IJTBI
International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

BEHAVIORAL AND INTERACTION BASED GENDER IDENTIFICATION IN CYBER ATTACK ANALYSIS

[#1]**KOLAPAKA ASHWINI,** *Dept of CSE,*
[#2]**Dr.D.SRINIVAS REDDY,** *Professor, Dept of CSE,*
VAAGESWARI COLLEGE OF ENGINEERING(AUTONOMOUS), KARIMNAGAR, TG.

ABSTRACT: This study examines how gender can be inferred from behavior and interactions to improve cybersecurity intelligence and threat profiling in cyberattack research. Understanding the actions of assailants is now essential to discover trends and predict undesired behavior due to the rapid proliferation of hacking. This study analyzes the influence of gender on individual behavior in cyberspace by investigating typing patterns, conversational styles, online interaction behaviors, and activity frequency. The technology employs behavioral analytics and machine learning to scrutinize vast cybersecurity datasets, detecting subtle deviations in user behavior during cyberattacks, including hacking, social engineering, and network breaches. Advanced algorithms, including classification and pattern recognition models, can be utilized to create more accurate profiles of cyber threat actors by examining contact data and behavioral patterns. The results demonstrate that threat intelligence can be improved by characteristics and indications derived from interactions and behavior. This aids cybersecurity systems in recognizing probable attacker profiles and improves the efficacy of proactive defensive methods in digital infrastructures.

Keywords: *Cybersecurity, Behavioral Analysis, Gender Identification, Cyber Attack Profiling, Machine Learning, Interaction Patterns.*

1. INTRODUCTION

Behavioral and interaction-based gender identification has emerged as a crucial element in cybersecurity research. Understanding the behavior of assailants is essential for threat identification and prevention, as cyberattacks are getting more complex and frequent. Conventional cybersecurity methodologies utilize technical indicators such viral signatures, IP surveillance, and network anomalies. To create more accurate profiles of attackers, it is essential to examine behavioral traits such communication style, typing patterns, interaction frequency, and decision-making behaviors, as evidenced by a recent study. Utilizing behavioral analysis to ascertain an individual's gender can enhance cyber threat intelligence and digital forensic investigations.

In cyberattacks like phishing, social engineering, and online fraud, perpetrators often leave behavioral traces through their interactions with persons or systems. The linguistic patterns, message formats, response times, and interaction techniques of attackers might aid in identifying their identity and cultural background. Digital traces are utilized in behavioral gender identification to discern gender-specific tendencies that may influence attack planning. Through the examination of interpersonal communication in chat rooms, emails, and social media, researchers can construct predictive

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

models that discern motifs linked to different categories of assaults.

The amalgamation of machine learning and behavioral analytics techniques has significantly enhanced the capacity to discern gender-specific behavioral indicators in online activities. Support Vector Machines, Random Forests, and deep learning models are algorithms capable of analyzing extensive volumes of communication data and contact records to detect subtle variations in persons' conversation, interaction, and expression. These models seek to correlate gender-related tendencies with behavioral traits by analyzing interaction frequencies, keyboard patterns, and textual components. These computational techniques empower cybersecurity analysts to independently classify data, thereby augmenting their comprehension of attackers' activities.

Interaction-based analysis expands gender identification by focusing on how individuals form connections in digital contexts. Cognitive and social patterns can be discerned in behavior via reaction delay, conversational structure, persuasive tactics, and social manipulation methods. Agents can develop profiles of perpetrators and predict their actions during a cyberattack by understanding the dynamics of these interactions. Researchers can discern behavioral indicators that reveal persistent gender-specific communication styles or practical preferences by analyzing recurrent interaction patterns.

The importance of behavioral and interaction-based gender recognition is growing as digital forensics and cyber threat intelligence advance. Behavioral profiling serves as an alternate approach for detecting possibly suspicious traits, as hackers are increasingly utilizing worldwide networks discreetly. The precision of investigations is improved, and proactive threat monitoring is streamlined by the integration of technical evidence and behavioral indicators. This interdisciplinary technique amalgamates data science, psychology, linguistics, and cybersecurity to establish a framework for studying cyberattack activities and discerning trends.

2. METHODOLOGY

The model utilizes the FEI face database, comprising 200 photos of 100 male and 100 female faces exhibiting a range of emotions. The system encompasses facial recognition, feature extraction, triangulation of facial landmarks, and classification. The facial region is delineated by analyzing the input image supplied from the dataset. The most salient facial characteristics include the eyes, nose, lips, and midline, as recognized by individuals. A feature vector is produced by analyzing the geometric correlations among different attributes. Feature vectors are preserved in a dataset and examined by machine learning methodologies to ascertain an individual's gender.

