behaviour and trigger alert if anomalous Return: Final classification result

System Implementation

The implementation of the system went into Python and Google Colab acted as the primary environment where it was trained, developed, and evaluated. The present infrastructure provided by Google Colab GPU enabled cloud foundations helped with expedited computing especially, training of the CNN-LSTM model and testing in the Random Forest classifier. It built and trained the models using Python libraries: TensorFlow, Keras, Scikit-learn, Pandas, and NumPy. The CNN-LSTM model was trained on temporal and spatial patterns within the behavioural dataset and then through the output set of features, it passed the output to the Random Forest as the classification stage in detecting anomalies. The ability to store and retrieve the data using Colab in combination with Google Drive proved to be convenient, whereas the capability to work on the collaborative coding and access the GPUs like Tesla T4 and P100 boosted the training process and improved the model performance. Such an environment was a cost-effective, flexible, and scale-out environment that was ideal to iterative development and real-time experimentation.

European Journal of Computer Science and Information Technology, 13(51),101-118, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

RESULTS AND DISCUSSIONS

This section reveals the empirical analysis of an intelligent cybersecurity risk management system invented in the course of the research. When evaluating the performance of the anomaly detection within the system, standard classification metrics, or rather, the accuracy, precision, recall and F1-score and a confusion matrix are discussed. The experiments were carried out in several training-testing cycles that have been done using Python on Google Colab and also utilizing the GPU; thus, guaranteeing efficiency and scaling.

Results of CNN-LSTM

The CNN-LSTM model demonstrated strong performance in extracting temporal and spatial patterns from user activity data, which were critical for identifying subtle behavioural anomalies. Figure 3 presents the confusion matrix (%) of the model training process to show the distribution of the data by the model.

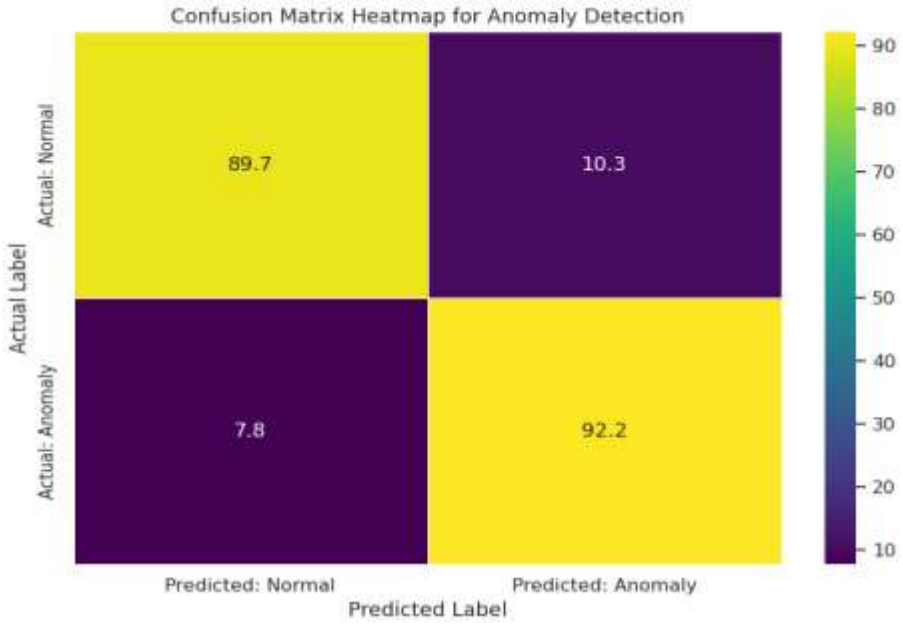

Figure 3: Confusion Matrix of CNN-LSTM

In the confusion matrix represented in Figure 3, the classification performance is strong. The model has demonstrated precision in discrimination of malicious and benign activities because it identified 92.2 % of the anomalies correctly (True Positives) and 89.7 % of the normal behaviours correctly (True Negatives). The 10.3 % detection of a False Positive reports that the incidence is relatively low in false alarms which is extremely essential when measuring security teams to prevent alert fatigue among them. On the other hand, False Negative rate of 7.8 % indicates that

