

Attack Modeling and Security Analysis Using Machine Learning Algorithms Enabled with Augmented Reality and Virtual Reality

Momina Mushtaq

Shri Mata Vaishno Devi University/Electronics and Communication Engineering, Katra, 182320, India
E-mail: mominamushtaq2@gmail.com

Rakesh Kumar Jha*

IIITDM Jabalpur/Electronics and Communication Engineering, Katra, 182320, India and Central University Jammu, Bagla Suchani, Jammu and Kashmir, India
E-mail: jharakesh.45@gmail.com
ORCID iD: <https://orcid.org/0000-0001-7321-4753>

*Corresponding author

Manish C. Sabraj

Shri Mata Vaishno Devi University / Electronics and Communication Engineering, Katra, 182320, India
E-mail: manish.sabraj@gmail.com

Shubha Jain

Department of Telecommunication, University of Maryland, College Park, Maryland, USA
E-mail: shubhajain1203@gmail.com

Received: 24 May 2023; Revised: 19 October 2023; Accepted: 13 December 2023; Published: 08 August 2024

Abstract: Augmented Reality (AR) and Virtual Reality (VR) are innovative technologies that are experiencing a widespread recognition. These technologies possess the capability to transform and redefine our interactions with the surrounding environment. However, as these technologies spread, they also introduce new security challenges. In this paper, we discuss the security challenges posed by Augmented reality and Virtual Reality, and propose a Machine Learning-based approach to address these challenges. We also discuss how Machine Learning can be used to detect and prevent attacks in Augmented reality and Virtual Reality. By leveraging the power of Machine Learning algorithms, we aim to bolster the security defences of Augmented reality and Virtual Reality systems. To accomplish this, we have conducted a comprehensive evaluation of various Machine Learning algorithms, meticulously analysing their performance and efficacy in enhancing security. Our results show that Machine Learning can be an effective way to improve the security of Augmented reality and virtual reality systems.

Index Terms: Algorithms, Augmented Reality (AR), Machine Learning, Security, Virtual Reality (VR).

1. Introduction

The technology, Augmented Reality (AR) and Virtual Reality (VR) have emerged as groundbreaking innovations, revolutionizing how we perceive and interact with the world around us. AR and VR offer immersive experiences, enabling users to explore captivating virtual realms and augment their perception of reality. However, with the increasing integration of AR and VR into various sectors, ensuring robust security measures becomes imperative to safeguard users and protect sensitive data.

Augmented Reality (AR) is a technology that overlays virtual elements onto the real world, enhancing our perception and interaction with the environment. AR typically involves the use of a device, such as a smartphone or smart glasses, which superimposes computer-generated graphics, text, or images onto the user's view of the physical world. This integration of virtual and real elements creates a seamless blend, augmenting the user's reality with additional information or digital enhancements [1]. Virtual Reality (VR), on the other hand, immerses users in a completely virtual environment,

shutting out the physical world. Through the use of specialized VR headsets or goggles, users can enter and interact with computer-generated environments that simulate real-world experiences or transport them to entirely fictional realms. VR offers a heightened sense of presence, enabling users to engage with virtual objects, explore simulated worlds, and even collaborate with others in virtual spaces [2].

The applications of AR and VR are diverse, spanning numerous industries and sectors. In the entertainment realm, AR and VR have transformed the gaming experience, allowing players to dive into lifelike virtual worlds, interact with virtual characters, and engage in immersive gameplay. Additionally, AR has found utility in medical training and patient care [3].

Surgeons can employ AR to overlay visualizations of critical data onto a patient's body during surgical procedures, aiding in precise interventions. VR, on the other hand, enables healthcare professionals to simulate challenging scenarios, providing immersive training experiences and refining their skills in a risk-free environment [4].

Beyond entertainment and healthcare, AR and VR have made significant inroads in industries such as architecture and engineering, retail and e-commerce, tourism, and real estate. These technologies empower architects to visualize and present design concepts to clients, allow retailers to offer virtual shopping experiences, enable virtual tourism explorations, and provide immersive virtual property tours to potential buyers.

AR/VR are widely used in various industries because AR/VR technologies offer benefits such as improved learning outcomes, reduced costs, increased productivity, and improved customer service [5].

As Augmented Reality (AR) and Virtual Reality (VR) continue to reshape industries and redefine user experiences, ensuring robust security measures is of paramount importance. The diverse applications of AR and VR necessitate the protection of user data, content integrity, and intellectual property. By addressing cybersecurity threats, implementing strong encryption and access control measures, and fostering user trust, we can unlock the full potential of AR and VR while creating a safe and secure immersive environment for users to explore, create, and interact within these transformative realms [6].

Machine Learning (ML) offers significant potential in reducing security risks in AR and VR environments. By harnessing the power of ML algorithms, security measures can be strengthened to mitigate vulnerabilities and protect users' sensitive information. ML algorithms can analyze vast amounts of data generated within AR/VR systems in real-time, allowing for the detection and identification of anomalous or suspicious activities. These algorithms can learn patterns of normal behavior and distinguish them from potential threats, enabling early warning systems and proactive defense mechanisms. Additionally, ML algorithms can adapt and evolve as new security risks emerge, continuously updating their models to stay ahead of malicious actors. By leveraging ML techniques, AR/VR systems can enhance authentication, access control, and intrusion detection, making them more resilient against cyber-attacks and ensuring a safer and more secure and immersive experience for users.

Contribution

This paper explores the emerging technologies of Augmented Reality (AR) and Virtual Reality (VR) and their potential to transform our daily lives. It presents a comprehensive compilation of extensive research that has been carried out in this particular field. It emphasizes the growing need for security measures as AR/VR technology advances. Furthermore, the paper proposes a Machine Learning-based approach to enhance security in AR/VR systems. It assesses the performance of various Machine Learning algorithms and identifies the algorithm that exhibits the most optimal performance.

