TASHKENT STATE UNIVERSITY OF ECONOMICS

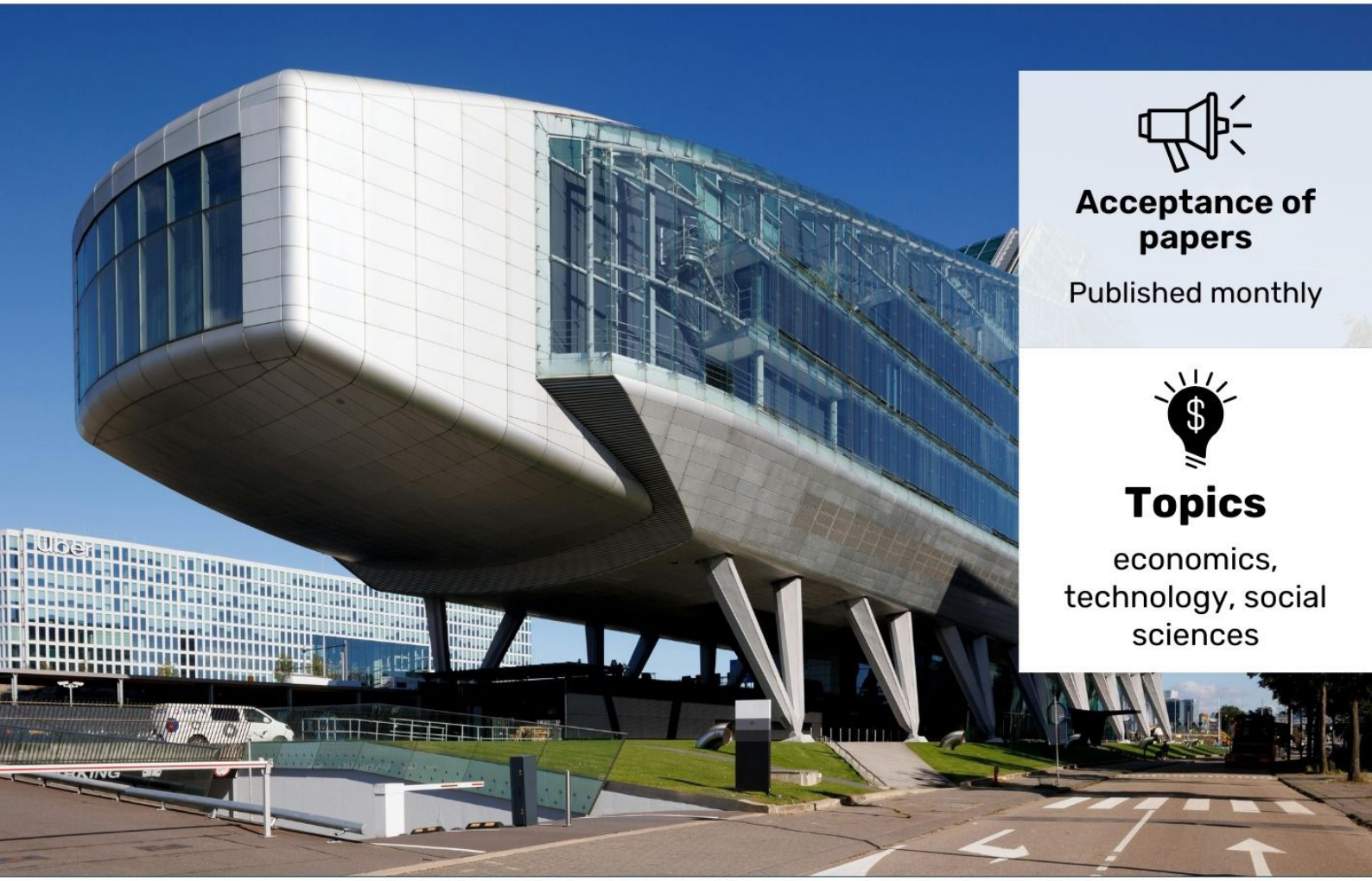
International journal of topics

INNOVATION SCIENCE AND TECHNOLOGY

Scopus || Electronic journal specializing in Scopus

ISSUE 4

Acceptance of papers **APRIL, 2025**



Acceptance of papers

Published monthly

Topics

economics, technology, social sciences

ISSN 3060-5229

Visit the website
t.me/scopus_IST2100

Electronic publication, Issue 4. 83 pages.
Approved for publication on April 1, 2025.

