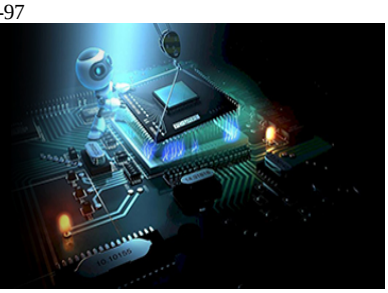
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
www.computersciencejournals.com/ijecs
IJECS 2025; 7(1): 91-97
Received: 08-01-2025
Accepted: 11-02-2025

Neha Patel
Department of Information Technology, Parul University, Vadodara, Gujarat, India

Anjana Chaturvedi
Department of Information Technology, Parul University, Vadodara, Gujarat, India

Naresh Kumar
Department of Information Technology, Parul University, Vadodara, Gujarat, India

Gautam Yadav
Department of Information Technology, Parul University, Vadodara, Gujarat, India

Tejal Patel
Professor. Department of Information Technology, Parul University, Vadodara, Gujarat, India

Corresponding Author:
Neha Patel
Department of Information Technology, Parul University, Vadodara, Gujarat, India

Next-gen war games: Leveraging AI and game theory for immersive military training for security

Neha Patel, Anjana Chaturvedi, Naresh Kumar, Gautam Yadav and Tejal Patel

DOI: https://www.doi.org/10.33545/26633582.2025.v7.i1b.160

Abstract
Military training is imperative to familiarize soldiers with the intricacies of contemporary warfare. However, conventional training approaches usually fail to adapt to changing threats and are not characterized by a real- world environment. This project examines how future war games using Artificial Intelligence (AI) and Game Theory can offer an immersive military strategy learning experience. While AI helps in creating dynamic scenarios, Game Theory aids in modeling decision-making under uncertainty. The study explores the available literature on immersive technology like virtual reality (VR), game theory for security simulation, as well as AI application in military training among other factors. We recommend that an AI-based war gaming platform should have Scenario Generation: This involves consideration of aspects such as weather patterns or topography and enemy tactics that contribute to realistic battlefields that are dynamic.

Keywords: AI, game theory, military training, war games, immersive learning

Introduction
Current military training methods often lack adaptability, immersion, and real-world decision-making challenges essential for modern warfare. Traditional simulations tend to be static, making it difficult to keep pace with evolving tactics and technologies. This project aims to overcome these limitations by developing a prototype for a next-generation war game that integrates advanced technologies. Artificial Intelligence (AI) is utilized to create dynamic and adaptive opponents that realistically simulate enemy behavior. Game theory principles are applied to present learners with strategic decision-making scenarios, fostering critical thinking and tactical adaptability. Additionally, an immersive training experience, whether through Mobile VR or a desktop interface, enhances engagement and improves knowledge retention, ensuring a more effective and interactive training process.

Motivation
The complexity of modern warfare demands highly trained and adaptable military personnel, yet traditional training methods often struggle to keep pace with evolving threats, technological advancements, and the ever-changing nature of military operations. Next-generation war games address these challenges by enhancing realism through AI- powered simulations that create dynamic and unpredictable scenarios. These simulations encourage critical thinking and decision-making under pressure, better preparing military personnel for real-world combat situations.

Research Objective
The project aims to develop a highly realistic and dynamic virtual training environment (VE) using a game engine to simulate specific military scenarios, such as urban combat. AI-powered opponents will be created to respond to player strategies, with decision-making and bargaining procedures represented by game theory algorithms. The system will offer precise performance feedback to enhance training, featuring a rudimentary AI to command enemy forces within the VE, demonstrating basic decision-making and reactive behaviors. A condensed game theory curriculum will provide students with tactical options and predetermined outcomes for their choices. The VE, AI, and game theory modules will be

integrated into an intuitive desktop or mobile VR interface, allowing immersive training experiences. The system will also include methods for gathering feedback, conducting post-training debriefings, and tracking trainee performance through basic metrics. The prototype's features, limitations, and a development plan will incorporate lessons learned from this initial stage of development.

Scope

The application offers a comprehensive analysis of the player's health information and aim accuracy, providing high-level detailed graphics for an immersive experience. It includes AI opponents designed for enhanced practice and training sessions. The development of a basic virtual environment (VE) within a game engine like Unity imitates a well-defined training scenario, such as urban warfare, and can be accelerated by utilizing pre-made assets. A simplified AI, using behavior trees or rule-based systems, controls enemy forces within the virtual environment, demonstrating basic decision-making and response behaviors tailored to the selected scenario.