2. Literature Survey

Over the past few years, the rapid progression of technology has brought about significant transformations in various domains, including the realm of cybersecurity. As organizations increasingly rely on interconnected systems and networks, the threat landscape continues to evolve and grow in complexity. To mitigate the risks associated with cyber-attacks, it becomes crucial to develop robust security mechanisms and strategies. In this regard, the integration of Machine Learning algorithms with Augmented Reality (AR) and Virtual Reality (VR) technologies has emerged as a promising approach for attack modelling and security analysis. Machine learning algorithms have demonstrated exceptional capabilities in analysing vast amounts of data and identifying patterns, making them well-suited for detecting and mitigating cyber threats.

By harnessing the power of machine learning, security professionals can gain valuable insights into attack patterns, identify vulnerabilities, and enhance the overall security posture of their systems.

The authors in [7] provide a comprehensive examination of the integration between mobile augmented reality (AR) and 5G mobile edge computing (MEC). The paper explores various aspects, including architectures, applications, and technical considerations related to this integration. The paper aims to offer a deep understanding of the state-of-the-art advancements in this field and serves as a valuable resource for researchers, practitioners, and decision-makers. By analysing existing literature and research findings, the paper sheds light on the potential benefits, challenges, and future directions of mobile AR with 5G MEC, contributing to the advancement and development of this emerging technology.

The authors of [8] presents an innovative approach that combines Augmented Reality (AR) with dynamic image recognition technology based on deep learning algorithms. The aim of the research is to enhance the accuracy and real-

time recognition of dynamic objects in AR applications. It addresses the limitation of traditional neural networks by integrating convolutional neural networks (CNN) with the XGBOOST algorithm for recognition.

The authors in [9] suggested the design and evaluation of a deep learning recommendation-based Augmented Reality (AR) system for teaching programming and computational thinking. Through empirical studies and user feedback, the system has demonstrated its effectiveness in providing personalized recommendations, enhancing engagement, and improving learning outcomes. The integration of AR technology with deep learning algorithms offers a unique and interactive learning experience, enabling students to develop programming skills and computational thinking in a personalized and immersive manner.

Table 1. Literature review

Ref.	Objective	Outcome	Applications	Advantages	Disadvantages
[7]	To conduct a comprehensive survey on the integration of mobile augmented reality (AR) with 5G mobile edge computing (MEC) technology.	It provides a comprehensive understanding of the state-of-the-art advancements, applications, architectures, and technical considerations in the integration of mobile augmented reality (AR) with 5G mobile edge computing (MEC).	Enhanced Gaming, Entertainment, Remote Collaboration, Smart Retail, Education and Training.	Real-time Data Analytics, Enhanced User Experience and Lower Latency.	Security and Privacy Concerns, high cost and Network dependence.
[8]	To develop a robust system that can recognize and track dynamic objects in the user's environment, enabling a seamless and immersive AR experience.	It presents a novel augmented reality (AR) dynamic image recognition technology based on deep learning algorithms. It aims to achieve improved accuracy and efficiency in real-time image recognition for AR applications and provide a robust and reliable solution for dynamic object recognition.	Healthcare, Training, Navigation and Manufacturing.	Real-Time Recognition and low error rate.	Training data requirements and large data set required.
[9]	To design and evaluate a deep learning recommendation-based augmented reality (AR) system for teaching programming and computational thinking.	It highlights the potential of using AR and deep learning algorithms in programming education, showcasing improved learning outcomes and increased engagement among students.	Education and learning.	Personalized learning, Improved learning outcomes and Enhanced engagement.	Privacy and Security Concerns, Constraints in terms of availability and cost.
[10]	To investigate and develop robust machine learning algorithms that can effectively identify and classify steady-state visual evoked potentials (SSVEPs), enabling more accurate and reliable control of wearable devices through brain signals	It demonstrates the effectiveness of the proposed machine learning algorithms in accurately identifying and classifying SSVEPs. The outcome showcases improved classification accuracy, leading to more reliable and precise control of wearable devices using brain signals.	Neurorehabilitation, Gaming, Cognitive assessment and Training.	Improved classification Accuracy, Versatility and Adaptability.	Need for Training Data, and Individual Variability.
[11]	To address the challenges of navigating complex indoor environments and ensuring efficient emergency evacuations.	showcases the system's ability to enhance indoor navigation by utilizing machine learning algorithms to accurately track user locations and provide personalized directions. Indoor navigation, Emergency evacuation, Smart homes and apartments	Indoor navigation, Emergency evacuation, Smart homes and apartments.	Enhanced navigation Accuracy, Real-time guidance and Emergency preparedness.	Environmental limitations, Infrastructure requirements, Privacy and security concerns.
[12]	To develop a reliable and intelligent system that can analyze medical data, including imaging and clinical information, using deep learning algorithms to provide accurate COVID-19 diagnoses.	It leverages extended reality (XR) and deep learning techniques and integrates various data sources, including clinic data and medical imaging, to provide accurate and reliable COVID-19 diagnoses.	Telemedicine and Remote consultations.	Improved diagnostic Accuracy, Remote accessibility, Timely diagnosis and treatment.	Technical expertise and Infrastructure.
Our paper	To address the security challenges posed by AR and VR, and propose a Machine Learning-based approach to address these challenges. Also, evaluate the performance of the different Machine Learning algorithms, and identify the algorithm that provides the best performance.	The proposed model effectively addresses the research gap identified in the above existing approach by providing solutions that lead to complexity reduction, high accuracy, and enhanced security.	Healthcare, Gaming, Medical pharmacy, Education etc.	Low computational time, High accuracy, less Complex, No infrastructure requirements, High security, Lower cost, Adapts to changes.	NA

The authors in [10] put forth a method to enhance the classification of steady-state visual evoked potentials (SSVEPs) in BCI-based wearable instrumentation using machine learning techniques. The application of these techniques has resulted in improved classification accuracy, enabling more reliable and precise control of wearable devices through brain signals. The proposed method holds significant potential in various applications, including assistive technologies, virtual reality, neurorehabilitation, gaming, and cognitive assessment.

The authors in [11] present an indoor Augmented Reality (AR) navigation and emergency evacuation system based on Machine Learning and IoT technologies. The system proposed offers enhanced navigation accuracy, real-time guidance, and improved emergency preparedness in complex indoor environments. The authors leverage Machine Learning algorithms and IoT integration and developed a system that provides users with personalized directions and evacuation instructions, promoting efficient and safe navigation.

