Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Spoofing Detection in Mobile Environment using Machine Learning

Mrs Divyashree K[1], Mrs Smitha BN[2], Kiran Raj SD [3], Rakshitha TH [4],Sinchana S Ediga [5], Vandana HT [6]

[1,2] Assistant Professors, Information Science Engineering.
[3,4,5,6] Undergraduate Student, Information Science Engineering

Abstract

Smartphone technology has been increasing a lot over the last few decades. It finds use in various applications like communication, banking, shopping, and many more, etc. Spoofing attack is a cybercrime where an attacker tries to access your device to access and manipulate the information in your device. This unauthorized attack occurs by the attacker attempting to use a fake identity to access your device. Some spoofing attacks are IP Spoofing, GPS Spoofing, Biometric Spoofing, etc. This attack leads to compromised user privacy, data leak and system integrity.

Our proposed system is a spoofing detection system which uses machine learning and security analysis techniques. It collects data like network behavior, device identifiers, sensor information to identify suspicious activities. It uses Classification algorithms like Support Vector Machines (SVM), K-Nearest Neighbors(KNN), Decision Tree algorithms. The proposed system aims to provide real time detection and alert mechanisms to improve mobile security. Performance evaluation is carried out using metrics like accuracy, precision, recall. This project contributes to enhance security in mobile environments by providing intelligent and automated spoofing detection framework.

Keywords: Smartphone, Spoofing attack, Spoofing Detection, machine learning algorithms, real-time detection, Accuracy, Precision.

1. Introduction

The advent of technology led to creation of Smartphones, a device which is lightweight, portable, and works similar to laptops and computers. It is mainly used in communication, financing, healthcare, education, etc.

Smartphones are used to hold confidential data which must be accessed by authorized users. Unauthorized users can try to access and manipulate this data through Cyber attacks. One such attack is spoofing, where a fake identity is used to bypass the security measures in mobile device to access the data. This leads to data theft, data leaks, privacy violations, unauthorized system access, financial losses, etc.

The proposed system is a spoofing detection system where machine learning algorithms to enhance the detection of spoofing and malware and enhance the security of mobile devices. It analyzes various network parameters like user behavior, application permissions, network traffic, location information, and sensor data to identify abnormal activities. It can also assist users and organizations to protect sensitive information and ensure safe communication of information.

2. Literature Survey

Many studies have been done on Spoofing detection. They show that Spoofing models are created for specific types of spoofing attacks and how they change along with newer spoofing attacks.

Here are some of studies on Spoofing attacks and the models the researchers have proposed:

1. Detection of SMS and Caller ID Spoofing – Lee, Park, Kim (2019)

The paper proposes a detection framework for SMS and Caller ID spoofing by analyzing signaling and metadata patterns in mobile networks.

2. GPS Spoofing Detection in Mobile Devices – Kumar & Raj (2020)

The proposed model detects GPS spoofing attacks directly on mobile devices using sensor fusion and consistency checks. It uses lightweight machine learning classifier like SVM or Decision Tree to run on mobile without external support.

3. Wi-Fi Spoofing Attack Detection in Mobile Networks – Sharma, Verma, Gupta (2020)

This paper proposes a model to detect Wi-Fi hotspot spoofing (e.g., evil-twin APs) in mobile networks. It monitors Wi-Fi probe responses, beacon frames, and associated parameters (MAC address, BSSID, channel, RSSI, security flags).

It extracts features such as:
- Multiple APs with identical BSSID but different physical characteristics (RSSI patterns).
- Sudden changes in AP behavior or configuration.

It then applies a machine-learning classifier (e.g., SVM, random forest) trained on legitimate vs. spoofed AP signatures.

4. Mobile Spoofing Attack Detection Using Machine Learning– Smith, Brown, Taylor (2021)

The paper proposes a general machine-learning-based framework for detecting various mobile spoofing attacks (SMS, caller ID, location, Wi-Fi, etc.).

It uses an ensemble ML model (e.g., random forest and neural network) to classify traffic/behavior as spoofed or legitimate. The model is designed as a layered detection system that can be deployed at network, OS, or app levels.

5. Biometric Spoofing Detection for Smartphones – Ahmed & Khan (2021)

The proposed model detects spoofed biometric inputs (face, fingerprint, voice) on smartphones.

It extracts: quality metrics (e.g., skin texture, reflection patterns for face; ridge continuity for fingerprints) and feeds them into a deep learning model (e.g., CNN for images, RNN for sequences) trained to distinguish real vs. spoofed biometrics (e.g., photos, masks, synthetic fingerprints, recorded voice).