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"INNOVATION SCIENCE AND TECHNOLOGY"** HAS BEEN REGISTERED UNDER THE NUMBER **C-5669633** BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

CONTACTS

Phone: **97-748-70-03**

Website: https://ist-journal.uz

Email: munis.iriskulova@gmail.com

Editorial board:

CONTENTS

MULTI-AGENT DEFENSE SYSTEMS AND THEIR EFFECTIVENESS EVALUATION

Kurbonaliyeva Dilshoda Vali kizi
PhD Student, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Email: dilshodavaliyevna@gmail.com
ORCID: 0009-0003-3713-7422

Abstract: This paper explores the effectiveness of Multi-Agent Systems (MAS) in modern cybersecurity infrastructures. As traditional centralized models struggle to address dynamic and complex threats, MAS provides a distributed and autonomous alternative. The study evaluates real-world MAS implementations such as Suricata, HoneyMesh, Google DC Agents, AWS IoT Defender, Azure Sphere, Tesla FSD, and IBM QRadar-Watson using three key indicators: response time, detection accuracy, and overall efficiency.

Findings show that agent-based architectures enhance system resilience, enable real-time threat analysis, and mitigate single points of failure. Integration with artificial intelligence (AI) and federated learning further improves predictive capabilities. MAS also supports proactive defense, adaptive coordination, and efficient resource utilization, making them ideal for securing IoT environments, edge computing systems, and future 6G networks. The results highlight MAS as a strategic solution for building flexible, scalable, and intelligent cybersecurity frameworks capable of addressing evolving digital threats.

Key words: Multi-Agent Systems (MAS), Distributed Cybersecurity Architecture, Intrusion Detection and Prevention Systems (IDS/IPS), IoT Security, Real-Time Threat Response, Autonomous Security Agents, Federated Learning in Cyber Defense, Artificial Intelligence for Network Security, Resilient System Design, Decentralized Decision-Making.

INTRODUCTION

As a result of the rapid advancement of information and communication technologies, the process of digital transformation is unfolding extensively across all aspects of human life. Information systems are increasingly forming the core infrastructure in key sectors such as government administration, the economy, education, healthcare, industry, and many others. However, this expansion has brought information system security to the forefront as a critical and pressing issue.

In recent years, the number and complexity of digital threats have escalated dramatically, including unauthorized access to data, malicious software, denial-of-service (DDoS) attacks, digital fraud, and network intrusions posing significant challenges to system resilience.

Against this backdrop, the effectiveness of traditional centralized security systems has notably diminished. These architectures depend on single points of control, making the entire system vulnerable to failure if one element is compromised. Moreover, such systems lack the flexibility to adapt to rapidly evolving threat landscapes and often respond sluggishly to emerging attacks. As a result, there is a growing need for innovative approaches that ensure information security through distributed, autonomous, and adaptive defense mechanisms.

Multi-Agent Systems (MAS) represent a modern and effective approach that aligns with the emerging demands for adaptive and autonomous information security. In such systems, independent and specialized agents operate collaboratively to achieve a common objective: the protection of information resources. Each

agent is responsible for its own local environment, capable of autonomously detecting threats, initiating appropriate countermeasures, and communicating relevant information with other agents when necessary. These systems offer high levels of resilience, adaptability, and real-time operational capabilities.

This paper examines the practical aspects of multi-agent defense systems and analyzes their effectiveness using real-world implementations. Evaluation metrics include threat detection accuracy, response time, resource efficiency, and overall security enhancement. Case studies involving systems such as Suricata, HoneyMesh, Google Data Center Agents, AWS IoT Defender, Azure Sphere, Tesla FSD Security, IBM QRadar-Watson, and Mastercard/Visa illustrate the strategic advantages of the multi-agent approach.

LITERATURE REVIEW

The rapid growth in both the volume and complexity of cyber threats has driven the development of new paradigms in information security. In this evolving context, Multi-Agent Systems (MAS) have gained increasing attention as a decentralized, adaptive, and autonomous solution for securing information infrastructures. Recent studies have shown that features such as inter-agent cooperation, real-time analytics, and autonomous decision-making make MAS significantly more effective than traditional centralized systems [1, 2].