The authors in [12] present a trustworthy and intelligent COVID-19 diagnostic system based on extended reality (XR) and deep learning techniques, integrated with the Internet of Medical Things (IoMT). The method utilizes XR technologies to access clinic data and employs deep learning algorithms to enhance the accuracy and efficiency of COVID-19 diagnosis. The system offers advantages such as improved diagnostic accuracy, timely treatment.

The literature survey makes it evident that Augmented Reality (AR) and Virtual Reality (VR) technologies bring forth inherent security concerns, necessitating the implementation of robust security measures. In response to this pressing issue, we have introduced a cutting-edge Machine Learning-based approach to tackle the diverse security challenges posed by AR/VR. Our proposed model has demonstrated exceptional efficiency and security, significantly alleviating the identified research gaps present in the existing survey. Notably, our method excels in mitigating complexity, enhancing accuracy, and fortifying overall security aspects, thereby providing a comprehensive solution to the security issues previously encountered in AR/VR environments. With this approach, we aim to foster a safer and more reliable foundation for the widespread adoption of AR/VR technologies in various domains.

2.1. Machine Learning

Machine learning is a subfield of artificial intelligence (AI) that empowers computers to acquire knowledge from data and make predictions or decisions autonomously, without relying on explicit programming instructions [13]. By analysing large volumes of data, the Machine Learning algorithms can discover patterns and relationships, allowing for the development of intelligent systems. Machine learning has diverse applications, ranging from healthcare to finance, and its future holds promises of advancements in deep learning and edge computing. It is a transformative field within artificial intelligence that has revolutionized various industries. Its ability to process and analyse vast amounts of data has opened up new possibilities for intelligent decision-making [14].

The fundamental concepts of machine learning include:

- **Data:** The foundation of ML lies in data. Large volume of labeled or unlabeled data are used to train models, making it crucial to have high-quality, representative datasets.
- **Training:** During the training phase, ML models learn patterns and relationships within the data. This process involves feeding the model with input and expected output, allowing it to adjust its internal parameters iteratively.
- **Algorithms:** ML algorithms can be broadly classified into three categories: supervised learning, unsupervised learning, and reinforcement learning. Supervised learning uses labeled data to train models, while unsupervised learning finds patterns and structures in unlabeled data. Reinforcement learning involves an agent interacting with an environment and learning from feedback to maximize a reward signal.

2.2. Machine Learning Algorithms

Machine learning algorithms are the fundamental building blocks of the field of Machine Learning, empowering computers to acquire knowledge from data and make informed predictions. These algorithms are designed to extract patterns, relationships, and insights from datasets, allowing machines to generalize from the training data and apply that knowledge to new, unseen instances. Some commonly used Machine Learning algorithms are:

- **Support Vector Machines (SVM):** It is a versatile and widely-used Machine Learning algorithm that has proven effective in both classification and regression tasks [15]. SVMs are particularly well-suited for problems with complex decision boundaries and can handle high-dimensional data efficiently. The core concept of Support Vector Machines (SVM) revolves around discovering a hyperplane that effectively separates distinct classes while preserving a margin of separation. This margin represents the distance between the hyperplane and the nearest data points from each class. By seeking the optimal hyperplane, SVM aims to maximize this margin, which enhances its ability to generalize and perform well. Support vectors, in SVM, correspond to the data points that reside closest to the decision boundary or hyperplane. These data points play a critical role in defining the decision boundary and determining the optimal hyperplane. SVM focuses on these support vectors during the training process, making it memory-efficient for large datasets.
- **Decision Trees:** They are highly interpretable Machine Learning algorithms that can handle both classification and regression tasks. They offer a clear and intuitive representation of the decision-making process by

constructing a tree-like structure. Decision Trees consist of nodes that represent features or decisions. The root node represents the initial decision, and subsequent nodes, called internal nodes, represent intermediate decisions based on different features. Leaf nodes, also known as terminal nodes, represent the final outcomes or predictions. Branches connect nodes and represent the different outcomes or paths that can be taken based on the feature values. Each branch corresponds to a specific value of a feature.

- **K-Nearest Neighbors (KNN):** It is an intuitive Machine Learning algorithm that finds applications in both classification and regression tasks. It belongs to the family of instance-based or lazy learning algorithms, as it does not explicitly learn a model but instead stores the training data and makes predictions based on the similarity of new instances to the existing data points. KNN operates on the principle of finding the k nearest neighbors to a given instance in the feature space. The " k " represents the number of neighboring data points that will be considered when making predictions. To determine the proximity between instances, a distance metric is used. Popular distance metrics commonly employed in data analysis include Euclidean distance, Manhattan distance, and cosine similarity. The selection of a suitable distance metric relies on the specific characteristics of the data and the requirements of the problem being addressed.

3. System Model

The system architecture shown in Fig.1, is designed with a hierarchical structure that enables seamless interaction between the master device and the slave device. This architecture is optimized to enhance the overall user experience by combining precise control and data transmission with immersive haptic feedback, resulting in a compelling and realistic audio-visual and tactile encounter. In this architecture, the master device acts as the central control unit, responsible for transmitting vital command signals, as well as precise position and velocity information, through a secure communication network. The slave device, on the other hand, receives these commands and provide haptic feedback, enriching the user experience with realistic audio/video, surface texture, and force/position sensations.