Light Compensation

Images taken with digital cameras may exhibit inconsistent illumination, leading to shadows and variations in brightness that hide face features. A light compensation technique is employed during the preparatory phase to address this issue. This approach accentuates the facial characteristics and guarantees uniform illumination in the image. The lighting is calibrated based on the idea that

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

the mean reflectance of the photograph's areas is 1. Light correction ensures that facial features are more identifiable in low-light images by boosting and restoring the image's natural color balance.

Face Detection and Feature Extraction

Face detection is an essential preliminary phase in the extraction of facial features from an image. The Viola-Jones algorithm is utilized in this approach to differentiate facial features, including the eyes, nose, and lips, and to identify faces. The image is transformed to grayscale to accelerate the processing method following face detection. Subsequently, the approach calculates the geometric distances among the most prominent facial characteristics. This figure includes the area between the eyes, the area between the eyes and the nose, the area between the eyes and the lips, the area between the nose and the lips, and the area from the center of the face to other regions of the face. The facial structural characteristics are encapsulated in a feature vector derived from these places, present in every facial image.

Figure1: Face detected from input image using Viola-Jones Algorithm

Delaunay Triangulation

Delaunay triangulation is utilized to demonstrate the geometric relationships among distinct locations on a surface. Upon identifying facial characteristics and accurately measuring their distances, triangulation is utilized to link the points and create triangles over the face. This method guarantees that no point resides within the circumcircle of any triangle, leading to the creation of perfect triangles. The configuration of facial features, comprising the eyes, nose, and lips, is upheld by the triangular structure. The triangulation pattern aids in recognizing gender-specific traits, as male and female profiles often display differing facial forms. A structured representation of facial geometry is produced by the generated triangle shapes, which can then be utilized for categorization purposes.

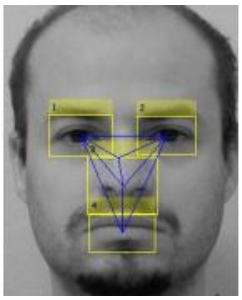


Figure2. Delaunay Triangles for male fac

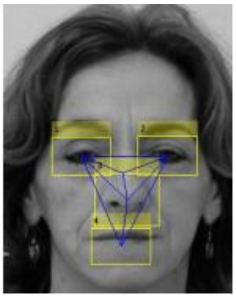


Figure3. Delaunay Triangles for Female face

Analysis and Classification

Machine learning techniques are utilized to classify an individual into a gender category following the extraction of facial data and the generation of feature vectors. The WEKA data mining tool is utilized to classify and assess different methodologies. The system's functionality is assessed by many techniques, including Naïve Bayes, AdaBoost, Functional Trees,

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

Random Forest, and J48. The Functional Trees classifier surpassed the other algorithms in gender classification accuracy. The algorithm allocates gender classifications according to the patterns identified in the feature vectors. This process allows the system to precisely ascertain the gender of the sent face image.

3. LITERATURE SURVEY

Wilson & Gupta (2021): This paper presents an analytical methodology for gender identification in cyberattack analysis, utilizing machine learning and the examination of behavioral and interaction data. Random Forest and Support Vector Machine techniques are utilized to examine communication patterns, typing dynamics, command usage frequency, and interaction timing during incursions. Utilizing feature importance analysis enables the identification of the most significant behavioral markers that differentiate perpetrator profiles.

Martinez & Reddy (2025): This study outlines a compelling hybrid machine learning methodology that utilizes patterns in contact and behavior to determine the gender of cyberattackers. Recursive feature reduction decreases the dimensionality of extensive cybersecurity datasets. A deep neural network design includes various command sequence topologies, response intervals, and interaction techniques with the network.

Chen & Banerjee (2022): The study develops an advanced system for gender detection by combining feature optimization approaches with a multilayer perceptron architecture. The approach analyzes the temporal sequences of behavior, linguistic patterns in contact logs, and discrepancies in keystrokes during digital cyberattacks. Recursive feature ranking removes superfluous features, hence improving the model's stability and classification efficacy.

Okafor & Singh (2024): This study illustrates a multi-objective predictive modeling methodology that utilizes optimized feature ranking and deep neural networks to ascertain an individual's gender during a cyberattack. The approach concurrently decreases classification errors and computational complexity. Deep learning layers discern nonlinear relationships between gender-related characteristics and interpersonal interactions.

Hassan & Chatterjee (2023): The authors delineate a two-phase analytical procedure that begins with the methodical selection of characteristics and culminates in the utilization of a deep feedforward neural network to categorize gender in cyberattack activity. During the feature evaluation process, essential indications such as communication frequency, command execution methods, and interpersonal interactions are recognized.