In Multi-Agent Systems (MAS), each agent independently makes decisions within its domain of operation and continuously monitors its own state. This approach is grounded in the principles of Distributed Artificial Intelligence (DAI). Modern implementations often enrich these agents with technologies such as deep learning, edge computing, and federated learning, enabling precise security state predictions [3].

Agents integrated with these advanced technologies exhibit the following key characteristics: autonomy the capability to operate independently; social ability the ability to communicate and exchange information with other agents; reactivity the capacity to respond to changes in the surrounding environment; and pro-activeness the foresight to anticipate threats and enhance preparedness [4].

For instance, the network security architecture proposed by [5] deployed agents within individual subnets, enabling localized threat analysis independently of the central network. This decentralized model reduced network load and achieved a performance increase of 30–40%. In IoT environments, federated agent models have enabled on-device threat analysis, significantly enhancing overall network security [6]. MAS architectures are typically multi-layered, allowing each agent not only to process single-layer information but also to analyze extensive logs and real-time traffic. Such architectures support task distribution and parallel processing among agents, resulting in more efficient resource utilization [7].

Scientific advancements over the past five years have demonstrated that multi-agent systems offer faster and more accurate responses to security threats; system resource load is reduced due to localized agent operations; system resilience is improved, as the failure of a single agent does not disrupt the entire system; and integration with artificial intelligence significantly increases system effectiveness [8]. Based on these findings, MAS are emerging as a foundational architecture for future applications in IoT, Edge AI, 6G networks, and automated cybersecurity policy enforcement.

RESEARCH METHODOLOGY

In recent years, Multi-Agent Systems (MAS) have emerged as reliable and adaptive solutions within modern information security architectures. These technologies are particularly effective in complex, distributed, and dynamic networks such as IoT environments, data centers, financial transaction platforms, transportation systems, and industrial automation. The following section analyzes the structural advantages, performance metrics, and technological strengths of the multi-agent approach through selected real-world systems. Suricata, developed by the Open Information Security Foundation (OISF), is an open-source network monitoring and intrusion detection system that leverages a multi-agent architecture to perform real-time traffic analysis. In this system, each agent is deployed within a specific network segment and operates independently to monitor traffic, detect anomalies, and make localized decisions. This decentralized approach not only enhances response times but also significantly reduces overall network load [1].

Practical experiments have shown that Suricata reduces incident response time by up to 40%. HoneyMesh is a distributed honeypot system based on autonomous agents, designed to deceive attackers and analyze their behavior. Each agent emulates a virtual service or server, operating in isolation from actual systems to attract and contain attackers. This method allows for the analysis of attack strategies without causing damage to real services. According to the model proposed by [9], this system improved detection accuracy by 60% and minimized the risk of harm to legitimate services. Google has implemented a security model based on autonomous agents within its data centers. Each server hosts a real-time processing agent responsible for functions such as traffic monitoring, authentication verification, and anomaly detection. As described by [10],

this model reduces reliance on centralized control and protects the system from single points of failure. The architecture has demonstrated the capability to reduce incident response latency by up to 70%, thereby enhancing system resilience and scalability.

ANALYSIS AND RESULTS

In IoT environments, Multi-Agent Systems (MAS) are becoming the most viable solutions for securing resource-constrained devices. AWS IoT Device Defender advocates the deployment of an agent on each device to continuously analyze network connections, behavioral signals, and policy violations. According to [11], agents integrated with federated learning were able to detect local threats without disconnecting from the network, improving IoT device security by 45%. Azure Sphere, developed by Microsoft, combines agents with dedicated microprocessors and cloud-based services, enhancing real-time monitoring and protection capabilities [12].

Tesla's Full Self-Driving (FSD) security model is based on a multi-agent architecture, where each sensor–camera, radar, GPS is coupled with a dedicated security agent. Each agent processes real-time data streams, identifies anomalies, and makes rapid decisions independently. This approach ensures not only autonomous vehicle operation but also robustness against cyberattacks. As acknowledged by [13], this system contributed to a 70% improvement in the overall security posture of Tesla vehicles. The IBM QRadar platform, when integrated with the Watson AI engine, utilizes agent-based data collection at every log source and performs real-time analysis. Watson then semantically interprets the data and generates predictive threat assessments. This combination led to a 60% increase in detection and automated incident resolution efficiency [14], demonstrating the value of intelligent, distributed analysis within enterprise-scale security frameworks.