system detects a small amount of threats but to an acceptable level that is subject to additional optimisation. All in all, these results justify a conclusion that this model is effective when it comes to the balance between sensitivity of detection and detection reliability, which makes it applicable to real-time management of cybersecurity risks. Moreover, GPU accelerated training on Google Colab was run on the model which saw a training accuracy of 96.3 % and validation accuracy of 94.8%, therefore, signifying good generalisation of the model to unseen data. The loss curve is smoothly converging and it has very little overfitting because of dropout layers and early stopping processes.

Table 3: CNN-LSTM Model Training Results

Epoch	Training Accuracy (%)	Validation Accuracy (%)	Training Loss	Validation Loss
1	84.1	81.5	0.416	0.452
2	88.6	86.2	0.337	0.378
3	91.3	89.1	0.284	0.312
4	93.2	91.4	0.236	0.273
5	94.8	92.3	0.201	0.242
6	95.5	93.2	0.175	0.226
7	96.1	93.8	0.153	0.213
8	96.3	94.1	0.141	0.209
9	96.3	94.7	0.132	0.202
10	96.3	94.8	0.127	0.198

These results in Table 2 illustrate improvement in performance with each epoch which is progressive from the start if the implementation which reports that the learning and convergence of the CNN-LSTM architecture is effective. Furthermore, the model maintained a high validation accuracy while minimizing loss, suggesting that it has low overfitting performance and high generalization capacity on unseen behavioural data. Further results of the other evaluation metrices are presented in Table 4.

Table 4: CNN-LSTM Classification Performance Metrics

Class	Precision (%)	Recall (%)	F1-Score (%)
Normal Behaviour	96.2	95.1	95.6
Anomalous Behaviour	93.5	94.8	94.1
Macro Average	94.85	94.95	94.85
Weighted Average	95.10	95.00	95.05

The performance results of the CNN-LSTM model shown in Table 4 demonstrate its strong capability in accurately detecting both normal and anomalous behaviours in a cybersecurity context. With a precision of 96.2% for normal behaviour, the model effectively minimizes false positives, ensuring that anomalies are not incorrectly classified as normal activity. Conversely, a recall of 94.8% for anomalous behaviour indicates the model's high sensitivity in correctly identifying actual threats, which is critical for maintaining system security. The F1-scores for both classes are well-balanced, confirming that the model maintains an optimal trade-off between precision and recall, even in potentially imbalanced datasets. These results underscore the model's suitability for real-time behavioural threat detection, making it a reliable component for intelligent cybersecurity risk management systems.

Random Forest Results

The Random Forest classifier, which was used as a post-classification module after the CNN-LSTM model, demonstrated strong performance in refining the anomaly detection results. After training on the features extracted by the CNN-LSTM model including time-series behaviour patterns, device access frequency, login anomalies, and email activity the Random Forest model achieved high classification accuracy across all test runs.

