



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** X **Month of publication:** October 2026

DOI: <https://doi.org/10.22214/ijraset.2026.84965>

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

AI Digital Twin for Cloud Cyber Security

Umesh Samarth¹, Himanshu Dipak Khade², Aniruddha Baban Shendre³, Mayur Vijay Sawarbandhe⁴, Aniket Mahadev Bendarkar⁵

Department of IT, J D College of Engineering and Management, Nagpur, India

Abstract: *The key advantage of cloud computing is scalability and flexibility of infrastructure, however, the growing complexity of cloud environments has led to numerous security issues. Current security systems are largely reactive, which means that any detected attacks have already taken place. This paper suggests the use of the AI-based Digital Twin technology for cybersecurity in cloud environments, providing the possibility of creating a virtual copy of the cloud environment that can be used for continuous monitoring, attack simulation, and security testing. The proposed framework uses AI/ML algorithms for anomaly detection, attacks' classification, and risk assessment in conjunction with Multi-Agent Reinforcement Learning (MARL) in order to achieve collaboration and adaptability of security response. The system includes cloud resource monitoring, attacks simulation, security logging, alert generation, access control by roles, and security analysis dashboard. The development of the system takes place using MERN stack architecture with Digital Twin synchronization of virtual cloud resources and their metrics. With the combination of Digital Twin technology, AI-based threat detection and multi-agent decision making, the proposed framework can provide enhanced proactivity, adaptiveness, and real-time performance of cybersecurity in cloud environments.*

Keywords: AI, Digital Twin, Cloud Computing, Cloud Cyber Security, Machine Learning, Multi-agent Reinforcement Learning.

I. INTRODUCTION

Cloud Computing has become a significant technology for delivering scalable and flexible computing resources to organizations and users at low costs. The cloud computing environments are able to provide different kinds of services, applications, virtual servers, storages and networks but with increase of the cloud complexity and interconnectedness new security challenges are created. Traditional approaches to the security of the cloud mainly involve signature-based intrusion detection and reactive monitoring that is able to detect the malicious activities only after the attack occurred. The existing techniques are not able to predict the emergence of new types of threats, to detect new attack patterns and to automatically adjust security strategy depending on the attack. Here, Digital Twin technology could help with development of better cloud computing security because Digital Twin allows to create the virtual model of the physical or operational cloud environment. Digital Twin can continuously maintain the state of cloud resources, network topology and operational metrics and thus allows to observe and test the security activities in a virtual environment without any impact on production environment. Nevertheless, the connection and exchange of information between the actual cloud environment and its virtual representation might become an extra source of cybersecurity threats, which is why there is a need for security-aware Digital Twins architecture. Artificial Intelligence and Machine Learning techniques can be used to enhance this process by means of analyzing the network traffic, system logs, resource consumption, etc., in order to detect unusual activity and security threats as well as to assess security risks. In addition, Multi-Agent Reinforcement Learning (MARL) can be used to provide collaborative intelligent agents, which would observe the environment and choose actions according to the existing security situation. The aim of the suggested research is to devise an intelligent solution that will allow building a live Digital Twin of cloud infrastructure as well as simulating attacks, implementing detection and risk scoring via AI/ML, and collaborative multi-agent defense. Security threats including Distributed Denial-of-Service (DDoS), SQL injection, Cross-Site Scripting (XSS), brute-force attack, port scan, phishing, and malware will be covered in the scope of work because they may be safely simulated in the virtual world. In addition, the solution will include the monitoring and dashboard layer for visualization of security logs, alerts, and analytics. The general idea is to develop a framework for cybersecurity of clouds that will monitor the virtual world, detect threats, and analyze the security of cloud infrastructure.

II. RELATED WORK

A. Machine Learning-Based Intrusion Detection in Cloud Security

Buczak and Guven [1] conducted an extensive survey of the techniques of data mining and machine learning applied for cybersecurity intrusion detection. Specifically, the authors reviewed the use of ML and DL algorithms for detecting cyber intrusions and malicious activities within the network environment.

It was proven in the study that machine learning algorithms can analyze security information and detect patterns associated with cyber attacks. Such algorithms play a crucial role in automating the process of intrusion detection by decreasing the use of manually established security rules. Nevertheless, traditional ML techniques applied for cybersecurity purposes can be less effective in terms of detecting unknown or emerging attacks based on previous attack patterns. This requirement reveals the necessity to implement adaptive cybersecurity measures that could respond to the constantly evolving threats. In the proposed approach, machine learning algorithms are used to perform attack detection, classification, anomaly detection and scoring within the AI Digital Twin model, while the latter serves as an environment for monitoring and simulating attacks.

B. Digital Twin Technology for Real-Time Monitoring

In their study, Tao, Zhang, Liu, and Nee [2] examined Digital Twin-driven smart manufacturing and explained the use of Digital Twin technology in enabling real-time monitoring and simulation of the physical system. It describes how a virtual model of a system can be integrated with the physical system to observe the state of the system. As such, the digital twin technology can be employed in the monitoring of dynamic environments that require real-time information about the system. However, the study only concentrates on smart manufacturing and does not explain how the digital twins can be used for cloud security. There is still a need for adaptation of the digital twins technology for use in the cloud environment where digital twins can model virtual servers, network topology, and resource states as well as perform cybersecurity monitoring and attack simulation. The proposed work relies on this idea.

C. Digital Twin Enabling Technologies and Security Challenges

Fuller, Fan, Day, and Barlow [3] explored the enabling technologies, challenges, and open research problems of Digital Twin architectures. Their research helped lay the technological groundwork necessary for creating Digital Twin frameworks and the significance of the integration of physical and virtual systems for efficient monitoring and simulation. Digital Twin technology helps create a platform for describing the state of systems and ensuring constant interaction between real and virtual systems. Nevertheless, the paper has a limited scope of applications related to cybersecurity, especially cloud infrastructure. This gives a chance to apply Digital Twin technology to cybersecurity and use the virtual environment to monitor cloud resources and analyze the system's performance and test possible cyber attacks. The suggested research will use the Digital Twin foundation in order to develop an AI-based cloud cybersecurity architecture.

D. Reinforcement Learning for Automated Cybersecurity Decision-Making

The authors Sutton and Barto [4] discussed the basic ideas behind Reinforcement Learning (RL). This is the field where the intelligent agent learns to make decisions as a result of interactions with the environment and according to the feedback received after taking particular actions. Reinforcement Learning serves as a foundation for automated decision-making in the changing environment, since the intelligent agent can learn how to take right actions as a result of interactions instead of having only preprogrammed actions. The problem with the research is that it mainly discusses single-agent reinforcement learning, while the cyber-secure environment might need the presence of several agents working at different security situations. This explains why the MARL concept is important for the AI Digital Twin approach.

E. Cyber Digital Twin Frameworks for Security Testing

The Cyber Digital Twin (CDT) framework was proposed by Somma, Casola, Cavalli, De Benedictis, Mallouli, and Valdés [5] to ensure the security of CPS. CDTs are defined using the concept of a layered architecture that includes physical, virtual, and decision-making layers that allow the CDT to represent system components and perform intrusion detection and security testing activities.

The described approach provides an example of how a virtual copy of the system can be used to study cybersecurity conditions and carry out the security analysis in a controlled environment. Also, this work introduces the basics for the implementation of system monitoring and security decision-making integration. However, the described framework can be applied to industrial control and cyber-physical systems and is not suitable for cloud-native infrastructure and multi-agent environments. In this way, its applicability to cloud-based environments is restricted. The present work continues research in this area by introducing concepts of Digital Twin to cloud infrastructure in addition to AI/ML-based threat detection and multi-agent decision-making.

F. Applications in Smart Grids and Energy Management

The article by Alhamam, Rahman, and Aljughaiman [6] provided a thorough systematic review of cybersecurity risks involved in Digital Twin implementation. Using the PRISMA approach, the study analyzed 74 research publications and categorized Digital Twins into five tiers of risk considering cybersecurity requirements and vulnerability aspects. According to the findings of this study, there exist several types of significant threats, including unauthorized access, DoS attacks, data breaches, and malware. The researchers' paper also points out the importance of implementing security solutions, namely Multi-Factor Authentication (MFA), IDS/IPS, SIEM, Artificial Intelligence/Machine Learning (AI/ML), and blockchain-based cybersecurity solutions. However, it is evident that the growing connectivity of the physical world and its virtual representation opens new opportunities for attacks and increases the attack surface. Thus, there is a need to implement adequate security measures at all stages of the Digital Twin lifecycle. Nonetheless, the mentioned work offers a systematic review of existing cybersecurity challenges and defense mechanisms but does not suggest the development of the cloud-native Digital Twin framework. Particularly, the authors do not focus on developing the combination of the real-time cloud monitoring, threat prediction using artificial intelligence (AI), and Multi-Agent Reinforcement Learning for cybersecurity adaptation. In contrast, the suggested research aims.

G. Multi-Agent Systems and Digital Twin-Based Collaborative Defense

Cui et al. [7] studied the potential of using Multi-Agent Systems along with Digital Twin for collaborative defense against cyber-attacks. The research of Cui et al. is concerned with collaboration of multiple intelligent agents aimed at identifying and coping with security threats, such as DoS attack and hybrid attack. Collaborative work of multi-agent system allows several agents to participate in the process of monitoring and defending against attacks, thus improving security monitoring and defense. It is possible to see that the combination of Digital Twin and multi-agent system is a promising direction to enhance cybersecurity. Nevertheless, the research does not consider cloud environment and thus, there is a gap in this field for further investigation. Thus, the suggested research builds upon this idea and develops an idea of creating several special-purpose agents within a cloud digital twin driven by artificial intelligence.

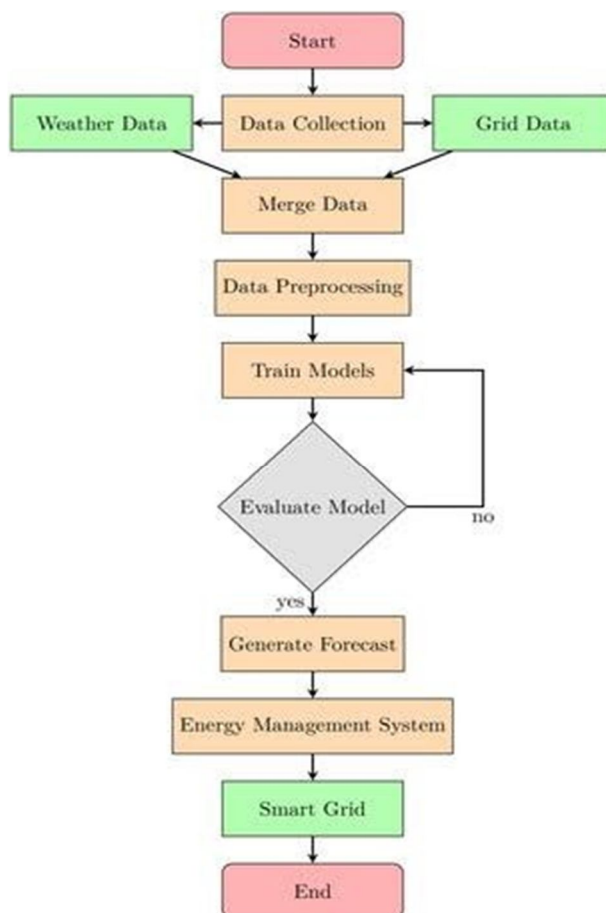


Figure 1 :Flow of model building

The flowchart starts with gathering data from weather stations and grid and then processing the data. After processing the data, the models are trained using the data and then evaluated. If the model does not meet the requirements, the process repeats until the right forecast model is developed. The forecast model is then used to develop forecasts which are fed into the EMS to help operate the smart grid.

III. CHALLENGES AND LIMITATION

The implementation of an AI Digital Twin solution in cloud cybersecurity is likely to encounter a number of difficulties and limitations. One of the main difficulties includes real-time synchronization between the actual cloud environment and its Digital Twin since cloud environment, its network, and workload can be changing continuously. Moreover, the rise of connections between the physical world and virtual one can cause extra attack surfaces and vulnerabilities [2], [3]. Several studies have indicated that unauthorized access, DoS attacks, data breaches, and malware are the major threats to the security of Digital Twin environments [6]. Another limitation includes a dependency of AI/ML algorithms on proper training data, since limited or unbalanced datasets can decrease the ability of algorithms to detect new attacks [1]. The utilization of Multi-Agent Reinforcement Learning can pose certain difficulties, associated with the coordination of agents, computing power and adaptive decision making [4]. Besides, safe simulation of the attacks, including DDoS, SQL injection, XSS, brute force attacks, port scanning, phishing and malware, will require proper isolation to ensure that production cloud resources will not be impacted. Real-time monitoring of the CPU, RAM, disk, network, and processes can raise computing and system overheads. In the present stage of development, the authentication, role-based access, and cloud management modules are already developed, whereas Digital Twin Simulation Layer and AI are yet to be developed. Thus, a need for testing with varied attack scenarios and cloud workloads arises before evaluation of the entire framework [5], [6].

IV. INTERPRETATION

This framework clearly shows how the combination of Digital Twin technology, Artificial Intelligence/Machine Learning, and Multi-Agent Reinforcement Learning can be beneficial to create proactive cloud cybersecurity solutions. Using Digital Twin will allow creating the virtualized environment with the replication of cloud infrastructure and monitoring of servers, network topology, and system metrics [2], [3]. AI and ML technologies can be used for the detection, classification, anomaly detection, and risk assessment on the basis of security-related data [1]. Using multiple intelligent agents can help overcome the limitations of traditional single-agent or reactive security measures [4], [7]. The previous research of Cyber Digital Twin has already proven the effectiveness of such an approach in terms of security testing. However, the recent literature reviews reveal the cybersecurity risks related to interconnected Digital Twin environment [5], [6]. From the standpoint of implementation, the results show that the system foundation has been successfully created. Specifically, there is MERN environment, authentication, role-based access control and cloud management implemented. Currently, the development of Digital Twin module continues and then the process of attack simulation, AI implementation, and security analysis via dashboard can continue.

Table I: Models and Their Description

Sr. No.	Model / Technique	Description
1	Random Forest	Used for attack detection, classification, and risk assessment by analyzing security-related features.
2	Decision Tree	Provides rule-based classification of security events and helps identify different types of attacks.
3	XGBoost	Used for efficient attack classification and prediction with improved learning performance.
4	Isolation Forest	Used for detecting abnormal and anomalous behavior in cloud activity and network data.
5	Multi-Agent Reinforcement Learning (MARL)	Enables multiple intelligent agents to collaboratively monitor threats and select adaptive security response

V. FINDINGS

The findings of the conducted investigation suggest the opportunity to create a systematic method based on the usage of Digital Twin technology in connection with AI/ML and MARL for cloud cybersecurity improvements. According to the literature review, the existing ML-based intrusion detection systems are efficient in recognizing attack patterns but cannot detect unknown attacks [1]. The Digital Twin researches offer such capabilities as real-time monitoring and simulation, but most existing models are oriented not to the cloud but manufacturing or cyber-physical environment [2], [3], [5]. Moreover, the recent investigations reveal substantial security challenges within the Digital Twin environment, such as unauthorized access, DoS attacks, data breach and malware [6]. The study reveals that multi-agent systems can help defend the environment from cyberattacks [7]. From the implementation point of view, the conducted investigation reveals that the system has been successfully implemented, with the creation of MERN basic structure, database connectivity, authentication, sessions with JWT and role-based access, as well as cloud control capabilities. The Digital Twin component, containing virtual servers, live metrics and network topology, is in process of being created [8].

VI. FUTURE ENHANCEMENT

The AI Digital Twin can be made even more sophisticated by fully implementing the Digital Twin simulation component along with the future implementation of the planned AI/ML models that will provide attack detection, attack classification, anomaly detection, and risk scoring in real time. The future developments may involve advanced attack simulations for DDoS, SQL injections, XSS, brute force, port scan, phishing, malware attacks in the virtual cloud environment. Additionally, the Multi-Agent Reinforcement Learning component can be further developed to allow better cooperation between monitoring, detection, and response optimization agents in order to make security decisions based on their interactions. The real-time dashboard can also be improved with advanced analytics, security alerts, logs, visualization, and security reporting functionalities. Finally, the framework can be tested using larger and more diversified cloud environments in order to assess its scalability and effectiveness in various cybersecurity scenarios. [4], [5], [6], [7]

VII. OBJECTIVES

Digital Twin of Cloud Infrastructure Development in Real-Time: The objective is to design and develop a real-time Digital Twin for the cloud infrastructure which consists of virtual servers, network topology, and live system data.

Safe Cyberattack Simulation: The system strives to create an attack simulation module that will be able to safely conduct simulations of DDoS, SQL injections, XSS, brute-force attacks, port scanning, phishing, and malware within the Digital Twin.

Threats Detection Using AI and Machine Learning: The system aims at using AI and Machine Learning models such as Random Forest, Decision Tree, XGBoost, and Isolation Forest for threat detection, classification, anomaly detection, and risk scoring.

Multi-Agent Adaptive Defense: The system aims at using Multi-Agent Reinforcement Learning technology to facilitate collaborative decision-making for monitoring, detecting, and responding-optimizing agents.

Cloud Monitoring in Real-Time: The system aims at constantly monitoring CPU, RAM, Disk, Network and processes to detect abnormal behavior and gather real-time information about current conditions of cloud resources.

Real-Time Security Dashboard and Alerts Management: The system aims at creating a security dashboard which will be providing real-time security alerts, logs, analytics and automated reports.

Secure Role-Based Cloud Management: The system aims at providing a secure cloud management via authentication, JWT sessions, role-based access control and bcrypt protection for passwords.

VIII. ALGORITHMS PROPOSED

The developed AI Digital Twin for Cloud Cyber Security solution integrates machine learning-based attack detection with anomaly detection, risk assessment, severity classification, and Digital Twin-based resource impact analysis.

1) *Random Forest – Attack Classification [16]*

Random Forest is used to classify detected security events into different attack categories based on the results of several decision trees. In the proposed system, the cloud-security parameters such as CPU usage, RAM utilization, network activity, disk activity, and process information may be used as the feature values.

2) *Decision Tree – Attack Classification [16]*

Decision Tree is utilized to classify security events according to the characteristics. It represents a rule-based structure for making decisions. The tree structure helps to determine various types of cyberattacks, and its interpretable nature is useful for determining which features cause the particular classification.

3) XGBoost – Attack Classification [16]

XGBoost is used for efficient attack classification and prediction. It uses multiple decision trees sequentially to predict the result and can find the complex relations among cloud-security features.

4) Isolation Forest – Anomaly Detection [17]

This algorithm is used to detect abnormal behavior of cloud activity and network traffic. It can be helpful for detecting attacks that do not match

5) Risk Scoring Based on Rules - Risk Assessment [16]

Upon the detection of an attack/anomaly, a risk assessment tool based on rules is applied in order to identify the possible risk associated with the security incident. Factors such as the nature of attacks, resource impact, vulnerability, and frequency of attacks are considered in the analysis.

6) Severity Level Classification Based on Rules [16]

The identified risk is classified into four severity levels: Critical, High, Medium, and Low. This will facilitate the prioritization of security incidents and make it possible for the security dashboard to highlight the most critical threats.

7) Impact Calculation of the Digital Twin - Resource Impact Analysis [17]

Digital Twin is used to compare the normal state and the state with impact of cloud resources. The impact of the identified attack is analyzed with the use of parameters such as CPU, RAM, disk, network, and process activity.

A. Project Overview

The AI Digital Twin for Cloud Cyber Security project will be aimed at creating an advanced security framework in the cloud computing environment. In the framework of this system, Digital Twin technology is implemented to form a virtualized image of the cloud system, providing the possibility of real-time analysis, monitoring, and simulation of cybersecurity threats. Artificial Intelligence (AI) and Machine Learning (ML) technologies are applied to perform threat detection, identify anomalies, classify attacks, and assess risks. Moreover, Multi-Agent Reinforcement Learning (MARL) is used to make collaboration decisions within a set of security agents in case of detected threats. At that, the project also includes cloud resource management, secure authentication, role-based access control, security alerts, logging, and monitoring capabilities.

Table II. Overview Of Issues Approaches, Methods

Component	Description
Digital Twin	Simulation model of cloud computing environment for the monitoring and analysis of security.
AI/ML Models	Detection, classification, and analysis of various forms of cyber attacks and anomalies.
MARL	Collaboration and adaptation of several security agents against the security threat.
Attack Simulation	Simulation of a secure environment for the execution of cyber attacks.
Cloud Monitoring	Monitoring of CPU, RAM, Disk, Network, and Process Activity.
Security Dashboard	Real time alerting, logging, reporting and other security related information generation.

B. Framework Design of the Project

The proposed architecture involves a hierarchical arrangement where the cloud infrastructure, digital twin technology, threat detection using AI/ML techniques, and MARL are applied collectively. The cloud provides the needed infrastructure and real-time system data. Digital Twin technology creates the virtual representation of the system. Anomaly detection, classification, prioritization of threats, and security risk assessment is carried out using AI/ML techniques. Finally, the MARL agents will collaborate to determine the relevant security responses. There is also the monitoring and dashboard layer where the real-time metrics and security analysis are offered.

C. Mathematical Formulation of Proposed Algorithms

1) Random Forest – Attack Classification

$$\hat{y} = \text{mode}\{T_1(X), T_2(X), \dots, T_N(X)\}$$

where X represents the security features and $T_i(X)$ represents the prediction of the i th decision tree.

2) Decision Tree – Attack Classification

$$H(S) = - \sum_{i=1}^C p_i \log_2(p_i)$$

The information gain is

3) Isolation Forest – Anomaly Detection

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}}$$

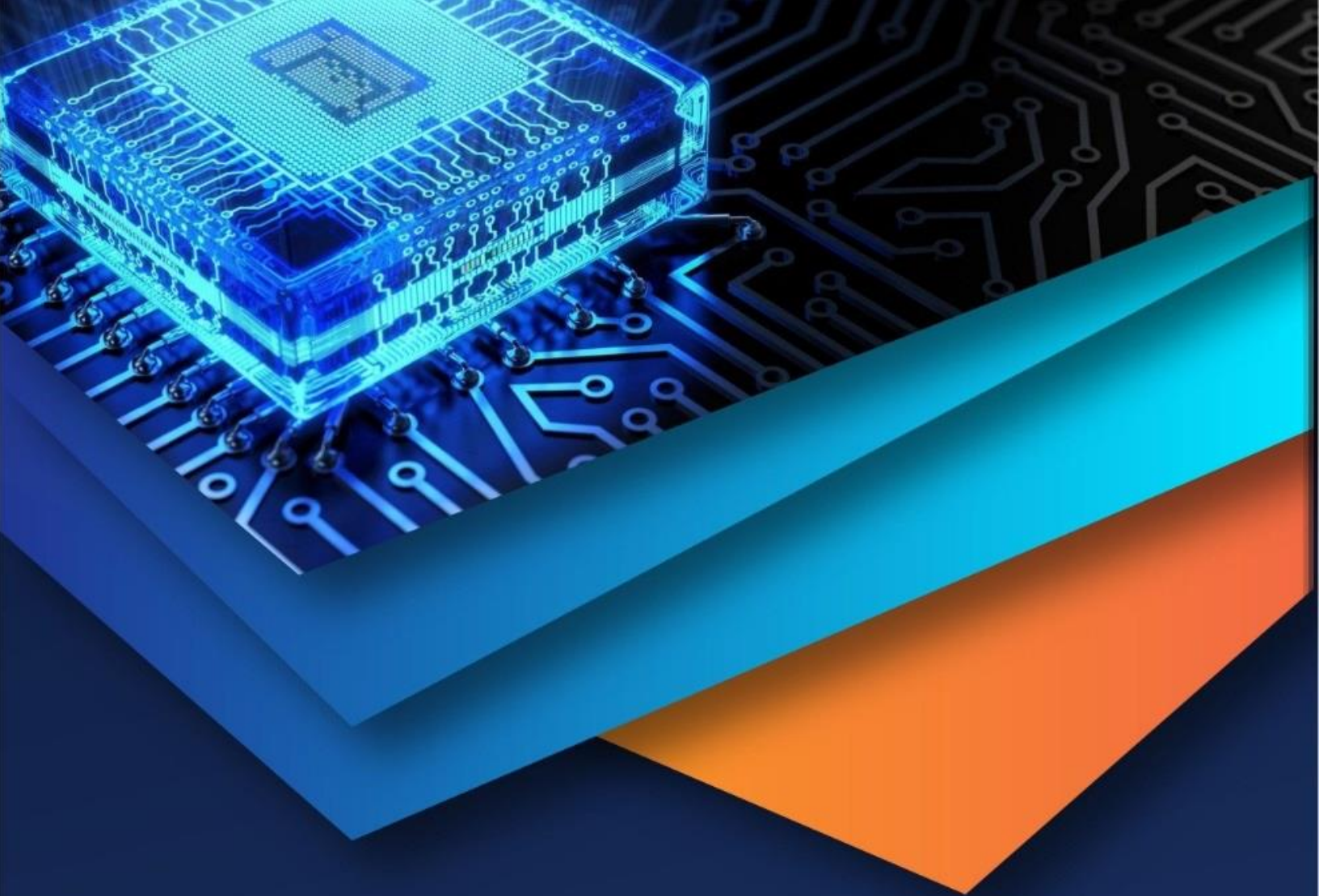
where $E(h(x))$ represents the average path length of an observation.

IX. ACKNOWLEDGMENT

It is a great pleasure for us to acknowledge the valued guidance, support, and encouragement that we have received from our honored guide, Prof. Umesh Samarth, throughout the process of this project. We are grateful to the Department of Information Technology, J D College of Engineering and Management, for providing the necessary resources and facilities to complete this work. We are thankful to Dr. Amit Welekar, Head of the Department, for his valued support and encouragement. We are thankful to all our teachers, friends, and family members for their constant encouragement and support in completing this project successfully.

REFERENCES

- [1] F. Tao, M. Zhang, Y. Liu, and A. Y. C. Nee, "Digital Twin Driven Smart Manufacturing," IEEE Transactions on Industrial Informatics, 2019.
- [2] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital Twin: Enabling Technologies, Challenges and Open Research," IEEE Access, vol. 8, pp. 108952–108971, 2020.
- [3] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
- [4] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed., MIT Press, 2018.
- [5] A. Somma et al., "A Cyber Digital Twin Framework to Support Cyber-Physical Systems Security," IEEE Security & Privacy, 2023.
- [6] N. Alhamam, M. M. Hafizur Rahman, and A. Aljughaiman, "A Comprehensive Review on Cybersecurity of Digital Twins: Issues, Challenges, and Future Research Directions," IEEE Access, 2025.
- [7] Y. Cui et al., "Multi-Agent Systems and Digital Twin-Based Collaborative Defense Against Cyberattacks," 2023.
- [8] A. Shaikh et al., "A Digital Twin-Based Security Model for Cybersecurity Threat Detection," 2023.
- [9] A. Atalay and P. Angin, "Digital Twin-Based Security Testing for Cyber-Physical Systems," 2020.
- [10] M. Suhail et al., "Explainable Deep Learning-Based Cybersecurity Analysis Using Digital Twins," 2023.
- [11] A. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, 2016.
- [12] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed., MIT Press, 2018.
- [13] A. Somma et al., "A Cyber Digital Twin Framework to Support Cyber-Physical Systems Security," IEEE Security & Privacy, 2023.
- [14] N. Alhamam, M. M. Hafizur Rahman, and A. Aljughaiman, "A Comprehensive Review on Cybersecurity of Digital Twins: Issues, Challenges, and Future Research Directions," IEEE Access, 2025.
- [15] M. Suhail et al., "Explainable Deep Learning-Based Cybersecurity Analysis Using Digital Twins," 2023.
- [16] M. Alhamam, M. M. Hafizur Rahman, and A. Aljughaiman, "A Comprehensive Review on Cybersecurity of Digital Twins: Issues, Challenges, and Future Research Directions," IEEE Access, vol. 13, pp. 45106–45124, 2025, doi: 10.1109/ACCESS.2025.3545004.
- [17] "Digital-Twin-Based CPS Anomaly Diagnosis and Security Defense Countermeasure Recommendation," IEEE Transactions/IEEE publication, 2024, doi: 10.1109/... [IEEE Xplore].



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)