iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49857

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Review on Intrusive Detection to Secure Social Internet of Things in Edge Computing

Bhumika M[1], Dr. Praveen Kumar K V[2]
[1]*Student, Dept. of Computer Science Engineering,*
[2]*Professor, Dept. of Computer Science Engineering, Sapthagiri Engineering College*

Abstract: ***This review paper presents an analysis of the latest developments in Intrusion Detection Systems (IDSs) for securing the Social Internet of Things (SIoT). The authors focus on the limitations of conventional IDSs and underscore the importance of leveraging advanced techniques, particularly deep learning, for efficient and effective intrusion detection in SIoT. The article evaluates various recent research studies that have utilized deep learning models for intrusion detection in SIoT. It discusses the types of deep learning models employed and offers valuable insights into the current state-of-the-art in IDSs for securing SIoT. The review concludes by highlighting the potential of deep learning techniques in achieving accurate and effective intrusion detection in SIoT networks.***

Keywords: Intrusive Detection System, deep learning technique, Social Internet of Things.

I. INTRODUCTION

The advent of the Internet of Things (IoT) in recent years has created vast opportunities for innovative services and technologies. IoT allows numerous devices and sensors to connect to the internet and share data, leading to new possibilities for advancement. However, the increasing number of connected devices also poses a significant security risk. Thus, ensuring security has become a top priority in the development of IoT technology.

One particular area of IoT that requires special attention is the Social Internet of Things(SIoT) refers to the integration of social media technologies and IoT, which allows for social interactions between individuals and smart objects. It involves the connection of physical objects to the internet and their integration with social media networks, allowing for real-time communication and collaboration among users and objects. This integration has the potential to create new opportunities for social interaction, knowledge sharing, and collaborative problem-solving.Examples of SIoT devices include smart homes, wearable health devices, and social robots. These devices have the potential to collect sensitive information about users, such as their personal preferences, health data, and social interactions. As such, it is crucial to ensure that SIoT devices are secure and protected from cyber-attacks.

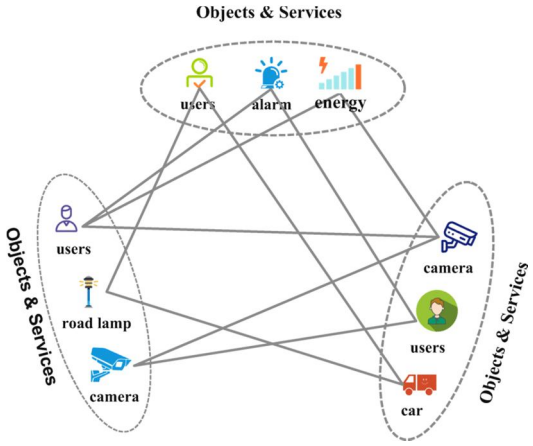


Fig.1.Example of SIoT

A cyber attack is a deliberate and malicious act that exploits computer systems and networks for various purposes, such as stealing information or disrupting services. Cyber attacks can manifest in various ways, such as malware, phishing, and denial-of-service attacks. They can have severe consequences, leading to financial losses, reputational damage, and physical harm. As technology reliance increases, organizations must remain vigilant against cyber attacks.

There are few types of cyber attacks they are:

1) *Malware:* Malware is a type of harmful software that is intentionally created to penetrate, harm, or interrupt a computer system, and to obtain data without the user's authorization or awareness.
2) *Phishing:* The practice of tricking people into divulging their personal information or login credentials through fake emails, websites, or social media messages.
3) *Denial-of-service (DoS):* This attack refers to a harmful and dangerous attempt to disturb normal traffic of a targeted server or network, rendering it inaccessible to legitimate users
4) *Ransomware:* A type of malicious software that uses encryption to lock files and demands payment in exchange for the decryption key.
5) *Social Engineering:* A strategy that takes advantage of human psychology to influence individuals into revealing confidential information or taking actions that may not be beneficial to them.