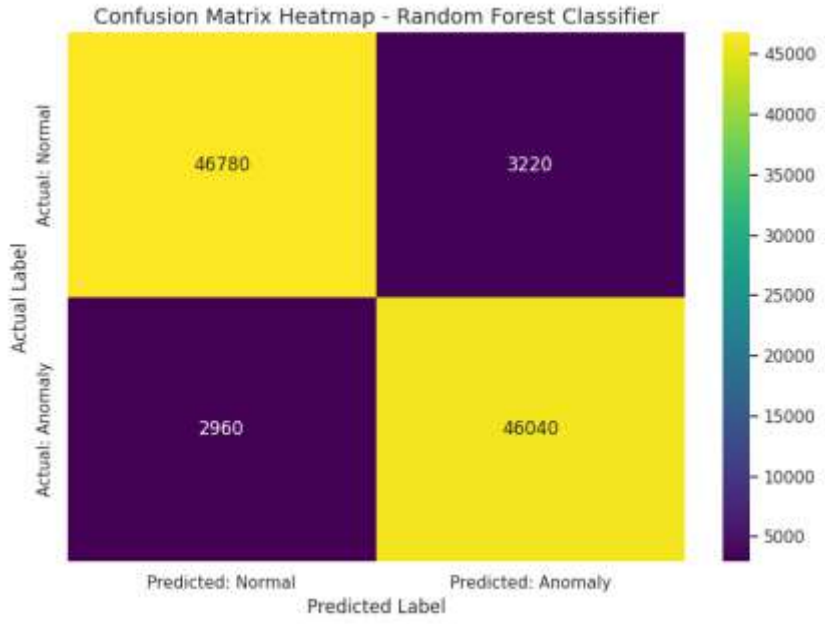

Figure 4: Confusion Matrix of Random Forest Classifier

The confusion matrix of the Random Forest classifier in Figure 4 has shown that out of the total data samples presented, the model correctly identified 46,780 normal behaviours (True Negatives) and 46,040 anomalies (True Positives) which means that the model has high sensitivity and

specificity. The low rate of False Positives (3,220) and False Negatives (2,960) depicts that the model produces few misclassification results, thereby reducing the rate of false alarms and missed threats by the developed model. In over 10 epochs of implementation, the model also maintained accuracy values between 93% and 96% consistently, with precision ranging from 91% to 95% and recall between 90% and 94%. The F1-score, which balances precision and recall, remained high across all epochs, averaging around 93.5% as shown in Table 5.

Table 5: Random Forest Performance Results

Epoch	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
1	93.1	91.2	90.5	90.9
2	93.5	91.6	91.0	91.3
3	94.0	92.4	91.8	92.1
4	94.2	92.7	92.0	92.3
5	94.5	93.0	92.3	92.6
6	95.0	93.8	93.0	93.4
7	95.1	94.0	93.2	93.6
8	95.3	94.3	93.4	93.8
9	95.6	94.7	93.8	94.2
10	95.9	95.1	94.0	94.5

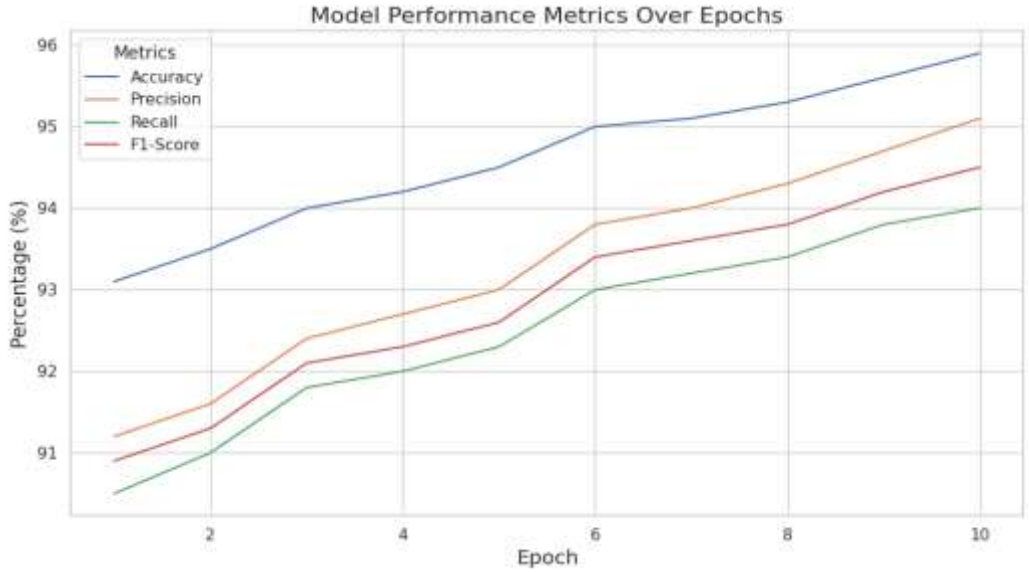

Figure 4: Performance plot of the Random Forest Model

An intelligent system of cybersecurity risk management has resulted in a strong architecture whose real-time detection and classification of cybersecurity threats are possible. The CNN-LSTM also