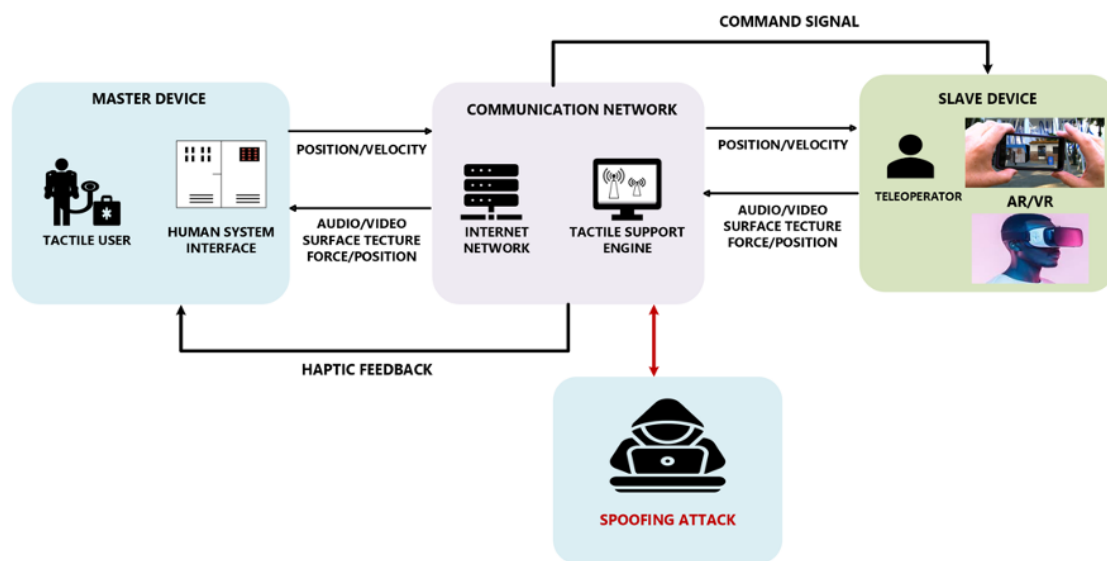


Fig.1. System architecture

While this architecture greatly enhances the immersion and engagement of users in AR/VR environments, it also introduces potential security vulnerabilities that must be addressed. One such vulnerability arises in the form of spoofing attacks, where malicious actors attempt to deceive the system by transmitting falsified command signals or manipulating the data transmitted between the master and slave devices. These attacks can occur at various points within the communication network, including between the master device and the slave device or even during data transmission over the secure communication network itself. Such actions are undertaken with the intention of manipulating the behavior of the AR/VR system, leading to adverse consequences for users and the overall system functionality. The implications of successful spoofing attacks in AR/VR environments are multi-faceted and far-reaching. Firstly, privacy breaches can occur if attackers gain unauthorized access to sensitive user data or personal information through the compromised system. Since AR/VR experiences often involve interactive and personalized content, protecting user privacy is of utmost importance to maintain trust and confidence in the technology. Secondly, spoofing attacks can lead to unauthorized access to the AR/VR system itself. This could potentially result in unauthorized control of the system, unauthorized manipulation of user experiences, or even the injection of harmful content, endangering user safety. Furthermore, these attacks could distort the real-world perception of users in the virtual environment, leading to physical harm if users are misled into interacting with objects or environments that are not actually present in reality.

To address the security risks associated with such attacks we propose a Machine Learning (ML) based security system as a powerful solution. ML algorithms can play a vital role in analyzing incoming command signals, detecting anomalies, and distinguishing between legitimate and potentially malicious inputs, thus bolstering the system's defence against spoofing attempts. The first step in leveraging ML for security is to train the algorithms on vast datasets that encompass a wide range of legitimate command patterns. These datasets are carefully curated to represent the typical behaviors and commands that the system should encounter during normal operations. By exposing the ML models to this diverse and comprehensive training data, they can learn to recognize the expected patterns and characteristics of valid command signals. Once the ML models are trained, they are integrated into the AR/VR system to perform real-time monitoring and analysis of incoming command signals. As new commands are received, the ML algorithms assess their characteristics against the patterns learned during training. If the algorithms detect any discrepancies or anomalies in the incoming signals, it raises an alert or triggers a security response, indicating a potential spoofing attempt.

The advantage of using ML-based security measures in our architecture is the ability to adapt and learn continuously. As the AR/VR system operates over time, the ML models can be updated with new data, allowing them to adapt to changes in command patterns and maintain accuracy in identifying spoofing attempts. Thus, the integration of ML-based security measures in the AR/VR system bolsters its resilience and safeguards the integrity of the communication network. By continuously adapting and updating the ML models, the system can stay ahead of evolving attack techniques and maintain a high level of security. As a result, users can enjoy a more trustworthy and immersive AR/VR experience, free from the risks posed by spoofing attacks.

4. Result Analysis

This section presents the comprehensive results derived from training the dataset using various Machine Learning algorithms. It encompasses the detection accuracy, computational time, prediction speed, and cost details obtained throughout the training process. By conducting a comparative analysis of these Machine Learning algorithms, we gain valuable insights into their performance and effectiveness.

4.1. Results Obtained after Training the Data Set through Different SVM Algorithms

Table 2, shows the accuracy percentage achieved using SVM algorithm and Table 3, shows the computational time, speed and cost required using SVM algorithm. The values used for the number of observations are normalized in order to fit it on the scale. Fig.2, shows the graph for Detection accuracy vs Number of observations using SVM algorithm and Fig.3, shows the Computational Time vs Number of observation using SVM algorithms.

Table 2. Accuracy obtained using SVM algorithm

No.of Observation	Linear SVM	Quadratic SVM	Cubic SVM	Gaussian SVM
0-250	100	100	100	99.54
250-500	100	100	100	99.72
500-750	100	100	100	99.96
750-1000	100	100	100	99.96
1000-1250	100	100	100	100
1250-1500	100	100	100	100

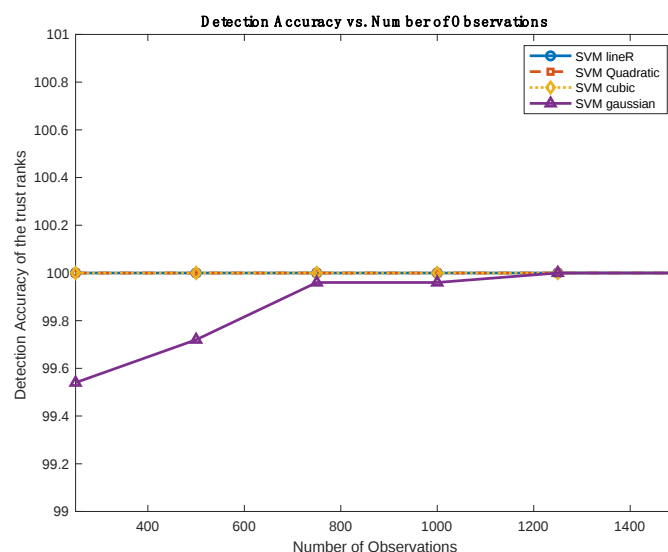


Fig.2. Detection accuracy vs Number of observations using SVM algorithm

After training the given dataset with various SVM algorithms, it was observed that linear, quadratic, and cubic SVM models consistently exhibited higher accuracy compared to the Gaussian SVM algorithm.

