Network-Based Suspicious User Identification in Encrypted Chat Platforms Using Metadata Correlation and Machine Learning Techniques

Mrs. K. Sangeetha[1], Arithiran R. G[2], Arul Raj V[3], Jeremiah Renswick J[4]
[1]Assistant Professor, Department of Computer Science and Engineering Paavai Engineering College, Namakkal, India
[2,3,4] Department of Computer Science and Engineering Paavai Engineering College, Namakkal, India

***Abstract*—End-to-end encrypted messaging platforms such as WhatsApp and Telegram provide strong privacy guarantees by preventing unauthorized access to message content. However, these protections also create challenges for digital forensic investigators attempting to detect suspicious user behavior across encrypted communication environments. Traditional forensic approaches depend heavily on message content inspection, which is no longer feasible in modern encrypted messaging systems.**

This paper proposes a metadata-driven suspicious-user identification framework capable of detecting coordinated communication patterns across encrypted chat platforms without violating encryption integrity. The proposed system analyzes timestamps, packet size distributions, session durations, communication frequencies, device identifiers, and network traffic characteristics to identify anomalous behavioral patterns. A machine learning pipeline combining clustering, classification, and correlation scoring is introduced to detect suspicious users with high accuracy while preserving user privacy.

Experimental evaluation demonstrates that the proposed framework improves anomaly detection performance compared with baseline statistical methods and supports lightweight deployment in forensic analysis environments.

***Index Terms*—Encrypted Messaging, Metadata Analysis, Digital Forensics, Suspicious User Detection, Machine Learning, Network Behavior Analytics**

I. INTRODUCTION

Encrypted messaging platforms have become one of the most widely used communication tools in modern digital ecosystems. Applications such as WhatsApp, Telegram, Signal, and Messenger provide strong end-to-end encryption mechanisms that ensure confidentiality of user conversations. While encryption significantly enhances user privacy, it simultaneously introduces challenges for investigators attempting to detect malicious or coordinated communication activities.

Modern cybercrime operations frequently exploit encrypted messaging platforms to coordinate illegal activities such as fraud, cyber-attacks, financial laundering, misinformation propagation, and organized criminal communication. Since message content cannot be inspected directly, investigators must rely on alternative analytical approaches.

Metadata-based forensic analysis represents a promising solution for this challenge. Metadata describes contextual properties of communication events without revealing message content. Examples include timestamps, communication frequency, packet sizes, routing characteristics, and device- level identifiers.

This research proposes a lightweight metadata-driven suspicious-user identification system capable of detecting behavioral anomalies across encrypted messaging environments.

II. MOTIVATION

Traditional digital forensic systems rely heavily on access to plaintext communication content. However, modern encryption protocols prevent such access by design. Consequently, investigators require new approaches that preserve encryption integrity while

enabling detection of suspicious communication behavior.

Metadata provides sufficient contextual information to identify hidden communication relationships without violating privacy constraints. Analyzing metadata enables investigators to detect suspicious user clusters, coordinated communication bursts, abnormal session durations, and unusual packet transmission behavior.

The motivation behind this research is to design a privacy- preserving forensic framework capable of identifying suspicious communication patterns across encrypted messaging platforms using only metadata-based analysis techniques.

III. PROBLEM STATEMENT

Encrypted messaging platforms prevent investigators from directly accessing message content. This limitation creates challenges for digital forensic investigations attempting to detect suspicious user behavior across multiple communication channels.

Existing network monitoring tools such as Wireshark pro- vide packet-level traffic inspection capabilities but are not optimized for detecting cross-platform behavioral correlations between encrypted chat users.

Therefore, there is a need for a metadata-driven suspicious- user identification system capable of detecting coordinated communication behavior across encrypted messaging plat- forms without accessing message content.

IV. RESEARCH OBJECTIVES

The objectives of the proposed research include:

- Develop a metadata-based suspicious-user identification framework
- Detect abnormal behavioral patterns without decrypting messages
- Apply machine learning algorithms for anomaly detection
- Provide visualization dashboards for investigator interpretation
- Reduce manual effort in forensic traffic analysis
- Enable lightweight deployment in digital investigation environments

V. RESEARCH CONTRIBUTIONS

The primary contributions of this work include:

- A privacy-preserving suspicious-user detection frame- work
- Metadata correlation scoring model for encrypted chats
- Multi-s t a g e anomaly detection pipeline
- Visualization-driven forensic analysis dashboard
- Lightweight deployment architecture for investigators

VI. LITERATURE SURVEY

Recent advances in encrypted communication platforms have created new challenges for digital forensic investigators. Since message contents cannot be accessed directly, researchers have proposed metadata-based behavioral analytics approaches as an alternative strategy.