Intrusion detection systems (IDSs) are commonly used to protect computer networks from cyber-attacks. These systems work by analyzing network traffic and identifying suspicious activity that may indicate an intrusion attempt. However, IDSs are not always effective in protecting IoT networks, particularly those in the SIoT domain. This is because SIoT networks are typically more complex and dynamic than traditional computer networks, making them harder to monitor and secure.

Network Intrusion Detection System (NIDS) is a cybersecurity tool used to monitor network traffic for signs of suspicious activity, policy violations, and potential security breaches. By analyzing network packets, NIDS can detect abnormal or malicious traffic that could indicate a security threat. When suspicious traffic is detected, NIDS generates alerts that provide security teams with information and intelligence to investigate and respond to potential security incidents.

Collaborative edge computing is a decentralized computing model where multiple edge devices work together to process and analyze data at the edge of the network. It enables the distribution of computing tasks among multiple devices, leading to faster processing and reduced latency. This approach enhances the performance and efficiency of edge computing while reducing the burden on individual devices.It has been proposed as an effective solution for addressing the security challenges of SIoT networks. It involves decentralizing computing tasks to devices located at the network edge, leading to enhanced efficiency, reduced latency, and improved security by minimizing the risk of data breaches.

Deep learning is a form of machine learning that leverages artificial neural networks to process and analyze extensive datasets. These networks are made to emulate the operation of the human brain, which enables the system to acquire knowledge and enhance its performance through practice, without the requirement of explicit programming. It involves the creation of multiple layers of interconnected nodes that can process and extract features from raw data, enabling the network to identify complex patterns and make accurate predictions. There are different types of deep learning algorithms. Deep learning algorithms have found extensive use in various fields, including and not limited to natural language processing, computer vision, and speech recognition.

The types of algorithms are:

a) Convolutional Neural Network (CNN) is a powerful deep learning algorithm designed for image and video analysis, consisting of multiple interconnected layers that can identify patterns and features from raw data. CNN is widely used for tasks such as object recognition and image classification.
b) Recurrent Neural Network(RNN) is a type of deep learning algorithm used primarily for processing sequential data such as text or speech. It uses feedback loops to allow information to persist and flow through the network, making it effective for tasks such as language translation, speech recognition, and natural language processing.
c) Generative Adversarial Network (GAN) is a powerful deep learning algorithm capable of detecting intrusions. The GAN consists of two neural networks - a generator and a discriminator. The generator generates new data samples, whereas the discriminator is trained to differentiate between genuine and generated data through an adversarial process.

Deep reinforcement learning (DRL) is a machine learning technique that uses trial and error to allow agents to learn in a dynamic environment. Unlike traditional reinforcement learning, DRL uses deep neural networks to approximate agents' optimal decision strategies and rewards them when they make desirable decisions. DRL has been successfully used in various applications such as gaming, robotics, and autonomous driving.

II. LITERATURE SURVEY

Several studies have been conducted on intrusion detection for SIoT. For instance, in The authors, Y. Zhao et al.[1] proposed an algorithm for detecting dense subgraphs in social Internet of Things (SIoT) networks, which is based on a two-step approach involving a greedy algorithm and a branch-and-bound algorithm. The authors claim that their algorithm is effective and efficient, and they provide theoretical analysis and experimental results to support their claims. The paper provides a detailed introduction to SIoT and the need for efficient algorithms for detecting dense subgraphs, and also briefly reviews existing algorithms in this area. Overall, the paper is well-written and presents an innovative algorithm that addresses the limitations of existing algorithms in the context of SIoT networks.

The authors Y. Zhang et al. [2] proposed a novel approach to improving the computing efficiency of mobile edge-cloud computing (MEC) networks by implementing a resource sharing mechanism.The proposed approach utilizes machine learning algorithms to optimize the allocation of computing resources between edge devices, cloud servers, and end-users by taking into account the current network conditions and resource availability. The authors demonstrate the effectiveness of their scheme through simulations and comparisons with existing resource allocation schemes.