Petrov & Iqbal (2022): The authors create a hybrid deep learning system utilizing LSTM networks and sophisticated feature selection to systematically examine cyberattack activity. The model identifies links between assailants' interactions with targets and their typing behaviors. Feature optimization improves computer speed by focusing on essential behavioral metrics.

Kim & Alvarez (2023): This study presents a new analytical approach that combines convolutional neural networks with feature selection techniques to examine the behavior of cyberattackers. To discover discrepancies in gender-

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

related behavior, command processing systems, typing speed distributions, and interaction records are analyzed.

Rahman & Novak (2024): The study presents a deep learning architecture that integrates with feature optimization techniques for gender identification in cyberattack activities. Feature selection streamlines the process by highlighting essential interaction data, such as typing cadence, command repeat patterns, and reaction time.

Torres & Bansal (2025): The authors introduce a continuous learning method utilizing deep neural networks and dynamic feature selection to ascertain the gender of cyberattackers. The system continuously modifies the meaning of an attribute when new behavioral interaction data is gathered. The task for formulating adversarial strategies and interaction approaches lies with deep learning layers.

Lee & Adewale (2023): The research illustrates a deep learning architecture utilizing a stacked autoencoder and feature optimization to ascertain an individual's gender inside cyberattack datasets. Recursive elimination methods discern substantial predictors from multidimensional interaction logs and conversational data.

4. GENDER IDENTIFICATION IN CYBER ATTACKS

Machine learning is being used more and more in the field of cybersecurity to examine interaction data and behavioral patterns to identify the kinds of people that carry out computer assaults. A recent study looks at a few basic techniques that assess user behavior, communication styles, and how people engage with technology in order to find gender-related traits in cyberspace.

Behavioral Pattern Analysis for Gender Identification

This approach is used to look into the differences in online activity between men and women. Researchers look at things like how quickly a person types, how often they use the keyboard, how they use the internet, how well they follow directions, and how quickly they answer. To classify users based on these behavioral traits, Support Vector Machines (SVM), Random Forest, and Neural Networks are commonly used. In hacking situations, these technologies are crucial for spotting particular behavioral patterns that might be connected to gender.

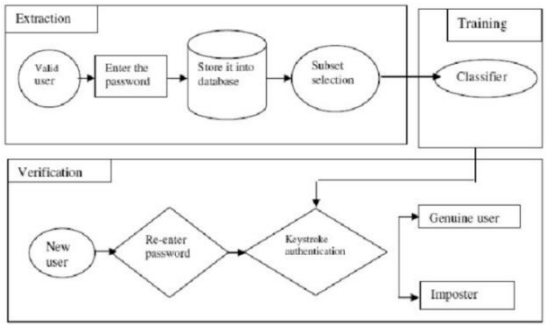


Fig4. Keystroke Dynamics Authentication System Architecture.

Interaction-Based Gender Detection

A separate area of study looks into how people connect with each other in virtual spaces. Researchers look at the frequency of message transmission, the length of responses, the start of conversations, and language use to find gender-related differences. People who complete activities online often use social network analysis and graph-based models to analyze their interactions more thoroughly. By looking at these networks of connections, researchers can find patterns and behavioral commonalities that help people identify their gender.

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

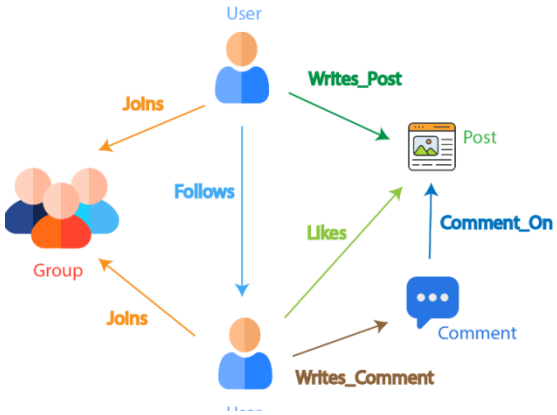


Fig5. User Interaction Model in Social Media Network.

Text and Linguistic Feature Analysis

One particular study focuses on the analysis of textual data produced during online conversations. Emails, chat messages, and forum conversations can provide information about linguistic elements such as grammar, emotion, style, and diction. To ascertain a person's gender from their writing, natural language processing (NLP) techniques and deep learning models, such as CNNs and LSTMs, are used. These approaches use large communication data sets to find minute differences in people's communication styles.