Table 3. Obtaining computational time, speed and cost using SVM algorithms

S.No	No.of Observation	Model	Linear SVM	Quadratic SVM	Cubic SVM	Gaussian SVM
		Parameters				
1	0-250	Computation time Prediction Speed cost	13.317 sec 8800obs/sec 0	22.412 sec 6100obs/sec 0	16.95 sec 7100obs/sec 0	29.541 sec 2800obs/sec 11
2	250-500	Computation time Prediction Speed cost	6.859 sec 9100obs/sec 0	10.333sec 8800obs/sec 0	15.763sec 5600obs/sec 0	21.209sec 3000obs/sec 7
3	500-750	Computation time Prediction Speed cost	6.179sec 14000obs/sec 0	9.733sec 9700obs/sec 0	15.016sec 8800obs/sec 0	18.344sec 2900obs/sec 1
4	750-1000	Computation time Prediction Speed Cost	5.5426sec 7000obs/sec 0	9.698sec 11000obs/sec 0	10.174sec 5800obs/sec 0	25.923 3000obs/sec 1
5	1000-1250	Computation time Prediction Speed cost	5.391sec 11000obs/sec 0	6.765sec 10000obs/sec 0	14.422sec 7800obs/sec 0	12.137sec 4500obs/sec 0
6	1250-1500	Computation time Prediction Speed cost	6.067sec 14000obs/sec 0	6.358sec 8200obs/sec 0	11.078sec 8600obs/sec 0	2.581sec 2500obs/sec 0

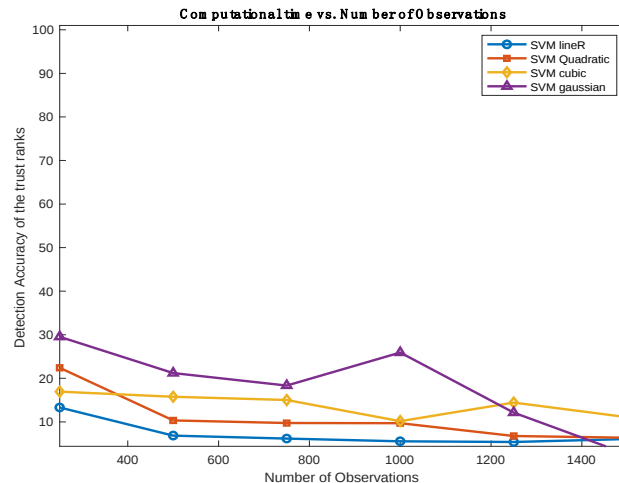


Fig.3. Computational time vs number of observation using SVM algorithms

Additionally, these SVM variants demonstrated superior performance in terms of computational time, prediction speed, and cost, surpassing the Gaussian SVM algorithm. With linear SVM having the lowest computational time. This outcome suggests that for the dataset used, linear SVM algorithm is a more suitable choice, offering better accuracy and efficiency in terms of computational resources and time.

4.2. Results Obtained after Training the Data Set through Different TREE Algorithms

Table 4, shows the accuracy percentage achieved using TREE algorithm and Table 5, shows the computational time, speed and cost required using TREE algorithm. The values used for the number of observations are normalized in order to fit it on the scale.

Table 4. Accuracy Obtained Using TREE Algorithm

No.of Observation	Fine TREE	Medium TREE	Coarse TREE
0-250	99.92	98.8	99.79
250-500	99.96	99.96	99.96
500-750	99.84	99.84	99.84
750-1000	99.84	99.84	99.84
1000-1250	99.88	99.88	99.88
1250-1500	99.84	99.84	99.84

Fig. 4, shows the graph for Detection accuracy vs Number of observations using TREE algorithm and Fig.5, shows the Computational Time vs Number of observation using TREE algorithms.

Upon training the given dataset with various TREE algorithms, it was observed that the Fine TREE algorithm demonstrated slightly higher accuracy compared to the Medium and Coarse TREE algorithm. Additionally, the Medium Tree algorithm exhibited superior performance in terms of computational time, prediction speed, and cost, surpassing the other tree algorithms. These results indicate that, for the specific dataset used, the Fine Tree algorithm offers slightly better accuracy, while the Medium Tree algorithm excels in terms of computational efficiency and cost-effectiveness.