The authors A. Ghosh et al. [3] proposes an edge-cloud computing architecture for IoT data analytics that incorporates deep learning techniques to enable intelligence at the edge. The proposed architecture leverages both edge devices and cloud servers to perform data analytics tasks, with the goal of reducing data transmission and processing overheads while improving data privacy and security. The authors discuss various challenges associated with implementing such an architecture, including resource constraints, data heterogeneity, and security concerns. They also present a case study on object recognition using deep learning on edge devices, demonstrating the feasibility and effectiveness of their approach.

The authors Z. Ning et al [4] introduces a novel computing and caching system for Internet of Vehicles (IoV) that integrates deep reinforcement learning (DRL) to optimize traffic control. The proposed model comprises mobile network operators (MNO), roadside units (RSU), and vehicles equipped with computing and communication capabilities. The use of DRL algorithms enables the system to learn and adapt to the network conditions, making it an effective approach for managing traffic in IoV.. The DRL-based traffic control algorithm takes into account the dynamic traffic status and adjusts the computing and caching resources accordingly to optimize the network performance. The experiment output show that the proposed system performs much efficiently than the traditional approaches in terms of delay, throughput, and network utilization. The paper provides an efficient solution for the emerging IoV networks with the potential for future improvements. The authors C. Chen et al.[5] proposed a deep learning-based edge traffic flow detection scheme for intelligent transportation systems. The proposed scheme is designed to monitor and analyze traffic flow data at the edge of the network, with the goal of detecting and predicting traffic congestion in real-time. The authors discuss the challenges of traditional traffic flow detection methods and explain how their proposed scheme can address these challenges. The scheme utilizes a convolutional neural network (CNN) to extract features from traffic flow data and a long short-term memory (LSTM) network to perform traffic flow prediction. The authors evaluate the performance of the proposed scheme using real-world traffic flow data and show that it outperforms traditional traffic flow detection methods in terms of accuracy and efficiency. The authors Z. Ning et al [6] proposed a decentralized game theoretic approach for mobile edge computing enabled 5G health monitoring for the Internet of Medical Things (IoMT). The authors discuss the challenges of implementing a health monitoring system for IoMT and how their proposed approach can address these challenges. The approach involves a game theoretic model for task offloading and resource allocation among the various entities in the system, including mobile devices, edge servers, and cloud servers. The authors evaluate the performance of the proposed approach using simulation experiments and show that it outperforms traditional centralized approaches in terms of latency, energy consumption, and network throughput.

The authors H. Yang et al. [7] introduced a novel solution to enhance the security of wireless communication using an intelligent reflecting surface (IRS) aided scheme that leverages deep reinforcement learning (DRL). The scheme optimizes the IRS's reflection coefficients to improve the quality of wireless transmission while strengthening the security of the communication. The authors evaluate the effectiveness of the proposed scheme through simulations, demonstrating its ability to improve both communication quality and security.

The author H. Yang et al. [8] proposed the concept which combines AI techniques and wireless communication technologies to enhance the fruition of 6G networks. It presents quite a lot of potential use cases of intelligent 6G networks, such as smart transportation, industrial internet, and intelligent healthcare. The paper also discusses the challenges and research directions for implementing such networks, including the need for more efficient AI algorithms, better hardware support, and collaboration among different domains Their paper offers a valuable contribution to the exploration of intelligent 6G networks and their potential impact on society.

The utilization of generative adversarial network algorithm (GAN) for intrusion detection in social Internet of Things (SIoT) via collaborative edge computing has been proposed by Laisen Nie et al. [9]. Their method involves the application of a GAN model to differentiate normal traffic samples from anomalous ones. The model is trained using a dataset that includes both normal and anomalous traffic samples, and the generated normal samples help enhance the accuracy of the intrusion detection system. Additionally, the approach utilizes collaborative edge computing to minimize the computational and communication overhead in SIoT. However, deep learning-based network intrusion detection systems (NIDS) are prone to attacks that evade detection and can result in damage, posing a significant challenge..