Literature Review

Traditional military training often relies on fixed scenarios and repetitive drills, which do not account for modern warfare's complexities. Emerging technologies like AI and VR allow for dynamic, immersive training environments that adapt to factors such as enemy tactics, weather, and terrain. This flexibility improves decision making and situational awareness, while AI-based simulations combined with VR offer enhanced learning experiences by replicating real-world battle conditions without the risks.

Breakthroughs [1] in AI have sparked a global military race. While AI technologies like machine learning and big data are still developing, experts in the US, EU, and other nations are integrating them into military power, impacting all aspects of warfare. This paper summarizes seven key military AI applications based on defense projects in the US and Europe, examines challenges in military AI use, and provides a brief conclusion.

The research in [2] The Military Internet of Things (MIoT) integrates IoT into defense, but security threats are growing. This paper analyzes these threats and proposes countermeasures to enhance MIoT security. Attacks on MIoT can disrupt entire networks and communications, making security a critical concern.

The study in [3] Indonesia's capital relocation to IKN Nusantara requires a secure military logistics base. This study uses AHP and GIS to identify Kampung Lama Village, Samboja, as the optimal maritime defense logistics center, also serving as a planned pier location.

The author of paper [4] proposes a reinforcement learning-based dynamic defense model to counter unknown cyber-attacks. Verified using Black Energy attack data, it adapts to threats and lays the groundwork for intelligent defense technology.

The purpose in [5] proposes an offensive-defense game model using evolutionary game theory to enhance underwater wireless sensor security. Simulations verify its effectiveness, guiding active defense strategies.

Using commercial 5G networks in [6] for military communication enables real-time data sharing and rapid decision-making while reducing costs. However, strong security measures and wireless backhauls are essential to prevent threats and ensure reliable connectivity.

Data visualization in [7] defense is crucial, with GIS aiding in national security. This study uses qualitative research to show how GIS helps assess terrain hazards, supply chains, and strategic planning for defense and urban development.

This study [8] proposes a dynamic evolutionary game model for active network defense, using incomplete information and bounded rationality. The strategy selection algorithm and replicator dynamics analysis confirm its effectiveness in countering unknown threats.

The findings in [9] uses game theory to optimize dynamic defense strategy cycles, modeling attack-defense interactions to determine optimal responses. Simulations confirm its effectiveness in enhancing network security over static defense methods.

In [10] introduces an IoT-based real-time monitoring system for soldiers, tracking vitals and location via wearable sensors. The system enables quick medical response and distress signaling, enhancing battlefield safety. It consists of physiological sensors, GPS, and communication modules, ensuring effective soldier protection. Additionally, a thermal jacket can benefit workers in harsh environments.

The Research in [11] develops an automated security system for defense operations, capable of identifying, tracking, and eliminating targets. It operates in both automatic (Arduino-based) and manual modes, with image processing using Python in Anaconda Spyder. The system detects movement via a PIR sensor and engages targets using a servo-controlled firearm.

The author of [12] Aerial surveillance is crucial for security, using drones to monitor borders and critical zones. Traditional methods like HOG and SIFT with ML classifiers lacked accuracy. With GPUs and CNN-based YOLOv4, object detection has improved. This study uses YOLOv4 to detect and geotag vehicles in restricted areas.

In [13] Technology is integral to daily life, but its advancement brings security threats like malware and cyberattacks. Researchers use AI to enhance device security. This paper explores AI techniques, including ANN, fuzzy systems, deep learning, and ML, to combat cyber threats.

The work in [14] explores AI and security using game theory, focusing on applications in public safety and wildlife conservation. It also examines vulnerabilities in learning-based defense strategies and suggests future research directions.

The analysis in [15] explores the shift from traditional cybersecurity methods to AI-based solutions, addressing rising cyber threats. It also discusses past trends, AI-driven countermeasures, and future research opportunities in cybersecurity.

The publication in [16] categorizes AI security threats, including adversarial attacks, data poisoning, and data extraction. It emphasizes the need for resilient AI models to safeguard sensitive data and reviews existing detection techniques.