The model outputs a spoof probability; the smartphone can then reject the authentication or request additional verification.

6. IoT and Mobile Device Spoofing Prevention Framework – Fernandez, Roy, Singh (2021)

The paper discusses a comprehensive framework to prevent spoofing across IoT and mobile devices.

The model runs ML-based anomaly detection models per domain (IoT, mobile) and enforces policies (block, quarantine, re-authenticate) when spoofing is detected.

7. Android Malware and Application Spoofing Detection – Chen, Zhao, Wang (2022)

The core idea of this paper is to create a model to detect Android malware and application spoofing (e.g., fake apps masquerading as legitimate ones).

The Proposed model uses static analysis of APKs, extracts permissions, API calls, package names, icons, and manifest attributes and builds feature vectors representing app behavior and identity.

The model is based of deep learning model (e.g., CNN over app "images" or embeddings, or a hybrid CNN+RNN over API sequences) to: classify apps as benign/malware and detect spoofed apps by comparing against known legitimate app signatures.

8. Real-Time Spoofing Detection System for Smartphones – Johnson, Williams, Clark (2022)

The paper proposes real-time, on-device system to detect spoofing attacks while the phone is in use.

The proposed model continuously monitors Network traffic (SMS, call logs, Wi-Fi connections), Location sensors (GPS, Wi-Fi/cell) and Application behavior (unnatural permission usage, background activities).

It uses lightweight ML models (e.g., logistic regression, small neural networks) optimized for low latency and low resource usage to make decisions (e.g., "this SMS is likely spoofed", "this AP is suspicious") and

triggers alerts or blocks actions in real time.

9. Machine Learning Based Mobile Security Framework – Patel, Mehta, Joshi (2023)

It proposes a mobile security framework that integrates multiple ML-based detectors for various spoofing and malware threats.

10. Deep Learning Approach for Mobile Spoofing Detection – Wang, Liu, Zhou (2023)

The paper proposes a deep learning-based system for detecting multiple types of mobile spoofing attacks.

The proposed model analyzes Network logs (SMS, calls), Location data, Wi-Fi and cell network information and App behavior indicators.
It uses a deep neural architecture (e.g., multi-head CNN/LSTM or transformer-style model) that learns joint representations across modalities and detect subtle patterns indicative of spoofing.

11. FakeAP Detector: An Android-Based Client-Side Application for Detecting Wi-Fi Hotspot Spoofing – Mwinuka et al. (2022)

The model proposes an Android app that detects Wi-Fi hotspot spoofing (evil-twin APs) without requiring root access.

It collects probe responses from nearby APs, including BSSID, MAC, channel, RSSI, security capabilities.
It compares observed AP characteristics against a reference of known legitimate APs (e.g., from prior scans or a database).

It uses an ML classifier to identify:
- APs with identical BSSID but inconsistent RSSI patterns.
- APs with suspicious configuration changes.

The paper reports detection accuracy of ~99% in open networks and ~99.7% in closed networks

12. Slice-Aware Spoofing Detection in 5G Networks Using Lightweight Machine Learning – Ganiuly & Bolatbek (2025/2026)

The paper proposes a model to detect spoofing attacks within 5G network slices using lightweight ML, tailored to each slice's traffic characteristics.

13. Android Malware Detection using Machine Learning: A Review – Chowdhury et al. (2023)

This review paper summarizes existing ML-based Android malware detection approaches.
The paper describes common deep learning algorithms like SVM, decision trees, random forests, CNNs,

RNNs/LSTMs, hybrid CNN+LSTM, where the typical performance is around 95–99% accuracy, but with issues like dataset bias and lack of standard evaluation metrics

14. A New Android Malware Detection Approach Using Bayesian Classification – Yerima, Sezer, McWilliams, Muttik

The proposed model in this paper uses Bayesian classification for Android malware detection. It extracts features from APKs (e.g., permissions, API calls, manifest attributes) and builds a probabilistic model using Bayesian classification

The paper estimates the probability that an app is malware given its feature vector. The model trains on labeled datasets of benign and malicious apps.

15. Detecting Android Malware Leveraging Text Semantics of Network Flows – Wang, Yan, Chen, Yang, Zhao, Conti

The model detects Android malware by analyzing the semantic content of network flows, treating them as text. It captures network flows from apps (e.g., HTTP/HTTPS requests, DNS queries) and converts flow data into textual sequences (e.g., URLs, domain names, request parameters) to learn patterns typical of malicious apps (e.g., communication with known bad domains, suspicious payload structures).