The authors Chaoyun Zhang et al.[10] conducted an analysis of the effectiveness of adversarial attacks on deep learning-based Network Intrusion Detection System (NIDS) and introduced two defense mechanisms. The first mechanism involves manipulating the input data using a pre-processing technique to improve the NIDS's robustness. The second mechanism, an adversarial training technique, modifies the NIDS's training process to enhance its resistance to adversarial attacks. The proposed mechanisms were evaluated for their performance and compared with existing defense mechanisms using publicly available datasets. The results indicated that the proposed mechanisms effectively improved the NIDS's robustness against adversarial attacks.

III. CONSOLIDATED TABLE

l. No.	Title of the paper	Description	Advantage	Limitation
1.	Effective and efficient dense subgraph query in large-scale social Internet of Things	The paper proposes the DEEDS algorithm for dense subgraph identification in large-scale social IoT networks, which outperforms the existing state-of-the-art algorithms in terms of accuracy and efficiency. The algorithm can be used in real-time social IoT applications such as fraud detection and social recommendation systems.	It can be applied in real-time social IoT applications such as social recommendation systems and fraud detection, enabling personalized recommendations and detection of fraudulent activities.	1).The algorithm may require significant computational resources to execute, which could limit its applicability in resource-constrained environments. 2).The algorithm may not be suitable for identifying subgraphs with specific properties or characteristics, as it is designed to identify only dense subgraphs.
2.	Efficient computing resource sharing for mobile edge-cloud computing networks	It proposes an algorithm for efficient computing resource sharing in mobile edge-cloud computing networks, enabling dynamic and efficient allocation of resources among different devices and cloud nodes, leading to improved system performance and reduced energy consumption.	It can be applied in real-time autonomous driving systems, where fast and efficient computing resource allocation is crucial for ensuring safe and reliable operation.	The algorithm may not be suitable for certain types of real-time applications with highly dynamic resource requirements, where a more adaptive resource allocation approach may be required.
3.	Edge-cloud computing for IoT data analytics: Embedding intelligence in the edge with deep learning	This paper proposes an edge cloud computing framework for IoT data analytics that uses deep learning to embed intelligence at the edge and enable efficient and scalable processing of large amounts of data generated by IoT devices	It can be applied in real-time processing of large volumes of IoT data, suitable for industrial automation, smart cities, and healthcare applications.	1).The use of deep learning algorithms for edge computing may require significant computational resources and expertise, limiting its applicability in certain contexts. 2).The proposed framework may require careful management of data privacy and security issues related to IoT data processing.
4.	Joint computing and caching in 5G-envisioned Internet of vehicles: A deep reinforcement learning-based traffic control system	This paper presents a traffic control system for shared computing and caching in the 5G-based Internet of Vehicles that utilizes Deep Reinforcement Learning. The system aims to enhance network performance by optimizing resource allocation and reducing latency.	The system manages traffic flow in 5G-enabled Internet of Vehicles in real-time, optimizing computing and caching resources to improve network performance, reduce latency, and enable new applications.	1).Limited scalability due to centralized architecture 2).Vulnerability to security and privacy issues