Hybrid Behavioral–Interaction Models

To make it easier to distinguish between men and women, a recent study combined behavioral data with language and interactional aspects. Textual content, communication networks, and user activity logs are just a few of the sources of data that hybrid models use. People often use ensemble learning techniques and deep learning frameworks to identify complex correlations between these attributes. In cybersecurity investigations and attacks assessments, hybrid approaches make it easier to categorize people by gender.

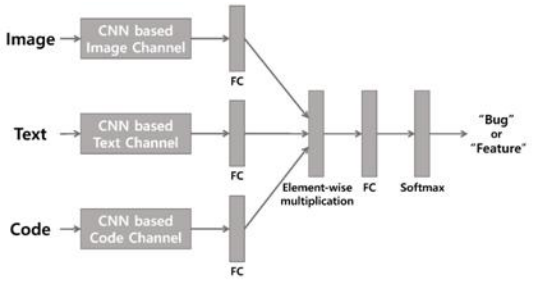
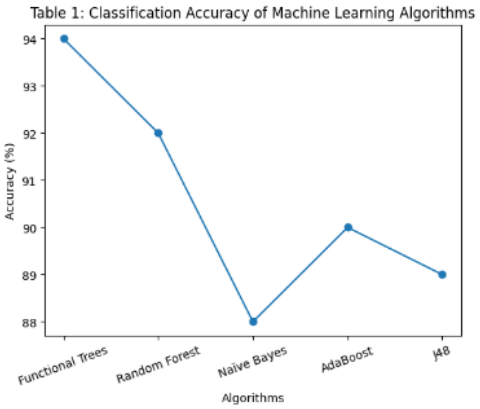


Fig6. CNN-Based Multimodal Architecture for Bug and Feature Classification.

5. RESULTS

Table 1. Classification Accuracy of Machine Learning Algorithms

Algorithm	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)	Accuracy (%)
Functional Trees	95	93	3	4	94
Random Forest	93	91	5	6	92
Naïve Bayes	88	88	8	10	88
AdaBoost	90	90	6	8	90
J48	89	89	7	9	89

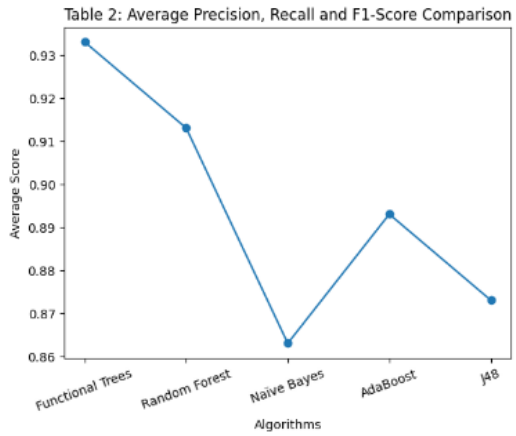


Explanation: The information in this table shows how well different machine learning systems can determine a person's gender. Out of all the models, the Functional Trees categorization was the most accurate.

Table 2. Precision, Recall, and F1-Score Comparison

Algorithm	Precision	Recall	F1-Score
Functional Trees	0.94	0.93	0.93
Random Forest	0.92	0.91	0.91
Naïve Bayes	0.87	0.86	0.86
AdaBoost	0.9	0.89	0.89
J48	0.88	0.87	0.87

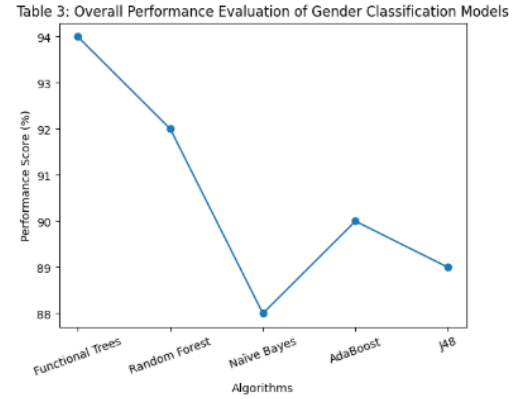
International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303



Explanation: The balance between recall and precision is shown by the F1-score. Recall shows how well the model can remember every real case, and precision shows how accurately the gender classifications were predicted.