The model is created by training a classifier to distinguish benign vs. malware based on these semantic representations.

3. Methodology

The System we propose is an intelligent spoofing detection framework designed to improve security in mobile environments using Machine Learning and Behavioral analysis techniques. The system monitors activities like application behavior, GPS location, sensor data to identify suspicious behavior. We can identify various Spoofing attacks like IP Spoofing, GPS Spoofing through continuous data analysis and monitoring

.

The collected data is preprocessed and analyzed using machine learning algorithms like Support Vector Machines(SVM), Decision Trees, K-Nearest Neighbors(KNN). They help classify activities as normal or malicious with higher accuracy. The system will also send real-time notifications whenever spoofing attacks are detected, helping users take immediate security actions. The proposed system provides better adaptability, higher detection accuracy, lower resource consumption and enhance protection of sensitive information in mobile environment.

Training Data Collection: The training is created by collecting user behaviors and activities that are already classified as either normal or malicious activity. It is better to have the data labeled correctly when used for training the model.

Data Preprocessing and Feature Extraction: The training data may have unwanted noise or missing features. It is necessary to process and remove missing data or noise .The important features are then extracted.

Machine Learning Model: A suitable machine learning algorithm like Support Vector Machine(SVM), Decision Tree is selected to be trained using the training dataset to create a spoofing detection model.

Testing of Model: The model is tested with real-time activities to see if it can accurately classify the actions as either malicious or normal. For malicious activities, the model should send alert or notifications to the authorized user. For normal usage, the model should not raise any alerts or it should flag the activity as normal. The accuracy of the model is calculated. If the accuracy is less than ideal, another machine learning algorithm can be used. We take the model with highest accuracy.

Model Deployment: The model with highest accuracy is chosen to be implemented in the spoofing detection framework application. The application must be maintained and updated regularly to avoid future spoofing attacks.

A Comparision to other Existing Detection Models: The System we proposed is more useful in these areas:

1.**Traditional Security Mechanisms**: Existing mobile security systems mainly use passwords, antivirus software, and firewalls to protect devices from unauthorized access and malware attacks.

2.**Signature-Based Detection**: Most systems identify spoofing attacks using predefined attack signatures

and stored threat databases. These methods are effective only for known attacks.

3.**Biometric and Two-Factor Authentication**: Some applications use fingerprint scanning, face recognition, and OTP-based authentication to improve user security and prevent unauthorized access.

4.**Dependency on Regular Updates**: Traditional security systems require continuous updates of virus definitions and attack signatures to detect newly developed spoofing techniques.

5.**Limited Detection of Advanced Attacks**: Existing systems struggle to identify unknown or dynamically changing spoofing attacks because they rely mainly on fixed rules and patterns.

6.**High Resource Consumption**: Continuous monitoring and scanning can increase CPU usage, memory usage, and battery consumption in mobile devices.

7.**False Alerts and Reduced Accuracy**: Many existing systems may incorrectly identify normal activities as threats, resulting in false positives and reduced reliability.

8.**Lack of Real-Time Intelligent Analysis**: Traditional systems do not effectively analyze user behavior and network activities in real time, making early spoofing detection difficult.

Applications of Proposed model:

1. Mobile Banking Security: Protects users from spoofing attacks during online banking and digital payment transactions.

2. Secure Communication: Prevents fake SMS, caller ID spoofing, and phishing attacks in mobile communication systems**.**

3. GPS and Navigation Protection: Detects GPS spoofing attacks in navigation, ride-sharing, and location-based applications.

4. Wi-Fi Network Security: Identifies fake Wi-Fi access points and prevents unauthorized network access**.**

5. Biometric Authentication Systems: Enhances security in fingerprint and face recognition systems by detecting biometric spoofing attempts.

6. Enterprise Mobile Security: Protects organizational mobile devices and confidential business data from cyber threats.

7. Mobile Malware Detection: Helps identify malicious applications that imitate trusted apps or services.

8. E-Commerce and Online Transactions: Improves security during online shopping and digital wallet

transactions.

9. IoT and Smart Device Security: Provides protection for connected mobile and IoT devices against spoofing-based cyberattacks.

10. Cybersecurity and Digital Forensics: Assists security analysts in monitoring, detecting, and investigating spoofing attacks in mobile environments.

Limitations: The main limitations this system may face are:

• **Limited Detection Capability:** This model may not be able to detect different attacks from spoofing attacks. Spoofing attacks may become more advanced in the future and may avoid being detected.