Sl. No.	Title of the paper	Description	Advantage	Limitation
5.	An edge traffic flow detection scheme based on deep learning in an intelligent transportation system	In this it proposes, a Deep Learning based roadside traffic flow detection method for intelligent transportation systems is proposed. It uses CNNs and edge computing for real-time detection and prediction to improve traffic management, reduce congestion, and increase safety.	It enables accurate and rapid detection and prediction of traffic flow, which can facilitate efficient traffic management and reduce congestion in intelligent transportation systems. By using edge computing, the system also reduces communication overhead and improves efficiency, making it suitable for real-time applications.	1).The proposed scheme requires a large amount of traffic data to train the CNNs effectively, which can be challenging to obtain in practice. 2).The accuracy of the scheme can be affected by factors such as changes in traffic patterns, weather conditions, and incidents.
6.	Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach	This proposes a game-theoretic approach for mobile edge computing-enabled 5G health monitoring in the Internet of Medical Things. It aims to optimize resource allocation and minimize latency, considering the trade-off between computational costs and quality of service, to improve healthcare services' efficiency and effectiveness.	The advantage of the proposed approach in real time is that it can adapt to dynamic network conditions and optimize resource allocation and latency in real time, which enables efficient and effective health monitoring in the Internet of Medical Things.	1).The approach requires a significant amount of computational resources to implement the game-theoretic model, which may not be feasible in some scenarios. 2).The approach does not consider the security and privacy issues that may arise from collecting and processing medical data
7.	Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications	In this , an intelligent reflective surface based on gain learning is proposed for secure wireless communication. The proposed surface uses gain learning to optimize signal reflection and improve communication security, with the goal of enhancing the quality and reliability of wireless communication	The real-time application of the proposed intelligent reflective surface is that it can optimize signal reflections and improve communication security in real time, thereby enhancing the quality and reliability of wireless communication.	1) The approach does not consider the impact of other wireless communication systems that use the same frequency band and may affect the performance of the proposed smart reflective surface. 2) The reinforcement learning algorithm used in the proposed approach requires a large amount of data for training, which can be time consuming and computationally intensive.

Sl. No.	Title of the paper	Description	Advantage	Limitation
8.	Artificial-intelligence-enabled intelligent 6G networks	In this, the potential of artificial intelligence (AI) to enable 6G smart networks. It discusses the challenges and opportunities of integrating AI into 6G networks, including improving security, increasing energy efficiency, and enabling new applications. The paper also highlights the need for collaboration between academia, industry, and standards organizations to realize the full potential of AI-enabled 6G networks.	The integration of AI into 6G networks enables intelligent resource allocation, efficient network management, and proactive threat detection and prevention, making it suitable for real-time applications such as autonomous vehicles, industrial automation, and telemedicine. .	There is no detailed analysis of the technical challenges and limitations of implementing AI-enabled intelligent 6G networks, such as the complexity of the algorithms, the accuracy of the data, and the interoperability with legacy systems.
9.	Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach	This proposes an approach based on generative adversarial networks (GAN) for intrusion detection in secure social Internet-of-Things (IoT) systems based on collaborative edge computing. The proposed approach uses GANs to generate synthetic data for training intrusion detection models and leverages collaborative edge computing to improve detection accuracy and reduce communication overhead.	1). The approach can be used in real-time to monitor and secure various social IoT applications, such as smart homes, wearables, and connected vehicles, by leveraging the collaborative edge computing architecture. 2). The approach's ability to generate synthetic data using GANs can help overcome the challenges of data scarcity and privacy concerns in social IoT systems, making it suitable for real-time applications	1).The proposed approach relies on the availability of sufficient training data to train the GAN model, which may be challenging in some social IoT scenarios, especially those where privacy concerns exist. 2).The effectiveness of the proposed approach in detecting new and unknown types of attacks in real-time has not been thoroughly evaluated and validated.
10.	Adversarial Attacks Against Deep Learning-based Network Intrusion Detection Systems and Defense Mechanisms"	This presents an analysis of attacks against deep learning-based network intrusion detection systems and proposes defense mechanisms to improve the robustness of the system against such attacks. The paper examines different types of attacks and evaluates the effectiveness of various defense strategies using benchmark datasets	1).Real-time defense mechanisms against hostile attacks in NIDS help maintain the integrity of critical network infrastructures and prevent cyberattacks. 2).They can increase the robustness and reliability of NIDS, improving their overall performance and accuracy in detecting network intrusions.	1).Attacks by attackers can be sophisticated and difficult to detect, making it difficult to develop effective defenses. 2).Defensive mechanisms may burden the NIDS with additional overhead and complexity, which may affect its performance and scalability.