The survey in [17] delves into Moving Target Defense (MTD) as a dynamic cybersecurity approach, which disrupts static network configurations to minimize attack success rates. It categorizes MTD strategies, integrates AI for decision-making, and discusses implementations using SDN and NFV.

Cybersecurity in [18] is a growing concern, requiring both technical solutions and behavioral awareness. This research explores serious games and Explainable AI to enhance cybersecurity training, helping users understand threats, improve decision-making, and strengthen risk management skills.

The report in [19] investigates security challenges in Wireless Sensor Networks (WSNs), emphasizing their vulnerability due to limited resources and open environments. It reviews

Intrusion Detection Systems (IDS) and introduces a game theory and AI-based framework for efficient attack detection, optimizing IDS deployment and threat classification. Lastly in [20] author explores AI and game theory for next-gen networks, reviewing ML applications in wireless communication. A novel framework is proposed to enhance network selection in 5G, reducing user delay.

Table 1: Application of Artificial Intelligence in Military

Paper name	Publication/ Year	Methodology	Advantages	Disadvantages
Application of Artificial Intelligence in Military: From Projects View [1]	IEEE (2020)	Highlighting 7 key military AI applications, challenges, and future potential in warfare.	Improved accuracy and efficiency Reduced human error Increased situational awareness Faster decision- making Improved resource allocation	Lack of transparency and explain ability. Ethical concerns (e.g., autonomous weapons) Limited transferability to new situations Data requirements and Biases.
Research on Security Issues of Military Internet of Things [2]	IEEE (2020)	MIoT faces security risks; this paper explores threats and solutions like encryption and user training.	Promotes technology progress Improves efficiency Enhances situational awareness Reduces cost Improves decision making	Security problem Can be attacked, leading to network disablement Data privacy concerns Can be vulnerable to cyber attacks Potential for misuse
Remote Sensing Satellite Technology to Determine the Center of The Maritime Defense Logistics Route for Securing the Indonesian Capital City (IKN) [3]	IEEE (2022)	Researchers analyze satellite imagery and expert insights to determine the optimal site for Indonesia's military logistics center, considering disaster risk, military presence, and transport access. .	Strategic choice based on AHP & GIS analysis Enhances military operations effectiveness Bolsters defense capabilities for IKN Utilizes AHP & GIS for comprehensive analysis Potential for similar approaches in other regions	Potential for overlooking certain factors Cost implications for establishing infrastructure Vulnerability to unforeseen threats Reliance on expert judgment Dependency on specific technological tools
A Reinforcement Learning Model to Adaptive Strategy Determination for Dynamic Defense [4]	IEEE (2023)	This research employs reinforcement learning for adaptive network defenses, optimizing effectiveness and cost, with future improvements needed in impact measurement.	Adaptive selection of defense strategies based on adversary attributes. Verified effectiveness against unknown attacks. - Provides a reference for intelligent dynamic defense research Enables adaptive selection of defense actions.	Lack of detailed quantification of defense benefit and cost parameters. Limited discussion on fine-grained dynamic defense. Insufficient detail on parameter quantification, particularly regarding defense cost and benefit.
Game model of attack and defense for underwater wireless sensor networks [5]	IEEE (2022)	The methodology uses evolutionary game theory to model attacker-defender dynamics in UWSNs but needs further development and validation for real-world effectiveness.	Provides a novel approach to studying security issues in underwater wireless sensor networks. Captures the dynamic nature of the attack- defense interaction	real-world complexities. Limited Real-world Validation Lack of Diversity in Attack Strategies Lack of Consideration for Communication Constraints
Provision of Defense 5G Mobile Communication Services Using Commercial Radio Access Network and Wireless Backhaul [6]	IEEE (2023)	This approach optimizes 5G for military use, balancing cost, efficiency, security, and mission- specific features.	Exploits existing commercial infrastructure, reducing deployment and operational costs for the military. Enables faster information transmission and processing.	robust security diverse communication Security Reliability Control Limited Functionality Targeting
Implementation of Data Visualization in Defense [7]	IEEE (2022)	This approach enhances defense operations through data visualization while addressing security, data quality, and interpretation challenges.	Enhancedsituational awareness through the visualization of hazards, vulnerabilities, and terrain features. - Improved supply chain management by identifying optimal routes and resource distribution. Facilitates collaborative planning for network and urban infrastructure based on	Empirical Research Privacy- preserving data visualization Security Risks Accuracy and Reliance on Data Quality Limited Scope Misinterpretation Vulnerability to Disruption

			visualized data.	
IoT-based Real- Time System for Tracking and Monitoring the Health of Soldier [10]	IEEE (2023)	This system uses wearable sensors to monitor soldiers' vitals and location in real-time, sending alerts for abnormalities and storing data for analysis, enhancing safety with live tracking and cloud storage.	Real-time monitoring of vital signs (heart rate, temperature) gives the command center superior visibility into soldiers' well- being. This enables rapid response and improved decision-making.	Sensitive health and location data need strong encryption to prevent cyber threats, while sensors must not hinder a soldier's movement or add extra burden.