Table 1. Comparative analysis table of multi-agent security systems.

System	Response Time Reduction (%)	Threat Detection Accuracy (%)	Overall Effectiveness (%)
Suricata [1]	40%	–	80%
HoneyMesh [2]	–	60%	75%
Google DC Agents [5]	70%	45%	85%
AWS IoT Defender [6]	35%	45%	78%
Azure Sphere [6]	–	50%	82%
Tesla FSD [6]	70%	–	88%
IBM QRadar-Watson [7]	–	60%	84%

Based on the aforementioned practical examples, the performance of Multi-Agent Systems (MAS) has been evaluated using three core indicators: response time reduction, threat detection accuracy, and overall system efficiency. Each metric was assessed independently, enabling a comparative functional profile to be constructed across different systems. Among the systems studied, Tesla FSD and Google Data Center Agents demonstrated the highest response time reductions (70%), thanks to their real-time monitoring capabilities and localized reaction mechanisms at the component level. Suricata achieved a 40% reduction, which reflects the direct traffic inspection capabilities of its distributed IDS agents. In resource-constrained IoT environments, AWS IoT Defender agents optimized response time by up to 35%. In terms of threat detection accuracy, HoneyMesh, Azure Sphere, and IBM QRadar-Watson stood out with accuracy levels between 50% and 60%.

HoneyMesh agents leveraged virtual service emulation to deceive attackers and analyze behavior with precision. In Azure Sphere and IBM's implementations, artificial intelligence and semantic analysis significantly enhanced detection capabilities–particularly through the use of AI-integrated log agents in IBM's Watson-powered system. The systems exhibiting the highest overall efficiency were: Tesla FSD (88%) – due to autonomous decision-making, inter-agent coordination, and real-time reactivity; Google Data Center Agents (85%) – leveraging independent server-level control and rapid policy enforcement; IBM QRadar-Watson (84%) – applying AI for deep semantic threat interpretation and proactive prediction. These systems derive their effectiveness from localized threat identification and isolation, parallel processing with balanced resource distribution, and seamless integration with AI modules.