IV. ACKNOWLEDGEMENT

Any achievement does not depend solely on the individual efforts but on the guidance, encouragement and co-operation of intellectuals, elders and friends. We extend our sincere thanks to **Dr**. **Kamalakshi Naganna**, Professor and Head, Department of Computer Science and Engineering, Sapthagiri College of Engineering, and **Dr Praveen Kumar K V** Professor, Department of Computer Science and Engineering, Sapthagiri College of Engineering, for constant support, advice and regular assistance throughout the work. Finally, we thank our parents and friends for their moral support.

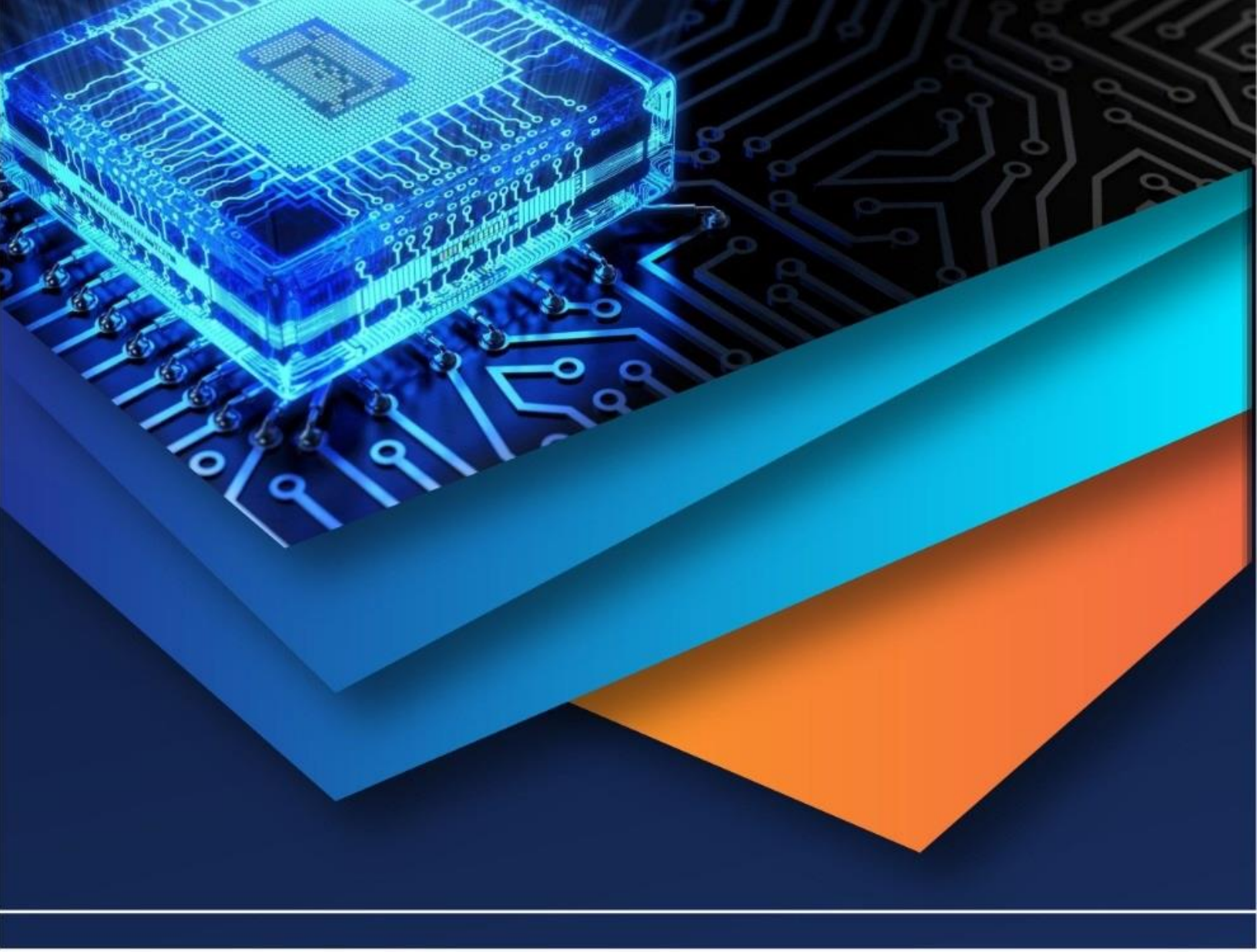
V. CONCLUSION AND FUTURE SCOPE

The papers reviewed in this study propose innovative solutions to address the challenges that arise in IoT networks. These solutions leverage advanced machine learning and deep learning techniques to enhance the performance, security, and efficiency of IoT systems. The effectiveness of the proposed solutions is supported by theoretical analyses and experimental results in various scenarios. However, there is still room for further research in this field. More efficient algorithms and architectures are needed to handle the increasing complexity and scale of IoT networks.

Future research could focus on developing more robust and scalable algorithms that can handle diverse network topologies and different types of data. The use of emerging technologies such as blockchain and edge computing may also improve the security and privacy of IoT systems. Additionally, integrating multiple domains could lead to the development of more intelligent and adaptable IoT systems. The future of IoT research is promising, and there is much potential for further advancements in this area.

REFERENCES

[1] Y. Zhao, X. Dong, and Y. Yin, “Effective and efficient dense subgraph query in large-scale social Internet of Things,” IEEE Trans. Ind. Informat., vol. 16, no. 4, pp. 2726–2736, Apr. 2020.