Graph-based anomaly detection methods model communication relationships between users as interaction networks. These approaches identify suspicious communities by analyzing edge weights, node centrality, interaction density, and clustering coefficients. However, many such models require long observation windows and large datasets.

Machine-learning-based anomaly detection techniques such as Support Vector Machines (SVM), Random Forest classifiers, and Isolation Forest models have demonstrated promising performance in detecting abnormal communication behavior using network traffic features.

Transformer-based models and deep sequence-learning architectures have recently been explored for log-level anomaly detection in cybersecurity applications. These models capture temporal dependencies in sequential communication behavior but require higher computational resources.

Metadata-driven forensic analysis frameworks provide an effective trade-off between privacy preservation and behavioral insight. By relying only on contextual communication attributes rather than message content, such systems enable investigators to identify suspicious users without violating encryption integrity.

VII. THREAT MODEL

The proposed suspicious-user identification framework assumes the presence of multiple adversarial behaviors within encrypted messaging environments.

A. Coordinated Communication Attacks

Groups of malicious users may coordinate activities using encrypted messaging platforms. Although message content remains hidden, their communication timing patterns often reveal correlation structures.

B. Bot-Driven Activity Patterns

Automated accounts frequently generate repeated traffic bursts with regular timing intervals. Such behavior differs significantly from human communication patterns and can be detected through metadata analysis.

C. Cross-Platform Identity Correlation

Suspicious actors may use multiple messaging platforms simultaneously. Metadata similarity across platforms can reveal identity linkage patterns.

D. Traffic Camouflage Attacks

Adversaries may attempt to disguise communication behavior using irregular message timing strategies. The proposed model addresses this challenge using multi-feature correlation scoring.

VIII. SYSTEM ARCHITECTURE

The proposed suspicious-user identification framework fol- lows a layered architecture consisting of six major processing components.

A. Metadata Collection Layer

This layer captures encrypted traffic metadata from monitored network interfaces. Captured attributes include:

- Timestamp sequences
- Packet size distribution
- Session initiation intervals
- Communication frequency
- Device-level identifiers

Collected metadata is stored in structured forensic datasets for further analysis.

B. Preprocessing Layer

Noise removal and normalization procedures improve dataset consistency. Duplicate traffic entries are removed and missing attributes are estimated using interpolation methods.

C. Feature Extraction Layer

Communication behavior indicators are extracted using statistical and temporal analysis techniques.
Examples include:

- Message burst frequency
- Average session duration
- Time-gap variance
- Packet-size entropy
- Communication periodicity index

D. Correlation Analysis Layer

This module computes similarity scores between user communication profiles using multi-dimensional feature vectors.

E. Machine Learning Layer

Anomaly detection algorithms identify suspicious behavioral clusters.

F. Visualization Layer

Results are presented using investigator-friendly dashboards containing network graphs and timeline analytics.

IX. METADATA CORRELATION MODEL

Let the metadata feature vector for user i be defined as:

$$F_i = (f_1, f_2, f_3, \ldots, f_n)$$

where each feature represents a behavioral communication attribute.

Similarity between two users i and j is computed using cosine similarity:

$$Sim(i,j) = \frac{F_i \cdot F_j}{|F_i|\,|F_j|}$$

Users with similarity scores above threshold θ are classified as potentially correlated suspicious entities.

X. FEATURE ENGINEERING PIPELINE

Effective suspicious-user detection depends heavily on selecting informative behavioral features.
The proposed feature engineering pipeline extracts the following metadata-derived attributes:

A. Temporal Features

- Message interval variance
- Communication start-time similarity
- Session synchronization score

B. Traffic Features

- Packet size entropy
- Burst density ratio
- Upload/download symmetry index

C. Device Features

- Device identifier reuse frequency
- IP switching probability
- Network location similarity score

XI. CORRELATION SCORING ALGORITHM

Algorithm 1 Metadata Correlation Scoring

Require: Feature vectors F_i, F_j
1: Compute cosine similarity
2: Compute time-gap similarity
3: Compute packet-distribution similarity
4: Aggregate weighted similarity score
5: return correlation score

XII. ISOLATION FOREST DETECTION ALGORITHM

Algorithm 2 Clustering-Based Detection

Require: Metadata feature dataset
1: Apply K-means clustering
2: Identify dense communication clusters
3: Detect outlier communication nodes
4: return suspicious cluster groups

Algorithm 3 Isolation Forest Detection

Require: Metadata dataset
1: Train isolation forest model
2: Compute anomaly scores
3: Rank suspicious users
4: return anomaly classification results

XIII. MACHINE LEARNING DETECTION PIPELINE

The proposed suspicious-user identification framework integrates a multi-stage machine learning pipeline designed to classify communication behavior based on metadata-derived feature vectors.
The pipeline consists of four major processing stages:

1) Dataset preparation
2) Feature normalization
3) Model training
4) Suspicious-user classification

During dataset preparation, communication metadata collected from network monitoring tools is transformed into structured feature vectors. Normalization improves classification performance by ensuring consistent feature scaling across all communication attributes.
The trained classification model generates anomaly scores for each user. Users exceeding predefined threshold values are marked as suspicious.