• **High False Positive Rate:** The model might mistake normal behaviors with malicious attacks. It can occur if model is not trained with newer data regularly**.**

• **Lack of Real-Time Detection:** The training dataset may be made with examples, which is different from real time data. When working with real data, it may make mistakes**.**

• **High Resource Consumption:** A mobile device has less resources compared to computers and laptops. So, models used for laptops and computers may not work with mobiles**.**

• **Reduced Accuracy:** Some machine learning algorithms may not provide the ideal accuracy of detecting malicious activities**.**

• **Scalability Issues:** The model may face problems when used on device other than the ones it is suitable, which means model may suitable for all mobile devices.

4. Expected Conclusion:

1. **Accuracy**: The accuracy of the model proves how the model will handle with normal activity and malicious activity. An ideal model must have a high detection accuracy

2. **Resource Consumption**: The model is created to use as less resources as possible. A preferable model must use less resources to detect fraudulent activity.

3. **Detection Time:** The model must be able to differentiate between a spoofing attack and regular activity in less time as possible as we may not know if our device is spoofed when the attack occurs unless the model detects it.

4. **Alert Notification:** The model must send an notification to the user when malicious activity is detected so that the authorized user can prevent any kind of losses or failures from the attack.

References

1. H. Lee, J. Park, and K. Kim, "Detection of SMS and Caller ID Spoofing," International Conference on Mobile Security, pp. 67–73, 2019.
2. R. Kumar and S. Raj, "GPS Spoofing Detection in Mobile Devices," IEEE Transactions on Information Security, vol. 8, no. 2, pp. 120–128, 2020.
3. P. Sharma, D. Verma, and N. Gupta, "Wi-Fi Spoofing Attack Detection in Mobile Networks", International Journal of Network Security, vol. 14, no. 4, pp. 201–209, 2020.
4. J. Smith, A. Brown, and R. Taylor, "Mobile Spoofing Attack Detection Using Machine Learning",International Journal of Mobile Computing and Technology, vol. 12, no. 3, pp. 45–52, 2021.
5. A. Ahmed and F. Khan, "Biometric Spoofing Detection for Smartphones", Journal of Cybersecurity and Privacy, vol. 5, no. 1, pp. 89–97, 2021.
6. L. Fernandez, P. Roy, and M. Singh, "IoT and Mobile Device Spoofing Prevention Framework", International Journal of IoT Security and Applications, vol. 7, no. 3, pp. 98–107, 2021.
7. Y. Chen, M. Zhao, and L. Wang, "Android Malware and Application Spoofing Detection", IEEE Access, vol. 10, pp. 33421–33430, 2022.
8. M. Johnson, T. Williams, and S. Clark, "Real-Time Spoofing Detection System for Smartphones", Journal of Mobile Information Systems, vol. 18, no. 2, pp. 75–84, 2022.
9. S. Patel, R. Mehta, and K. Joshi, "Machine Learning Based Mobile Security Framework," IEEE International Conference on Smart Computing, pp. 155–161, 2023.
10. X. Wang, Y. Liu, and H. Zhou, "Deep Learning Approach for Mobile Spoofing Detection," IEEE Access, vol. 11, pp. 44510–44520, 2023
11. LUNODZO J. MWINUKA , ABEL Z. AGGHEY, SHUBI F. KAIJAGE , (Senior Member, IEEE),AND JEMA D. NDIBWILE: FakeAP Detector: An Android-Based Client-Side Application for Detecting Wi-Fi Hotspot Spoofing Digital Object Identifier 10.1109/ACCESS.2022.3146802
12. Daniyal Ganiuly, Nurzhau Bolatbek : Slice-Aware Spoofing Detection in 5G Networks Using Lightweight Machine Learning
13. Md Naseef-Ur-Rahman Chowdhury, Ahshanul Haque, Hamdy Soliman, Mohammad Sahinur Hossen, Tanjim Fatima, and Imtiaz Ahmed ; Android Malware Detection using Machine learning: A Review
14. Suleiman Y. Yerima, Sakir Sezer, Gavin McWilliams (Centre for Secure Information Technologies),.Igor Muttik (Senior Research Architect): A New Android Malware Detection Approach Using Bayesian Classification
15. Shanshan Wang, Qiben Yan, Member, IEEE, Zhenxiang Chen , Bo Yang, Chuan Zhao, and Mauro Conti, Senior Member, IEEE: Detecting Android Malware Leveraging Text Semantics of Network Flows