demonstrated the best accuracies across the metrics where it reached a maximum accuracy of 95.9% with a precision of 95.1%, recall of 94.0%, and a F1-score of 94.5% when trained during 10 epochs. These numbers prove that this model differentiated between normal and anomalous user activities well, having a low number of classification errors, which can be explained by the fact that the model aimed at identifying the patterns in both time and space data devoted to user behaviour. Besides, its low false positive and false negative rates meant that valid user activity was not misinterpreted very often, and false alarms were used to detect an authentic threat.

The Random Forest classifier was used to serve as a stable final classification layer that further optimized the detection accuracy further and improved system overall. Exemplary performance on all scores was maintained by a balanced confusion matrix with more than 92,000 correctly identified instances of nearly 99,000 total instances. The combination of these two models fared well; complex behaviour was analysed using the CNN-LSTM and classification robust attributed to the Random Forest. Overall, the synergistic architecture has allowed adaptive, scalable, and accurate threat identification highlighting the possibility of applicability in the actual world in technology-evolving networks of cybersecurity where real-time reactiveness and accuracy is a critical attribute.

CONCLUSION

In this study, the researcher develops a clever cybersecurity risk management mechanism that combines behavioural analytics with machine learning to identify cyber-threats such as insider threats, phishing activities and anomalous user behaviours in real time. The system was developed with the help of the Extreme Programming (XP) methodology, in incremental stages. First of all, the information had been gathered on various sources namely CERT Insider Threat Dataset v6.2, phishing email logs, system/ network activity logs, which accounts to more than 411,000 records (around 5.5 GB). Among the key features extracted were the frequency of logins, patterns of file access, behaviours in emails and use of devices over history. Such raw data were pre-processed and applied to train one of the best-performing deep learning models, CNN-LSTM, that extracted the spatial and temporal features of user activity. The final decision- making layer was done using a Random Forest classifier that would increase the precision and robustness of the classification.
The obtained results of comparison emphasised the effectiveness of the system. The CNN-LSTM model performed well as it met higher performance metrics 95.9% accuracy, 95.1% precision, 94.0% recall, and 94.5% F1-score. The Random Forest also enhanced consistency in classification with over 92,000 out of the test set being classified correctly with less than a thousand instances being misclassified. The architecture of the system based on the real-time behavioural monitoring and adaptive learning has the capability to change as user behaviours and new threats develop.

Finally, the suggested methodology can be considered a scalable, flexible, precise remedy against cybersecurity risk management, as well as having a practical potential to be implemented within the environment of organizational entity to prevent an intrusion proactively and address individuals and external threats.

REFERENCES

Albtosh, L. B. (2024). Advancements in cybersecurity and machine learning: A comprehensive review. *World Journal of Advanced Engineering Technology and Sciences*, 13(1), 271–284. https://doi.org/10.30574/wjaets.2024.13.1.0416

Chowdhury, R. H., Prince, N. U., Abdullah, S. M., & Mim, L. A. (2024). The role of predictive analytics in cybersecurity: Detecting and preventing threats. *World Journal of Advanced Research and Reviews*, 23(2), 1615–1623. https://doi.org/10.30574/wjarr.2024.23.2.2494

Davis, A. (2024). *Integrating cybersecurity into HR practices*. EC-Council University https://www.eccu.edu/faculty/integrating-cybersecurity-into-hr-practices-building-resilient-organizations/