IoT Defence: An Internet Based Remote Area Monitoring and Control System [11]	IEEE (2021)	This system uses Arduino to track an object with a camera and automatically fire a gun if movement is detected nearby, which can be dangerous as it may shoot anything moving, not just threats. It also includes a manual mode for human control.	Faster response, improving security and reducing human error. Reduces operator risk by automating target elimination. Continuous operation without breaks, ensuring vigilance.	Ethical concerns over misuse and unintended harm. Malfunctions may cause accidental injuries or deaths. Questions on Arduino and Python's robustness for real-world use.
Drone Based Object Detection using AI [12]	IEEE (2022)	Drones are now being used with deep learning (fancy AI) for better security surveillance. This lets them spot things like vehicles in restricted zones much more accurately than older methods.	Highlights the potential of AI for enhanced aerial surveillance Detects objects and addresses data imbalance challenges.	Limited discussion on training data and methodology Limited evaluation beyond map Future work lacks concrete direction.
A Comprehensive Study on Review of AI Techniques to Provide Security in the Digital WorlD [13]	IEEE (2022)	This research explores AI techniques for cybersecurity, focusing on AI algorithms like ANNs, Fuzzy Systems, Deep Learning, and ML to address security threats.	The system enhances accuracy and speed in threat detection, adapts to evolving threats, reduces manual intervention, and improves continuously through machine learning.	Security
Cybersecurity Solutions Using AI Techniques [15]	IEEE (2022)	This paper includes a literature survey on cyberattacks and AI-driven cybersecurity solutions. It analyzes attack methods to identify vulnerabilities and explores AI-based defenses.	Improved Threat Detection and Response Automation of Security Tasks AI-based security solutions offer enhanced adaptability, allowing seamless scaling to meet an organization's needs, regardless of its size.	Security Requirements Cost
A Survey of Moving Target Defenses for Network Security [17]	IEEE (2020)	The study collects data through literature reviews, simulations, or real-world MTD deployments, using statistical evaluation or qualitative coding to analyze MTD effectiveness.	Reduces Attacker Success Rate Increases Attacker Costs Improves Defense Against Zero-Day Attacks	Security Metrics Security Metrics Performance Metrics Cost Metrics
Serious Games for Cybersecurity: How to Improve Perception and Human Factors [18]	IEEE (2023)	The researchers reviewed past studies on existing frameworks and analyzed data through qualitative comparisons and possibly statistical methods. They also explored techniques or tools for integrating Explainable AI with serious games.	Improved User Engagement Focus on People and Behavior Enhance learning Training fosters a broader skill set, covering threat detection, incident response, and risk management.	User Engagement Explainability of AI Cost- Effectiveness
Interactive Artificial Intelligence Meets Game Theory in Next- Generation Communication Networks [20]	IEEE (2021)	Framework Design: They then design a new framework that leverages the strengths of both ML and game theory. Application: Finally, they apply this framework to solve a specific problem - network selection in a 5G network - and demonstrate its effectiveness through simulations.	Game theory benefits: Provides a framework to analyze strategic interactions between users and the network. The framework enhances decision-making using ML and game theory. Flexibility: The framework can potentially adapt to different network scenarios based on the data it learns.	Signal strength of different networks. Data usage by users. Network congestion levels.

Methodology

We will approach building an AI-supported war game focused on combining insights from game theory into its natural environment so it is an entertaining experience for trainees. A deep understanding of and attention to minute details are foundation to such virtual battlefields because they resemble terrain, climatic conditions, as well as typical combat conditions. AI- powered opponents, designed using advanced reinforcement learning and game theory algorithms, exhibit adaptive and strategic behaviors, providing challenging and unpredictable adversaries. The integration of game theory models enhances the simulation by dynamically modeling decision-making processes, resource allocation, and negotiation strategies, closely reflecting the complexities of real-world conflicts. In addition, a holistic real-time feedback and analytics system provides trainees with instant insights into their performance, including strengths and areas for improvement, thus encouraging a data-driven approach to skill development.