XIV. DATASET CONSTRUCTION FRAMEWORK

Since encrypted messaging platforms restrict direct access to message content, metadata-based datasets were constructed using simulated network-monitoring environments that emu- late encrypted chat behavior.
Each dataset entry contains:

- Communication timestamp
- Packet size
- Session duration
- Device identifier hash
- Communication frequency
- IP switching rate

The dataset includes both normal-user communication behavior and synthetically generated suspicious-user traffic pat- terns.
Synthetic suspicious behavior includes:

- synchronized message bursts
- periodic automated transmissions
- cross-platform interaction timing similarity

These synthetic behavioral injections enable supervised model training.

XV. TRAINING PIPELINE ARCHITECTURE

The training pipeline uses supervised and unsupervised anomaly detection models.
Supervised classification models:
- Support Vector Machine
- Random Forest Classifier
- Gradient Boosting Model Unsupervised anomaly detection models:
- Isolation Forest
- K-Means Clustering
- Density-Based Spatial Clustering (DBSCAN)

Hybrid classification improves suspicious-user detection ac- curacy by combining supervised prediction with unsupervised anomaly scoring.

XVI. EVALUATION METRICS

Model performance is evaluated using multiple classification metrics.

A. Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

B. Precision

$$Precision = \frac{TP}{TP + FP}$$

C. Recall

$$Recall = \frac{TP}{TP + FN}$$

D. F1 Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

These evaluation metrics ensure reliable classification per- formance.

XVII. EXPERIMENTAL RESULTS

Experimental evaluation demonstrates that metadata-based suspicious-user classification achieves strong performance across multiple datasets.
Random Forest classifiers achieved the highest detection accuracy due to their ability to model nonlinear feature re- lationships.
Isolation Forest models demonstrated strong performance in detecting outlier communication behavior without labeled training data.
Clustering-based approaches successfully identified coordinated user groups exhibiting synchronized communication behavior.

XVIII. VISUALIZATION ENGINE

Investigator interpretation plays an important role in digital forensic analysis. Therefore, the proposed framework integrates visualization modules that provide graphical representation of suspicious-user relationships.
Visualization outputs include:
- interaction graphs
- timeline correlation charts
- communication heatmaps
- anomaly-score dashboards

Graph visualization enables investigators to identify coordinated communication clusters quickly.
Timeline-based visualizations highlight synchronized messaging behavior across users.
Heatmaps reveal packet-distribution similarity patterns.

XIX. DEPLOYMENT ARCHITECTURE

The suspicious-user identification framework supports both centralized and distributed deployment models.
Centralized deployment architecture includes:
- network monitoring node
- metadata processing server
- machine learning engine
- visualization dashboard

Distributed deployment supports large-scale forensic monitoring environments across enterprise networks.
Edge-level metadata collectors transmit compressed communication features to centralized analysis engines.

XX. SCALABILITY CONSIDERATIONS

Scalability is an important requirement for real-world deployment in large communication networks.
The proposed framework supports horizontal scaling using distributed metadata collectors.
Feature extraction modules operate independently, allowing parallel processing across multiple nodes.
Machine learning classification tasks can be executed using cloud-based processing infrastructure.

This architecture ensures support for high-volume encrypted traffic analysis.

XXI. SECURITY ANALYSIS

The proposed framework maintains encryption integrity by avoiding message content inspection.
Security benefits include:
- privacy preservation
- encryption compliance
- metadata-only analysis
- resistance to content-based evasion attacks

Adversarial users attempting to modify communication timing behavior may reduce correlation strength but cannot fully eliminate behavioral signatures.
Multi-feature correlation scoring improves detection robust- ness.

XXII. PRIVACY PRESERVATION MODEL

Privacy preservation is a fundamental requirement for encrypted communication analysis systems.
The proposed framework ensures privacy protection through:
- metadata-only feature extraction
- anonymized device identifiers
- hashed network attributes
- restricted investigator access control

This approach ensures compatibility with modern privacy regulations.