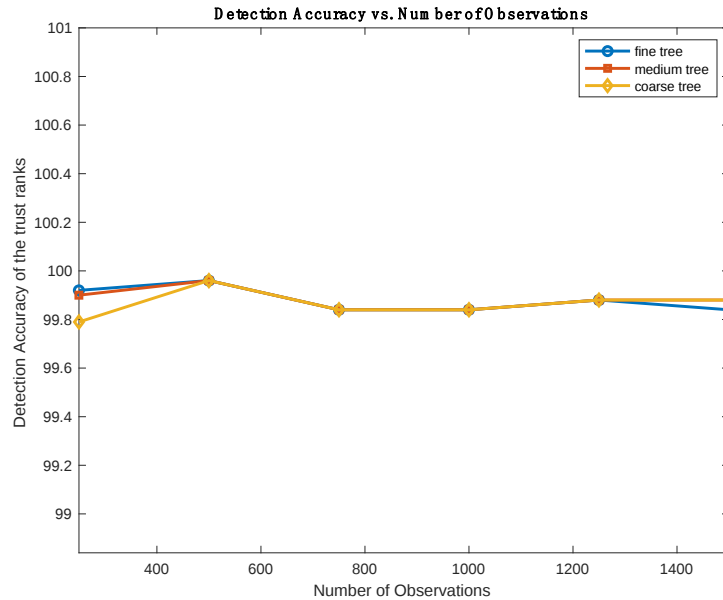


Fig.4. Computational time vs number of observation using TREE algorithms

Table 5. Obtaining computational time, speed and cost using TREE algorithms

S.No	No.of Observation	Model	Fine TREE	Medium TREE	Coarse TREE
		Parameters			
1	0-250	Computation time Prediction Speed cost	14.316sec 9500obs/sec 2	14.371sec 6000obs/sec 2	9.860sec 11000obs/sec 2
2	250-500	Computation time Prediction Speed cost	7.683sec 36000obs/sec 1	4.470sec 21000obs/sec 1	4.7932sec 31000obs/sec 1
3	500-750	Computation time Prediction Speed cost	7.705sec 33000obs/sec 4	4.709sec 18000obs/sec 4	4.920sec 31000obs/sec 4
4	750-1000	Computation time Prediction Speed cost	7.955sec 38000obs/sec 4	4.573sec 30000obs/sec 4	4.528sec 24000obs/sec 4
5	1000-1250	Computation time Prediction Speed cost	7.8983sec 42000obs/sec 3	4.878sec 33000obs/sec 3	5.157sec 22000obs/sec 3
6	1250-1500	Computation time Prediction Speed cost	9.1732sec 40000obs/sec 0	4.819sec 36000obs/sec 4	5.605sec 27000obs/sec 4

4.3. Results Obtained after Training the Data Set through Different KNN Algorithms

Table 6, shows the accuracy percentage achieved using KNN algorithm and Table 7, shows the computational time, speed and cost required using TREE algorithm. The values used for the number of observations are normalized in order to fit it on the scale. Fig.6, shows the graph for Detection accuracy vs Number of observations using KNN algorithm and Fig.7, shows the Computational Time vs Number of observation using KNN algorithms.

After training the dataset using different KNN algorithms, it was observed that the Fine KNN algorithm exhibited slightly higher accuracy when compared to the Medium and Coarse Tree algorithms. Notably, the Fine KNN algorithm outperformed the other tree algorithms in terms of computational time, prediction speed, and cost, showcasing superior overall performance.

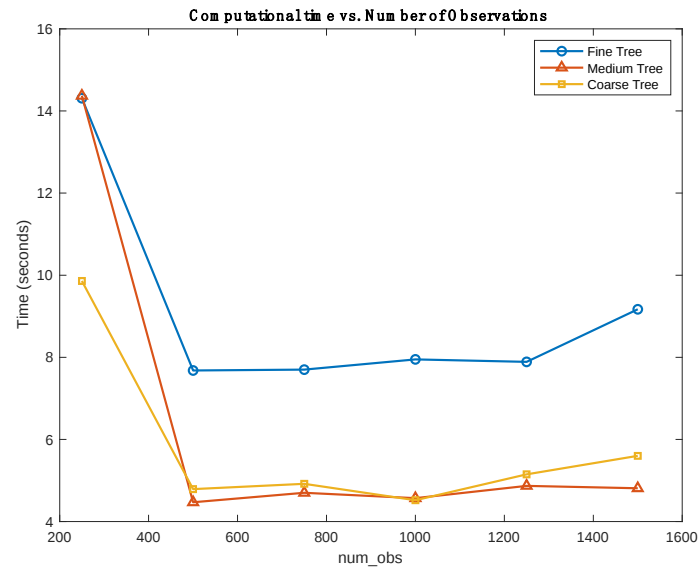


Fig.5. Computational time vs number of observation using TREE algorithms

Table 6. Accuracy Obtained Using KNN Algorithm

No.of Observation	Fine KNN	Medium KNN	Coarse KNN	Cosine KNN	Cubic KNN	Weighted KNN
0-250	99.96	99.79	98.68	97.71	99.63	99.83
250-500	99.92	99.84	97.24	96	99.16	99.92
500-750	100	99.88	98	95.36	99.44	99.92
750-1000	99.96	99.80	98.32	95.92	99.72	100
1000-1250	100	100	96.88	95.64	99.92	100
1250-1500	100	99.96	97	95	99.76	99.96