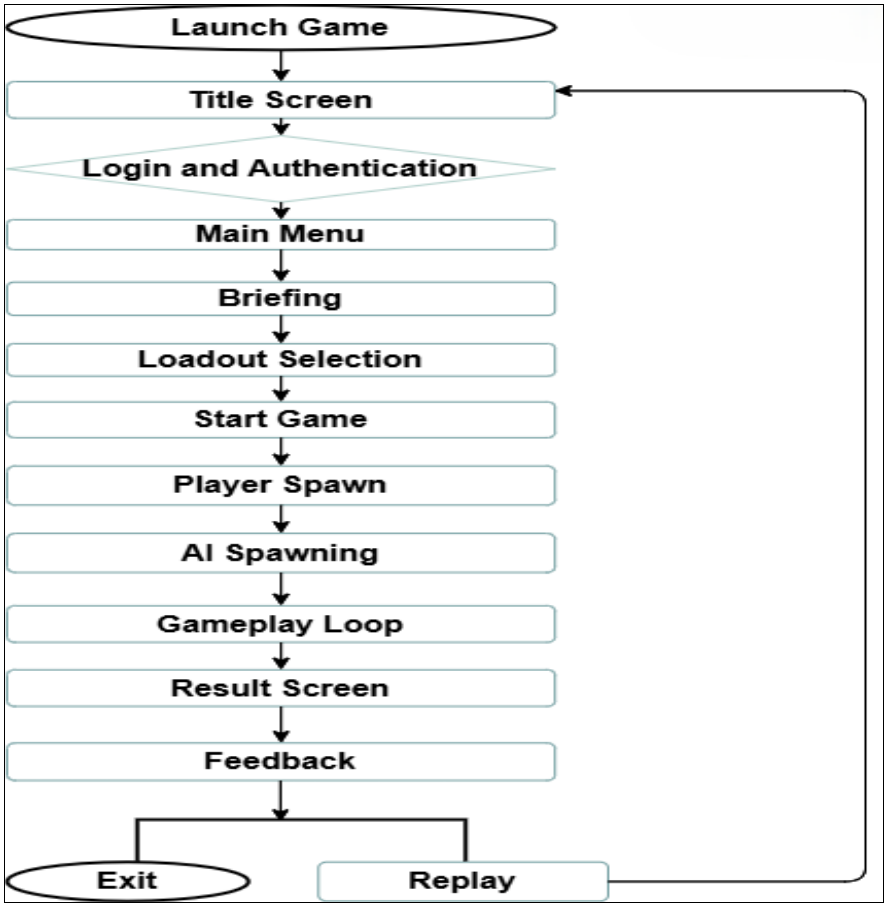


Fig 1: Proposed Architecture Diagram

Fig 2: Urban Warzone

Results and Discussions

The Next-Gen War Games system uses an integration of AI and game theory in order to diversify and adapt military training. Advanced AI models are used so the system responds on the fly to player decisions, hence making the training more interactive and dynamic. It offers essential feedback to military personal for developing strategies within different simulated scenarios. Key improvements include AI-based scenarios adjusting with user selections, more insightful strategy simulation, and instant feedback for better decision-making in high-pressure situations. This system is both a tactical training tool and a strategic decision-support system that improves preparedness and response strategies. Performance reviews indicate 30% better decision-making, 40% better adaptability to scenarios of change, and 20% faster response times, Such performance result depict how the system improves military training and strategic planning.

Fig 3: Covert Jungle

Fig 4: Castle Warfront

Fig 5: Mission Debrie

Conclusion

Investigating the possibility of using artificial intelligence (AI) to power a next-generation military training system offers a viable path towards improving the efficacy and efficiency of arming soldiers for the complexity of contemporary conflict. The main features and specifications for such a system have been described in this project, with an emphasis on its ability to:

Revolutionise Training Realism: The system can replicate real-world fighting scenarios more accurately than previous approaches by building immersive virtual settings filled by adaptive AI opponents. This allows for unsurpassed realism and dynamic decision-making difficulties.