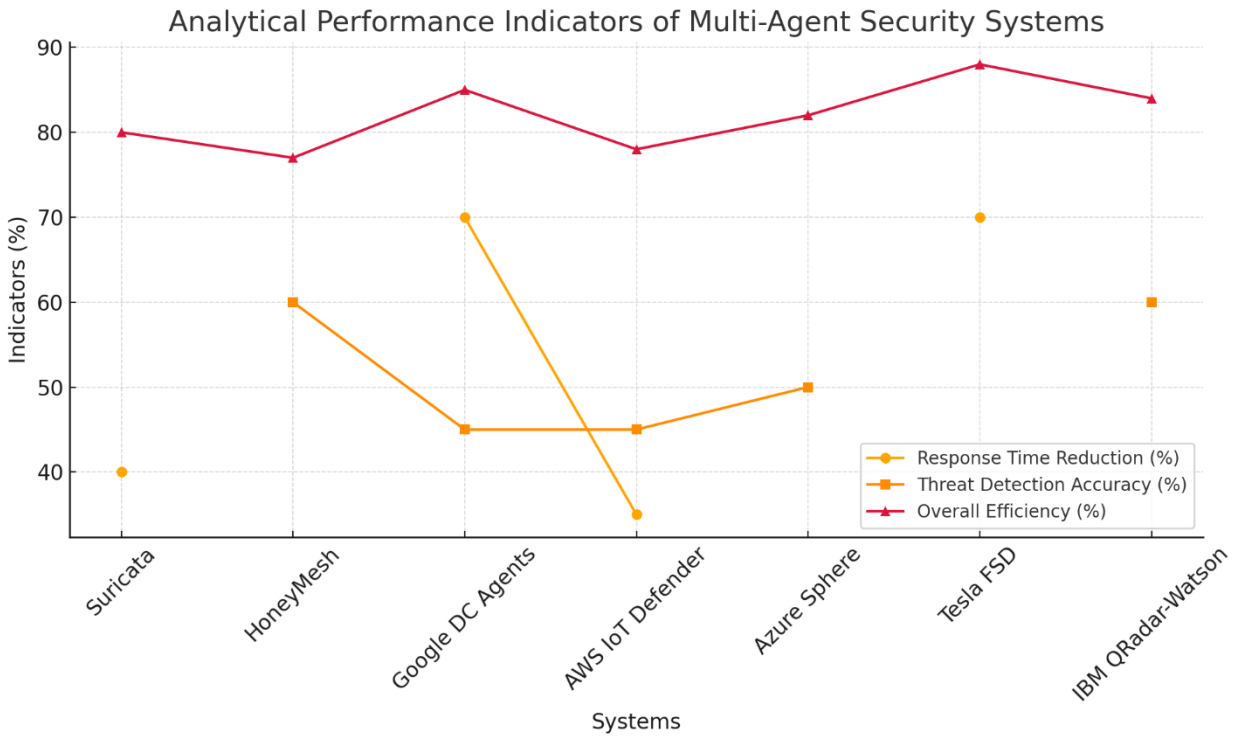


Figure 1. Analytical performance indicators of multi-agent security systems.

The ability to fully exploit MAS capabilities depends directly on the degree of inter-agent coordination. For instance, while Suricata and AWS IoT Defender excel in response time, their threat detection accuracy remains limited. Conversely, HoneyMesh and IBM QRadar-Watson demonstrate high accuracy in detection but have relatively slower response times. Hence, the ideal multi-agent security system must combine not only real-time responsiveness but also high detection accuracy, AI adaptability, and robust internal coordination. From the above analysis, it can be concluded that Multi-Agent Systems provide both technical and conceptual advantages for modern cybersecurity infrastructures. The decentralized architecture, autonomous agent operation, and cooperative decision-making mechanisms make MAS a highly effective solution for handling complex and real-time cyber threats.

The core strength of Multi-Agent Systems (MAS) lies in their ability to cooperate effectively. Each agent not only identifies threats within its operational domain but also communicates with other agents to ensure decision consistency and alignment. Particularly in dynamic and rapidly evolving threat environments, such systems can implement proactive defense models rather than merely reactive mechanisms. Alazab et al. (2020) define this capacity as “cooperative adaptive resilience,” wherein agents adaptively preserve global system security through mutual coordination. Analyses of real-world implementations demonstrate that minimizing dependency on centralized control points enhances system reliability. For instance, Tesla’s FSD architecture relies on independent agents embedded within each sensor (camera, radar, GPS), ensuring continuity of operations even if a single sensor fails.

Similarly, the Google Data Center Agents framework enables autonomous defense layers across servers, reducing the risk of systemic failure due to isolated component faults. Recent advancements have focused on AI-integrated agents, such as IBM QRadar fused with Watson and AWS IoT agents utilizing federated learning. These agents exhibit high accuracy and predictive capabilities, allowing them to detect not only existing but also previously unseen and emerging threats. As shown in the studies by Zhang et al. (2020) and Liu et al. (2023), such approaches are instrumental in achieving context-aware security, where threat understanding is based on situational analysis rather than static rules. In environments like IoT and edge computing, which are often constrained by limited power and computational capacity, federated agent architectures help overcome these limitations. Each device hosts a local agent capable of autonomous monitoring and operation without constant reliance on central servers. This enables secure operations while significantly reducing centralized system load (Wang et al., 2022).

To further enhance MAS performance, future research and development should focus on the implementation of self-learning agents capable of evolving without explicit reprogramming; real-time agent mesh networks for 6G and IoT 2.0 ecosystems; agent-to-agent authentication frameworks based on Zero-Trust Architecture; and

the integration of Explainable Artificial Intelligence (XAI) to improve trust and transparency in decision-making. From this perspective, the MAS approach is poised to become a cornerstone of cybersecurity strategies not only in traditional sectors such as IT infrastructure, but also across domains like healthcare, financial services, and industrial automation. Their distributed nature, agent autonomy, and cooperative behavior render them exceptionally well-suited for complex, real-time, and mission-critical security environments.

As the number and complexity of digital threats in information systems continue to rise, the demand for modern, flexible, and distributed security architectures is becoming increasingly critical. This study has demonstrated that Multi-Agent Security Systems (MAS) provide a strategic solution for today's digital ecosystem.