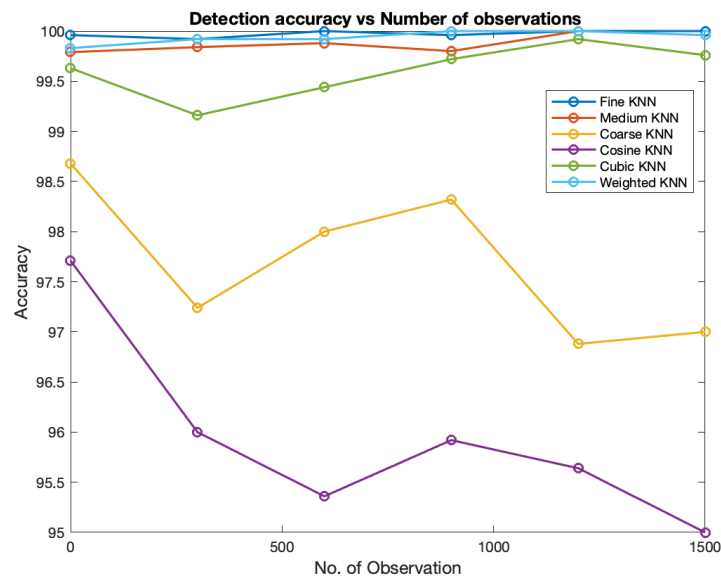


Fig.6. Detection accuracy vs Number of observation using KNN algorithms

Table 7. Obtaining computational time, speed and cost using KNN algorithms

S.No	No.of Observation	Model	Fine KNN	Medium KNN	Coarse KNN	Cosine KNN	Cubic KNN	Weighted KNN
		Parameters						
1	0-250	Computation time	5.877sec	8.9268sec	6.896sec	6.488sec	9.403sec	11.407sec
		Prediction Speed	9700obs/s	7100obs/s	7200obs/s	9300obs/s	2600obs/s	7400obs/s
		cost	1	5	33	55	9	4
2	250-500	Computation time	3.8004sec	7.215sec	5.130sec	3.276sec	5.285sec	4.003sec
		Prediction Speed	17000obs/s	12000obs/s	10000obs/s	13000obs/s	5400obs/s	10000obs/s
		cost	2	2	69	100	2	2
3	500-750	Computation time	3.776sec	5.901sec	4.049sec	3.416sec	4.509sec	4.259sec
		Prediction Speed	16000obs/s	13000obs/s	9900obs/s	13000obs/s	5500obs/s	8900obs/s
		cost	0	3	50	116	14	2
4	750-1000	Computation time	3.596sec	5.502sec	4.264sec	3.517sec	4.983sec	3.6574sec
		Prediction Speed	16000obs/s	11000obs/s	10000obs/s	14000obs/s	6300obs/s	9900obs/s
		Cost	1	5	42	102	7	0
5	1000-1250	Computation time	10.551sec	13.33sec	14.362sec	13.904sec	10.58sec	8.441sec
		Prediction Speed	7100obs/s	5400obs/s	4800obs/s	6400obs/s	6200obs/s	6500obs/s
		cost	0	0	78	109	2	0
6	1250-1500	Computation time	4.046sec	8.879sec	7.7608sec	6.8381sec	6.768sec	6.366sec
		Prediction Speed	13000obs/s	11000obs/s	7400obs/s	700obs/s	7200obs/s	11000obs/s
		cost	0	1	75	123	6	1

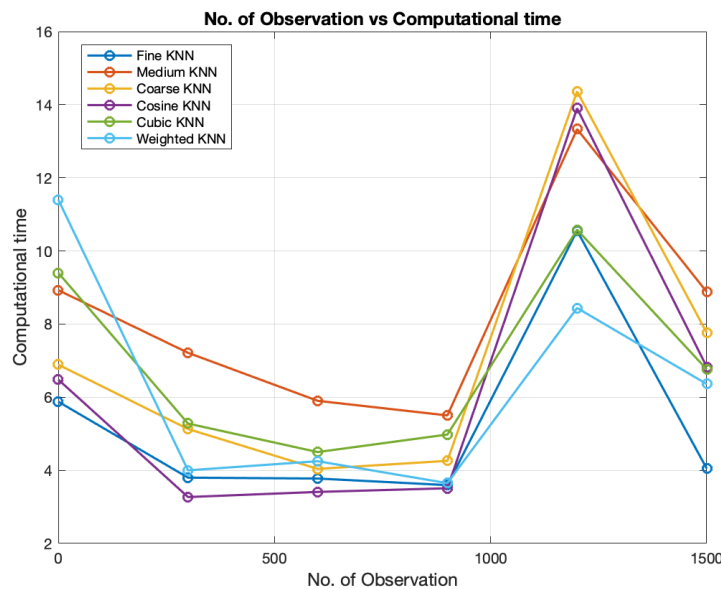


Fig.7. Computational time vs number of observation using KNN algorithms

5. Conclusions

The revolutionary advancements of Augmented Reality (AR) and Virtual Reality (VR) have reshaped our perception and interaction with the world. These innovative technologies are gaining widespread recognition and have the potential to redefine our engagement with the surrounding environment. Despite their transformative capabilities, AR and VR also bring forth unique challenges in terms of security due to their interconnected nature and the vast amount of data they generate. As virtual worlds merge with the physical one, the potential for unauthorized access, data breaches, and malicious attacks becomes a significant concern. Thus, making it important to enable security measures. The paper highlights the critical need for security in the domains of Augmented Reality (AR) and Virtual Reality (VR), emphasizing the potential vulnerabilities and risks associated with these immersive technologies. To address these security challenges posed by AR/VR, we have proposed a ML based approach. By harnessing the capabilities of Machine Learning (ML) algorithms, the system can detect anomalies and distinguish between legitimate and potentially malicious inputs, effectively strengthening its defence against spoofing attempts. The paper also assesses the performance of various machine learning algorithms by simulating them in MATLAB and identifies the algorithm that exhibits the most optimal performance.

Our analysis has evaluated several ML algorithms and their performance in this context, aiming to determine which ones are most effective for ensuring security in AR and VR systems. Based on our comprehensive evaluation, the results indicate that among the various SVM algorithms evaluated, linear SVM emerges as the optimal choice, offering not only commendable accuracy but also low computational time, making it better suitable for security applications. With approximately 0.19% higher accuracy compared to Gaussian SVM, linear SVM proves its efficacy in safeguarding sensitive data while maintaining a low computational time of around 6 seconds. In the realm of KNN algorithms, fine

KNN shows better result, showcasing a remarkable accuracy approximately 4.79% greater than Cosine KNN. Moreover, fine KNN requires lowest computational time among the other KNN algorithms with a low computational time of approximately 4 seconds. This impressive blend of accuracy and efficiency solidifies fine KNN as a compelling choice for security-related tasks. For Tree algorithms, Fine TREE stands out with higher accuracy compared to other TREE algorithms, with 0.08% higher accuracy than Medium TREE. Although Fine TREE demonstrates its proficiency in providing security, Medium TREE excels in computational efficiency, having lower computational time of around 5 seconds. The decision between Fine TREE and Medium TREE is guided by specific security requirements and the trade-off between accuracy and computational time.

As the field of AR and VR continues to evolve, further research and advancements in ML algorithms will be crucial to stay ahead of emerging security challenges and ensure the protection of users' privacy and data.