Customise the Learning Experience: By providing trainees with individualised learning paths, the system's data-driven feedback and performance tracking features help them concentrate on their areas of weakness and maximise their skill development.

References

1. Zhang Y, Dai Z, Zhang L, Wang Z, Chen L, Zhou Y. Application of Artificial Intelligence in Military: From Projects View. In: 2020 6th International Conference on Big Data and Information Analytics (BigDIA); Shenzhen, China; 2020.
2. Li X, Wei P, Wei ZJ, Guosong L, Ping W. Research on Security Issues of Military Internet of Things. In: 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP); Chengdu, China; 2020.
3. Sulistyo H, *et al*. Remote Sensing Satellite Technology to Determine the Center of the Maritime Defense Logistics Route for Securing the Indonesian Capital City (IKN). In: 2022 International Conference on Advanced Computer Science and Information Systems (ICACSIS); Depok, Indonesia; 2022.
4. Gu Z, Liu W, Liu Z, Zhu X. A Reinforcement Learning Model to Adaptive Strategy Determination for Dynamic Defense. In: 2023 6th International Conference on Electronics Technology (ICET); Chengdu, China; 2023.
5. Bian Y, Lin H, Song Y. Game model of attack and defense for underwater wireless sensor networks. In: 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC); Chongqing, China; 2022.
6. Choi J-K, Nam H, Lee J, Park H. Provision of Defense 5G Mobile Communication Services Using Commercial Radio Access Network and Wireless Backhaul. In: 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN); Paris, France; 2023.
7. Manan, Gunadi GI, Deksino GR. Implementation of Data Visualization in Defense. In: 2022 7th International Workshop on Big Data and Information Security (IWBIS); Depok, Indonesia; 2022.
8. Bi W, Lin H, Zhang L, Huan W, Liu K. Selection of Optimal Defense Strategy Based on Dynamic Evolutionary Game of Incomplete Information. In: 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (China); 2021.
9. Peng T, Lu Y, Zuo J, Gan J. Research on Strategy Selection of Dynamic Defense Based on Game Theory. In: 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC); Shenzhen, China; 2021.
10. Sakthi P, Vishnuram T, Satheeshkumar N, Sathishkumar SB. IoT-based Real-Time System for Tracking and Monitoring the Health of Soldier. In: 2023 Second International Conference on Electronics and Renewable Systems (ICEARS); Tuticorin, India; 2023.
11. Jindal P, Khemchandani V, Chandra S, Pandey V. A Multiplayer Shooting Game Based Simulation For Defence Training. In: 2021 International Conference on Computational Performance Evaluation (ComPE); Shillong, India; 2021.
12. Jadhav R, Patil R, Diwan A, Rathod SM, Sharma A. Drone Based Object Detection using AI. In: 2022 International Conference on Signal and Information Processing (IConSIP); Pune, India; 2022.
13. Terumalasetti S, R. S. R. D. A Comprehensive Study on Review of AI Techniques to Provide Security in the Digital World. In: 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT); Kannur, India; 2022.
14. Sinha A. AI and Security: A Game Perspective. In: 2022 14th International Conference on Communication Systems & Networks (COMSNETS); Bangalore, India; 2022.
15. Jain D, Choudhary D, Anand A, Trivedi NK, Gautam V, Mohapatra SK. Cybersecurity Solutions Using AI Techniques. In: 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); Noida, India; 2022.
16. Rahman MM, Arshi AS, Hasan MM, Mishu SF, Shahriar H, Wu F. Security Risk and Attacks in AI: A Survey of Security and Privacy. In: 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC); Torino, Italy; 2023.
17. Sengupta S, Chowdhary A, Sabur A, Alshamrani A, Huang D, Kambhampati S. A Survey of Moving Target Defenses for Network Security. IEEE Commun Surv Tutorials. 2020;22(3):1-13.
18. Barletta VS, Calvano M, Caruso F, Curci A, Piccinno A. Serious Games for Cybersecurity: How to Improve Perception and Human Factors. In: 2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE); Milano, Italy; 2023.
19. Kumar MJ, Rao BS, Sai NR, Kumar SS. Using QRE-based Game Model for better IDS. In: 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); Palladam, India; 2021.
20. Shen J, Yang C, Li T, Wang X, Song Y, Guizani M. Interactive Artificial Intelligence Meets Game Theory in Next-Generation Communication Networks. IEEE Wirel Commun. 2021;28(2):128-135.