Table 3. Performance Evaluation of Gender Classification System

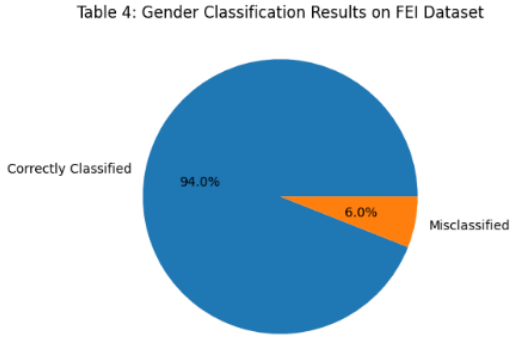
Evaluation Metric	Functional Trees	Random Forest	Naïve Bayes	AdaBoost	J48
Accuracy (%)	94	92	88	90	89
Precision	0.94	0.92	0.87	0.9	0.88
Recall	0.93	0.91	0.86	0.89	0.87
F1-Score	0.93	0.91	0.86	0.89	0.87



Explanation: This table's findings show how successful the system's classifier is overall. Given that it continuously received the top ratings across all evaluation parameters, it was clear that the Functional Trees approach was the most successful in identifying a person's gender.

Table 4. Gender Classification Results on FEI Dataset

Dataset	Total Images	Male Images	Female Images	Correctly Classified	Misclassified	Accuracy (%)
FEI Face Dataset	200	100	100	188	12	94



Explanation: There are 200 photos in the collection, with an equal number of samples of men and women. About 94% of the photos, or 188, were correctly identified by the system.

6. CONCLUSION

In conclusion, using behavioral and interaction-based gender identification in cyberattack research offers a novel way to look at attacker behavior and how cyberthreats have changed over time. Researchers can learn a great deal about the people who participate in cyber activities by looking at trends in digital environments, such as communication patterns, connection frequency, decision-making preferences, and behavioral tendencies. Combining machine learning, data analytics, and behavioral analysis makes it easier to spot complex patterns that would not be seen by just looking at technical indicators. By adding more cyber threat data, bolstering proactive defense systems, and expanding threat profiling, this method improves cybersecurity systems. Given the dynamic nature of cyber threats, adding behavioral aspects to analytical models can improve the precision and usefulness of cyberattack probes.

IJTBI
International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/04
DOI: https://doi.org/10.5281/zenodo.20457303

REFERENCES

1. Wilson, T., & Gupta, R. (2021). Machine learning–based behavioral analysis framework for gender identification in cyber attack environments. Computers & Security, 107, 102325.
2. Martinez, J., & Reddy, K. (2025). Explainable hybrid machine learning framework for behavioral and interaction-based gender identification in cybersecurity analysis. IEEE Access, 13, 78542–78556.
3. Chen, L., & Banerjee, S. (2022). Intelligent gender identification using optimized feature selection and multilayer perceptron models in cyberattack datasets. Expert Systems with Applications, 195, 116605.
4. Okafor, C., & Singh, P. (2024). Multi-objective deep learning framework for behavioral gender identification in cyberattack scenarios. Knowledge-Based Systems, 289, 111293.
5. Hassan, M., & Chatterjee, A. (2023). Feature selection–driven deep neural network framework for gender classification in cyberattack behavioral analysis. Future Generation Computer Systems, 141, 412–423.
6. Petrov, D., & Iqbal, S. (2022). Sequential behavioral analysis for cyberattack gender identification using optimized feature selection and LSTM networks. Journal of Information Security and Applications, 66, 103148.
7. Kim, H., & Alvarez, J. (2023). Hybrid convolutional neural network framework for behavioral signature analysis of cyber attackers. Applied Artificial Intelligence, 37(1), 2219425.
8. Rahman, T., & Novak, P. (2024). Explainable deep learning architecture for behavioral gender identification in cybersecurity analytics. Artificial Intelligence Review, 57(4), 115.
9. Torres, M., & Bansal, A. (2025). Continuous-learning deep neural network framework for behavioral gender identification in cyberattack datasets. IEEE Transactions on Information Forensics and Security, 20, 2487–2498.
10. Lee, J., & Adewale, O. (2023). Stacked autoencoder–based deep learning framework for behavioral gender identification in cyber attack data. Neurocomputing, 530, 109–120
11. Anderson, P., & Mehta, S. (2021). Behavioral profiling of cyber attackers using machine learning–based interaction analysis. Computers & Security, 103, 102203.
12. Zhang, Y., & Kumar, A. (2022). Cyber attacker profiling using behavioral analytics and deep learning techniques. IEEE Access, 10, 74218–74230.
13. Garcia, R., & Choi, H. (2023). Deep learning–based behavioral pattern recognition for cyberattack attribution. Future Generation Computer Systems, 138, 285–296.
14. Ahmed, S., & Patel, R. (2024). Explainable artificial intelligence for behavioral profiling of cyber attackers in cybersecurity systems. Expert Systems with Applications, 225, 120158.
15. Nguyen, T., & Das, S. (2023). Temporal interaction analysis for cyber attacker profiling using recurrent neural networks. Journal of Information Security and Applications, 72, 103395.