XXIII. ETHICAL CONSIDERATIONS

Metadata-based suspicious-user detection systems must operate within legal and ethical boundaries.
The proposed framework follows ethical design principles including:
- privacy-preserving analytics
- investigator accountability
- transparent detection methodology
- minimal data collection policy

These safeguards ensure responsible forensic deployment.

XXIV. COMPARATIVE ANALYSIS

The proposed system was compared with existing metadata- based anomaly detection approaches.

TABLE I COMPARISON WITH EXISTING SYSTEMS

Method	Privacy Safe	Accuracy	Scalability
Content Inspection	No	High	Medium
Traffic Statistics	Yes	Medium	High
Graph Analytics	Yes	High	Medium
Proposed Model	Yes	High	High

The proposed framework demonstrates improved balance between privacy, accuracy, and scalability.

XXV. LIMITATIONS

Although the proposed system provides strong detection capability, some limitations remain.
Metadata-only analysis cannot reveal semantic meaning of communication content.
Highly adaptive adversaries may attempt to introduce artificial noise into communication timing patterns.
Future research should explore integration of behavioral fingerprinting techniques.

XXVI. FUTURE WORK

Future enhancements may include:
- Graph neural network integration
- transformer-based anomaly detection
- cross-platform identity linking
- federated learning deployment
- real-time suspicious-user detection

These improvements will enhance detection performance in large-scale communication environments.

XXVII. CONCLUSION

This paper presented a metadata-driven suspicious-user identification framework designed for encrypted messaging platforms.
The proposed system enables investigators to detect coordinated communication behavior without accessing message content.
Machine learning-based anomaly detection combined with metadata correlation improves suspicious-user identification accuracy while preserving privacy and encryption integrity.
Experimental evaluation demonstrates that the proposed framework provides a scalable and privacy-

compliant solution for forensic analysis of encrypted communication environments.

REFERENCES

[1] S. Alam and M. Faisal, "Anomaly Detection in Social Networks," IEEE Access.
[2] J. Su et al., "Transformer-Based Anomaly Detection Models," IEEE Transactions.
[3] O. A. Ekle and W. Eberle, "Dynamic Graph Anomaly Detection," ACM.
[4] M. Landauer et al., "Deep Learning Log Analysis," IEEE Security.
[5] L. Xing et al., "Social Network Anomaly Detection Survey," IEEE Access.
[6] W. Wang et al., "Encrypted Traffic Analysis Techniques," IEEE Communications.
[7] R. Sommer and V. Paxson, "Outside the Closed World," IEEE Security Privacy.
[8] T. Ahmed et al., "Network Traffic Classification Using ML," IEEE.
[9] Z. Lin et al., "Behavior-Based Intrusion Detection," IEEE.
[10] S. Axelsson, "Intrusion Detection Systems Survey," ACM.
[11] L. Breiman, "Random Forests," Machine Learning Journal.
[12] C. Cortes and V. Vapnik, "Support Vector Machines," Machine Learning.
[13] F. Pedregosa et al., "Scikit-Learn ML Library," JMLR.
[14] L. Ruff et al., "Deep One-Class Classification," ICML.
[15] M. Ester et al., "DBSCAN Algorithm," KDD.
[16] F. T. Liu et al., "Isolation Forest," ICDM.
[17] A. Patcha and J. Park, "Anomaly Detection Survey," Computer Net- works.
[18] S. Garfinkel, "Digital Forensics Research," IEEE Security.
[19] R. Anderson, "Security Engineering," Wiley.
[20] N. Provos and T. Holz, "Virtual Honeypots," Addison Wesley.
[21] K. Scarfone, "Guide to IDS," NIST.
[22] M. Bishop, "Computer Security," Addison Wesley.
[23] P. Barford et al., "Traffic Anomaly Detection," ACM.
[24] J. Ullrich, "Packet-Level Detection," SANS.
[25] T. Fawcett, "ROC Analysis," Pattern Recognition Letters.
[26] G. Hinton, "Deep Learning," Nature.
[27] Y. Bengio, "Representation Learning," IEEE.
[28] A. Krizhevsky, "CNN ImageNet," NIPS.
[29] I. Goodfellow, "GAN," NIPS.
[30] J. Dean, "Large-Scale Distributed ML," Google.
[31] OpenSSL Documentation.
[32] Wireshark Network Analyzer Manual.
[33] Zeek Network Monitoring Framework.
[34] ELK Stack Documentation.
[35] Apache Spark MLlib Documentation.
[36] TensorFlow ML Framework.
[37] PyTorch Documentation.
[38] Scapy Packet Analysis Library.
[39] NetworkX Graph Analytics Library.
[40] Matplotlib Visualization Toolkit.