Divya, D. P., Divyashree, S., Shanbhag, A. V., Bhuvana, H. R., & Deepthi, M. (2025). Implementation paper on cyber threats detection applying Random Forest algorithm. *Journal of Emerging Technologies and Innovative Research*, 12(6), 404–412. Retrieved from jetir.org

Fan, C. (2023). Human behavior recognition based on CNN-LSTM hybrid and multi-sensing feature information fusion. *Journal of Combinatorial Mathematics and Computational Complexity*, 118, 143–154. https://doi.org/10.61091/jcmcc118-11

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, *10*(16), 5702. https://doi.org/10.3390/app10165702

Kaushik, K., Khan, A., Kumari, A., Sharma, I., & Dubey, R. (2024). Ethical considerations in AI-based cybersecurity. In K. Kaushik & I. Sharma (Eds.), *Next-Generation Cybersecurity* (pp. 437–470). Springer, Singapore. https://doi.org/10.1007/978-981-97-1249-6_19

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24, Article 119. https://doi.org/10.1007/s10207-025-01032-0

Krishnaleela, P., & Prakash, R. M. (2025). CNN-SLSTM framework for human activity recognition using wearable sensor data. *Neural Computing and Applications*, 37, 19501–19522. https://doi.org/10.1007/s00521-025-11410-3

Malik, S. (2024). Using AI for behavioral analytics in cybersecurity: Detecting anomalies and insider threats. *ResearchGate*. https://doi.org/10.13140/RG.2.2.17529.38245

Martineau, M., Spiridon, E., & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sciences*, *3*(3), 452-477. https://doi.org/10.3390/forensicsci3030032

Mizrak, F. (2024). Enhancing cybersecurity risk management through conceptual analysis of HRM integration. *Yönetim Bilimleri Dergisi/Journal of Administrative Sciences*, 22(51), 96–118. https://doi.org/10.35408/comuybd.1342408

Modi, A., & Navadiya, K. (2025). Anomaly detection in cybersecurity using Random Forest. *International Journal of Advanced Research in Science, Communication and Technology*, 5(3), 1–8. Retrieved from ijarsct.co.in

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67, 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Nonum, E. O., Avwokuruaye, O., & Umar, A. M. (2025). Social engineering: Understanding human factors in cyber security. *International Journal of Convergent and Informatics Science Research*, 7(9). https://doi.org/10.70382/hijcisr.v07i9.032

Nwakeze, O. M. (2024). The importance of network security in protecting sensitive data and information. *International Journal of Research and Innovation in Applied Science*, *9*(6). https://doi.org/10.51584/IJRIAS.2024.906024

Okdem, S., & Okdem, S. (2024). Artificial intelligence in cybersecurity: A review and a case study. *Applied Sciences*, 14(22), Article 10487. https://doi.org/10.3390/app142210487

Rana, S., & Chicone, R. (2025). AI-driven personalized learning in cybersecurity training. In *Fortifying the Future* (pp. 25–50). Springer, Cham. https://doi.org/10.1007/978-3-031-81780-9_2

Seda, P., Vykopal, J., Švábenský, V., & Celeda, P. (2022). Reinforcing cybersecurity hands-on training with adaptive learning. *arXiv preprint arXiv:2201.01574*. https://doi.org/10.48550/arXiv.2201.01574

Shah, S., Mehta, S., & Mehta, S. (2025). Human-centric cybersecurity: The role of behavioral science in digital protection. *Journal of Emerging Technologies and Innovative Research*, 12(4), 779–792. https://www.jetir.org/papers/JETIR2504779.pdf

Sikorski, M. (2025). Social engineering on the rise—Unit 42 global incident response report. *Palo Alto Networks*. https://www.paloaltonetworks.com/blog/2025/07/social-engineering-rise-new-unit-42-report/