References

- [1] P. Bhattacharya *et al.*, "Coalition of 6G and Blockchain in AR/VR Space: Challenges and Future Directions," *IEEE Access*, vol. 9, pp. 168455–168484, 2021, doi: 10.1109/ACCESS.2021.3136860.
- [2] W. Wazir, H. A. Khattak, A. Almogren, M. A. Khan, and I. Ud Din, "Doodle-Based Authentication Technique Using Augmented Reality," *IEEE Access*, vol. 8, pp. 4022–4034, 2020, doi: 10.1109/ACCESS.2019.2963543.
- [3] R. Chengoden *et al.*, "Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions," *IEEE Access*, vol. 11, pp. 12764–12794, 2023, doi: 10.1109/ACCESS.2023.3241628.
- [4] T. Everson, M. Joordens, H. Forbes, and B. Horan, "Virtual Reality and Haptic Cardiopulmonary Resuscitation Training Approaches: A Review," *IEEE Syst J*, vol. 16, no. 1, pp. 1391–1399, Mar. 2022, doi: 10.1109/JSYST.2020.3048140.
- [5] S. K. Sharma, I. Woungang, A. Anpalagan, and S. Chatzinotas, "Toward Tactile Internet in beyond 5G Era: Recent Advances, Current Issues, and Future Directions," *IEEE Access*, vol. 8, pp. 56948–56991, 2020, doi: 10.1109/ACCESS.2020.2980369.
- [6] Y. Wang *et al.*, "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Communications Surveys and Tutorials*, 2022, doi: 10.1109/COMST.2022.3202047.
- [7] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A Survey on Mobile Augmented Reality with 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 2, Institute of Electrical and Electronics Engineers Inc., pp. 1160–1192, Apr. 01, 2021, doi: 10.1109/COMST.2021.3061981.
- [8] Q. Cheng, S. Zhang, S. Bo, D. Chen, and H. Zhang, "Augmented Reality Dynamic Image Recognition Technology Based on Deep Learning Algorithm," *IEEE Access*, vol. 8, pp. 137370–137384, 2020, doi: 10.1109/ACCESS.2020.3012130.
- [9] P. H. Lin and S. Y. Chen, "Design and Evaluation of a Deep Learning Recommendation Based Augmented Reality System for Teaching Programming and Computational Thinking," *IEEE Access*, vol. 8, pp. 45689–45699, 2020, doi: 10.1109/ACCESS.2020.2977679.
- [10] A. Apicella *et al.*, "Enhancement of SSVEPs Classification in BCI-Based Wearable Instrumentation Through Machine Learning Techniques," *IEEE Sens J*, vol. 22, no. 9, pp. 9087–9094, May 2022, doi: 10.1109/JSEN.2022.3161743.
- [11] S. J. Yoo and S. H. Choi, "Indoor AR Navigation and Emergency Evacuation System Based on Machine Learning and IoT Technologies," *IEEE Internet Things J*, vol. 9, no. 21, pp. 20853–20868, Nov. 2022, doi: 10.1109/JIOT.2022.3175677.
- [12] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu, and V. Chang, "Trustworthy and Intelligent COVID-19 Diagnostic IoMT through XR and Deep-Learning-Based Clinic Data Access," *IEEE Internet Things J*, vol. 8, no. 21, pp. 15965–15976, Nov. 2021, doi: 10.1109/JIOT.2021.3055804.
- [13] S. V. Mahadevkar *et al.*, "A Review on Machine Learning Styles in Computer Vision - Techniques and Future Directions," *IEEE Access*, vol. 10, Institute of Electrical and Electronics Engineers Inc., pp. 107293–107329, 2022, doi: 10.1109/ACCESS.2022.3209825.
- [14] M. Gupta, R. K. Jha, and S. Jain, "Tactile based Intelligence Touch Technology in IoT configured WCN in B5G/6G-A Survey," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3148473.
- [15] S. Jeong, J. G. D. Hester, W. Su, and M. M. Tentzeris, "Read/Interrogation Enhancement of Chipless RFIDs Using Machine Learning Techniques," *IEEE Antennas Wirel Propag Lett*, vol. 18, no. 11, pp. 2272–2276, Nov. 2019, doi: 10.1109/LAWP.2019.2937055.

Authors' Profiles



Momina Mushtaq is currently a Student in the School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India. Her research interest in Wireless Networks, Machine Learning.



Rakesh K. Jha (S'10, M'13, SM 2015) is currently an Associate Professor in the Department of Electronics and Communication Engineering, Indian Institute of Information Technology Design and Manufacturing Jabalpur, India. He has also worked as an Associate Professor at SMVD University, J&K, India. He is among the top 2% researchers of the world. He has published more than 61 SCI Journals Papers including many IEEE Transactions, IEEE Journal, and more than 25 International Conference papers. His area of interest is Wireless communication, Optical Fiber Communication, Computer Networks, and Security issues. Dr. Jha's one concept related to the router of Wireless Communication was accepted by ITU in 2010. He has received the young scientist author award by ITU in Dec 2010. He has received APAN fellowship in 2011, 2012, 2017 and 2018 and student travel grant from COMSNET 2012. He is a senior member of IEEE, GISFI and SIAM, International Association of Engineers (IAENG) and ACCS (Advance Computing and Communication Society). He is also a member of, ACM and CSI, with many patents and more than 6001 citations to his credit.



Dr. Manish Sabraj is currently an Assistant Professor in the School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India. He has received his B.Tech degree in Electronics and Communication from Govt. College of Engineering and Technology Jammu and Kashmir, India, in 2001 and M.Tech degree in Electronics and Communication from IIT Guwahati, Guwahati, India, in 2003. He has completed his Ph.D. degree from Shri Mata Vaishno Devi University, Jammu and Kashmir, India in 2013. His research interest includes Digital Signal Processing, Wireless Sensor Networks, and Spectrum estimation and analysis.



Shubha Jain (shubhajain1203@gmail.com) earned her bachelor's degree in electronics and telecommunications from SGSITS, Indore, India, and her master's degree in telecommunications from the University of Maryland, College Park, Maryland, USA. Currently, she is working with Amazon, USA.

How to cite this paper: Momina Mushtaq, Rakesh Kumar Jha, Manish C. Sabraj, Shubha Jain, "Attack Modeling and Security Analysis Using Machine Learning Algorithms Enabled with Augmented Reality and Virtual Reality", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.4, pp.118-129, 2024. DOI:10.5815/ijcnis.2024.04.08