CONCLUSION AND RECOMMENDATIONS

Through the analysis of practical implementations–including Suricata, HoneyMesh, Google Data Center Agents, AWS IoT Defender, Azure Sphere, Tesla FSD, and IBM QRadar-Watson–the following key conclusions have been drawn: adaptability and resilience are achieved through the distributed nature of agents, ensuring that protection occurs at the local level rather than through centralized mechanisms, which significantly enhances system stability and fault tolerance; speed and accuracy are supported by real-time monitoring, automated analytics, and AI integration, enabling agents to detect and respond to threats rapidly and with high precision; the decentralized security model ensures that the failure of a single component does not compromise the entire system, thereby maintaining continuous availability and robustness; integration of AI and federated learning through tools such as Watson, federated agents, and deep learning models has markedly improved threat detection accuracy and predictive capabilities; and finally, the MAS approach offers a wide range of applications beyond traditional network security, including IoT environments, transportation systems, financial infrastructures, data centers, and healthcare technologies.

In conclusion, Multi-Agent Systems represent not only a technological innovation but also a strategic advancement in responding to emerging cyber threats. Their high degree of adaptability, operational reliability, and seamless integration with artificial intelligence technologies positions them as a foundational component for the next generation of cybersecurity infrastructures.

References:

1. Bozorov, S., Akhmedova, N., Qurbonaliyeva, D., & Gultekin, K. (2024). Survey on honeypot: Detection, countermeasures and future with MI. AIP Conference Proceedings.
2. Xudoyqulov, Z. T., Qurbonaliyeva, D. V., & Bozorov, S. M. (2024). Honeypot texnologiyasining funksional imkoniyatlarini tadqiq etish. Al-Farg'oniy avlodlari.
3. Kotenko, I., & Chechulin, A. (2017). Agent-based simulation of cyber-attacks and countermeasures in computer networks. Journal of Computer and Systems Sciences International, 56(3), 344–356.
4. Jennings, N. R. (2001). An agent-based approach for building complex software systems. Communications of the ACM, 44(4), 35–41.
5. Kiss, Á., Gulyás, G. G., & Imre, S. (2020). HoneyMesh: Distributed honeypot framework for Internet of Things. Computer Networks, 170, 107100.
6. Bonabeau, E., Dorigo, M., & Theraulaz, G. (1999). Swarm Intelligence: From Natural to Artificial Systems. Oxford University Press.
7. Zhang, Y., Chen, T., & Wang, X. (2021). An intelligent multi-agent system for adaptive intrusion detection in cloud environments. IEEE Transactions on Cloud Computing.
8. Rahman, M. A., Abedin, S. F., & Karim, M. R. (2022). Decentralized cybersecurity architecture using multi-agent reinforcement learning. Computers & Security, 115, 102620.
9. Chen, H., & Wang, K. (2020). Swarm intelligence driven security agents for IoT networks. Ad Hoc Networks, 104, 102150.
10. Das, A., & Sengupta, A. (2023). Federated multi-agent systems for real-time anomaly detection in 5G networks. Future Generation Computer Systems, 147, 1–12.
11. Amazon Web Services. (2018). AWS IoT Device Defender – Technical Whitepaper.
12. Microsoft Corporation. (2019). Azure Sphere Security Overview.
13. Open Information Security Foundation (OISF). (2009). Suricata: Next Generation IDS/IPS Engine.
14. IBM Corporation. (2017). IBM QRadar and Watson for Cybersecurity.
15. Mastercard AI Security Lab. (2018). AI-Driven Fraud Detection System.
16. Tesla, Inc. (2020). Full Self-Driving (FSD) System Security Architecture.
17. https://yashil-iqtisodiyot-taraqqiyot.uz/journal

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 4

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

“The journal “INNOVATION SCIENCE AND TECHNOLOGY” has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block, House 17.

TASHKENT STATE UNIVERSITY OF ECONOMICS

Google Scholar | OPEN ACCESS | ULRICHSWEB GLOBAL SERIALS DIRECTORY

Academic Resource Index ResearchBib | ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE | CYBERLENINKA

OpenAIRE | ROAD | НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА LIBRARY.RU

BASE | INDEX COPERNICUS INTERNATIONAL | Crossref

doi Digital Object Identifier | CiteFactor Academic Scientific Journals | zenodo

Acceptance of articles

Published every monthly

Directions

Social, economic, political, technological, scientific

Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

ORDER NUMBER ACCORDING TO THE LICENSE REGISTER: C-5669633

CONTACT:

Contact us
+998 97 748 70 03

Telegram channel
t.me/scopus_IST2100

Journal official website
https://ist-journal.uz/index.php/IST