[2] Y. Zhang, X. Lan, J. Ren, and L. Cai, “Efficient computing resource sharing for mobile edge-cloud computing networks,” IEEE/ACM Trans. Netw., vol. 28, no. 3, pp. 1227–1240, Jun. 2020.
[3] A. Ghosh and K. Grolinger, “Edge-cloud computing for IoT data analytics: Embedding intelligence in the edge with deep learning,” IEEE Trans. Ind. Informat., vol. 17, no. 3, pp. 2191–2200, Mar. 2021.
[4] Z. Ning et al., “Joint computing and caching in 5G-envisioned Internet of vehicles: A deep reinforcement learning-based traffic control system,” IEEE Trans. Intell. Transp. Syst., early access, Feb. 5, 2020, doi: 10.1109/TITS.2020.2970276
[5]] C. Chen, B. Liu, S. Wan, P. Qiao, and Q. Pei, “An edge traffic flow detection scheme based on deep learning in an intelligent transportation system,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 3, pp. 1840–1852, Mar. 2021.
[6] Z. Ning et al., “Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach,” IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 463–478, Feb. 2021.
[7] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q.Wu,“Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications,” IEEE Trans. Wireless Commun., vol. 20, no. 1, pp. 375–388, Jan. 2021.
[8] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K.Wu, “Artificial-intelligence-enabled intelligent 6G networks,” IEEE Netw., vol. 34, no. 6, pp. 272–280, Nov. 2020.
[9] Laisen Nie , Yixuan Wu , Xiaojie Wang, Lei Guo, , Guoyin Wang, Xinbo Gao, Shengtao Li , “Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach” IEEE Trans. Computional Social System, Vol. 9, No. 1, Feb. 2022.
[10] Chaoyun Zhang, Xavier Costa-Perez, and Paul Patras, “Adversarial Attacks Against Deep Learning-based Network Intrusion Detection Systems and Defense Mechanisms”



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY