ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME -10

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 10

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

RISK-AWARE MULTI-LAYERED NETWORK DEFENSE MODEL FOR PROTECTING IOT AND 5G-ENABLED DIGITAL INFRASTRUCTURES

Karimova Iqbol Madaminovna
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti Kompyuter injiniringi fakulteti Axborot xavfsizligi kafedra katta o‘qituvchisi
E-mail: karimovaiqbolatuit@gmail.com

Annotatsiya. Ushbu maqolada IoT va 5G texnologiyalari asosida ishlaydigan zamonaviy raqamli infratuzilmalarni himoyalash uchun riskga asoslangan ko‘p qatlamli tarmoq xavfsizligi modeli taklif etiladi. Bugungi kunda tarmoqlarning murakkablashuvi, qurilmalar sonining ortishi va kiberhujumlarning takomillashuvi an’anaviy himoya usullarini yetarli bo‘lmay qolishiga olib kelmoqda. Tadqiqotda firewall, Intrusion Detection and Prevention System, encryption, network segmentation va Security Operations Center komponentlari yagona himoya arxitekturasida birlashtiriladi. Taklif etilgan model tarmoq trafikini nazorat qilish, tahdidlarni real vaqt rejimida aniqlash, ma’lumotlarni shifrlash va xavf darajasiga qarab javob choralarini avtomatlashtirishga qaratilgan. Natijalar ko‘p qatlamli va riskga asoslangan yondashuv IoT va 5G muhitlarida tarmoq barqarorligini oshirishini ko‘rsatadi.

Kalit so‘zlar. Tarmoq xavfsizligi, firewall, IDPS, shifrlash, IoT xavfsizligi, 5G, risk tahlili, ko‘p qatlamli himoya, kiberbarqarorlik.

Аннотация. В данной статье предлагается риск-ориентированная многоуровневая модель сетевой защиты для современных цифровых инфраструктур, функционирующих на базе технологий IoT и 5G. Усложнение сетей, рост количества подключенных устройств и развитие кибератак приводят к тому, что традиционные методы защиты становятся недостаточными. В исследовании объединяются firewall, Intrusion Detection and Prevention System, encryption, network segmentation и Security Operations Center в единую архитектуру защиты. Предложенная модель направлена на контроль сетевого трафика, обнаружение угроз в реальном времени, шифрование данных и автоматизацию ответных мер в зависимости от уровня риска. Результаты показывают, что многоуровневый и риск-ориентированный подход повышает устойчивость сетей в IoT- и 5G-средах.

Ключевые слова. сетевая безопасность, firewall, IDPS, шифрование, безопасность IoT, 5G, анализ рисков, многоуровневая защита, киберустойчивость.

Abstract. This article proposes a risk-aware multi-layered network defense model for protecting modern digital infrastructures based on IoT and 5G technologies. The increasing complexity of networks, the rapid growth of connected devices,

ISSN 3030-3907

and the sophistication of cyberattacks make traditional security methods insufficient. The study integrates firewalls, Intrusion Detection and Prevention Systems, encryption, network segmentation, and Security Operations Center components into a unified defense architecture. The proposed model focuses on controlling network traffic, detecting threats in real time, encrypting sensitive data, and automating response actions according to risk level. The results show that a multi-layered and risk-aware approach can improve network resilience in IoT and 5G environments.

Keywords. Network security, firewall, IDPS, encryption, IoT security, 5G, risk analysis, multi-layered defense, cyber resilience

INTRODUCTION.

The rapid development of digital technologies has significantly changed the structure, scale, and complexity of modern network infrastructures. Organizations now rely on cloud services, mobile applications, Internet of Things devices, 5G communication systems, distributed platforms, and industrial control networks. These technologies improve communication speed, automation, and operational efficiency, but they also increase the number of potential attack points.

Traditional network security models often depend on isolated tools such as firewalls, antivirus systems, or basic access control mechanisms. However, modern cyber threats are more complex and adaptive. Attackers use phishing, malware, ransomware, botnets, insider access, misconfigured devices, and advanced persistent threats to bypass simple protection systems. Therefore, organizations need integrated and adaptive security architectures that can provide prevention, detection, protection, and response at the same time.

The uploaded source document emphasizes the importance of a multi-layered network defense strategy that integrates firewalls, Intrusion Detection and Prevention Systems, and encryption to counter evolving cyber threats [1]. In addition, modern 5G and beyond networks require modular and adaptive security mechanisms because their architecture is highly distributed and dynamic [2]. Automation in network security configuration is also becoming essential because manual rule management cannot respond quickly enough to rapidly changing threats [3].

The relevance of this study is especially high for IoT and 5G-enabled infrastructures. IoT devices are often resource-constrained and may have weak built-in security, while 5G networks support massive connectivity and low-latency communication. These features make such environments attractive targets for cybercriminals.

The main purpose of this article is to propose a risk-aware multi-layered network defense model that combines firewalls, IDPS, encryption, segmentation,

ISSN 3030-3907

and Security Operations Center monitoring into a unified cybersecurity framework. The scientific novelty of the article is the use of a risk-based decision mechanism that evaluates threat severity, vulnerability level, asset value, detection confidence, and potential impact before selecting the appropriate response action.

LITERATURE REVIEW.

Network security is a collection of technologies, policies, and processes designed to protect digital systems from unauthorized access, misuse, disruption, and data theft. The source article defines network security as a layered approach that protects data and systems through firewalls, intrusion detection systems, encryption protocols, user education, and continuous monitoring.

Firewalls are one of the most important components of network defense. They filter incoming and outgoing traffic according to predefined security rules. Hardware firewalls provide centralized protection for organizational networks, while software firewalls offer device-level control. Next-Generation Firewalls extend traditional firewall functions by adding application-level filtering, deep packet inspection, and intrusion prevention capabilities. Modern network management studies also show that artificial intelligence, automation, and security integration can improve the effectiveness of firewall configuration and monitoring.

Intrusion Detection and Prevention Systems play a critical role in identifying suspicious behavior. Network-based IDS monitors' traffic across network segments, while host-based IDS analyzes local system activity. IDPS tools can detect anomalies, generate alerts, and automatically block malicious traffic. Their role is especially important in IoT and 5G environments, where many devices continuously exchange data. Research on NIDS and NIPS also confirms that intrusion detection and prevention mechanisms are necessary for protecting internet infrastructure against large-scale attacks [4].

Encryption is another essential layer of network security. It converts readable data into unreadable cipher text, preventing unauthorized access during transmission or storage. Symmetric encryption is fast and suitable for large amounts of data, while asymmetric encryption supports secure key exchange and digital signatures. Hybrid encryption combines both methods to achieve a balance between performance and security [5]. Cryptographic and detection-based techniques are also important for maintaining data integrity in distributed networks [6].

Security Operations Centers provide centralized monitoring, analysis, and response. A SOC combines people, processes, and technologies to detect threats, investigate incidents, and coordinate response actions. SOC-based monitoring is

ISSN 3030-3907

important because technical tools alone are not enough; effective cybersecurity also requires trained personnel, incident handling procedures, and continuous improvement of defense strategies [7].

IoT, 5G, and edge computing environments create new cybersecurity challenges because they increase the number of connected devices and expand the attack surface. In IoT-based supply chain and control systems, connected devices can improve automation and monitoring, but they also introduce new cyber risks that require continuous protection and risk assessment [8]. Edge computing environments require special attention because data processing is moved closer to end devices, which improves latency but creates additional security and privacy requirements [9].

Previous research on advanced network security strategies also emphasizes the importance of combining firewalls, intrusion detection systems, encryption, access control, artificial intelligence, cloud security, and proactive monitoring into a unified cybersecurity framework [10]. Therefore, modern cybersecurity requires a coordinated architecture rather than isolated protection tools.

Table 1

Main security mechanisms in multi-layered network defense

Security component	Main function	Advantage	Limitation
Firewall	Filters network traffic	Blocks unauthorized access	Limited against internal attacks
IDPS	Detects and prevents intrusions	Real-time monitoring and response	May generate false positives
Encryption	Protects data confidentiality	Secures data in transit and at rest	Requires key management
Network segmentation	Separates network zones	Limits attack spread	Requires careful design
SOC	Centralized monitoring	Improves incident response	Requires skilled personnel

RESEARCH METHODOLOGY.

The methodology of this study is based on structural modeling and risk-aware analysis of network security components. The proposed model integrates five security layers: perimeter filtering, intrusion detection and prevention, encryption, segmentation, and automated response.

ISSN 3030-3907

The first layer is the traffic control layer. This layer uses firewalls and Next-Generation Firewalls to inspect and filter incoming and outgoing traffic. It blocks unauthorized connections and applies policy-based access control. This layer is important because firewalls remain the first line of defense in many network environments.

The second layer is the threat detection layer. This layer uses IDPS tools to analyze traffic patterns, detect anomalies, and identify known attack signatures. IDPS can operate using signature-based, anomaly-based, and behavioral detection methods. This layer is necessary because advanced attacks may bypass firewall rules and appear as legitimate traffic.

The third layer is the data protection layer. This layer applies hybrid encryption to protect sensitive information. Symmetric encryption is used for fast data transfer, while asymmetric encryption is used for secure key exchange. This approach supports both efficiency and confidentiality in modern communication systems.

The fourth layer is the segmentation layer. This layer divides the network into smaller zones, such as IoT zone, user zone, server zone, and administrative zone. If one segment is compromised, the attacker cannot easily move across the entire infrastructure. This is especially useful for IoT and 5G environments where device diversity is high.

The fifth layer is the response layer. This layer uses automated incident response mechanisms to block suspicious traffic, isolate compromised devices, update firewall rules, and notify the Security Operations Center. Automation helps reduce response time and supports proactive defense.

Mathematical risk model

The total risk score of a network event is calculated as follows:

$$R = \alpha T + \beta V + \delta D + \lambda C$$

where:

R

is the total risk score;

T

is the threat severity level;

V

is the vulnerability level of the affected system;

A

is the asset value;

D

is the detection confidence score;

ISSN 3030-3907

C

is the potential impact on confidentiality, integrity, and availability;

$\alpha,\beta,\gamma,\delta,\lambda$

are weight coefficients.

The response decision is determined by the following rule:

$$Response = \begin{cases} Monitor, & R < \theta_1 \\ Alert, & \theta_1 \leq R < \theta_2 \\ Block, & \theta_2 \leq R < \theta_3 \\ Isolate, & R \geq \theta_3 \end{cases}$$

where:

$\theta_1, \theta_2, \theta_3$

are predefined response thresholds.

This model allows the security system to respond according to the actual level of risk. Low-risk events are monitored, medium-risk events generate alerts, high-risk events are blocked, and critical events trigger device or segment isolation.

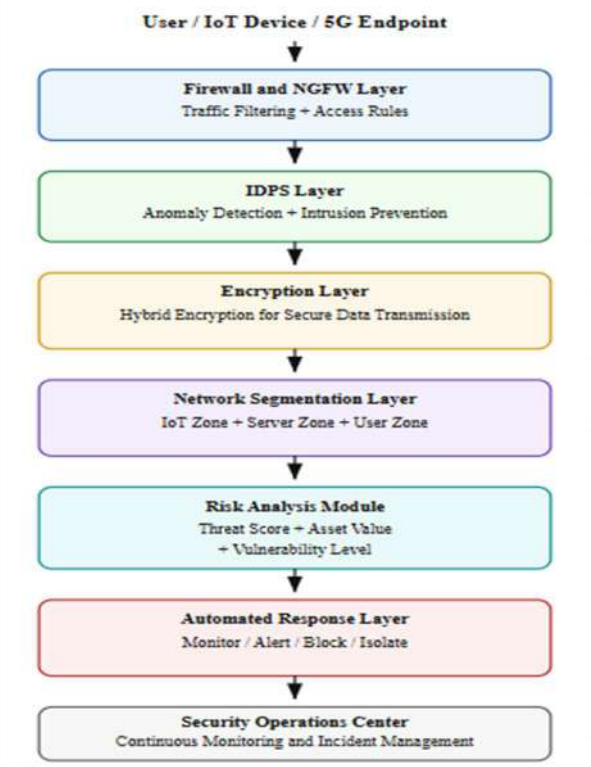


Figure 1. Architecture of the risk-aware multi-layered network defense model [1].

The figure illustrates the proposed defense architecture. First, traffic from users, IoT devices, and 5G endpoints passes through firewall and NGFW filtering. Then, IDPS analyzes suspicious activity and prevents attacks. Encryption protects transmitted data, while segmentation limits lateral movement. The risk analysis module calculates the threat level, and the automated response layer selects the

ISSN 3030-3907

appropriate action. Finally, the SOC monitors incidents and supports long-term network resilience.

RESULTS AND DISCUSSION.

The proposed model improves network defense by combining prevention, detection, protection, and response mechanisms into one coordinated architecture. Compared with traditional isolated tools, the model provides stronger resilience because every security layer supports the others.

The firewall layer reduces exposure by filtering unauthorized traffic. This is especially important for IoT and 5G networks, where many devices communicate simultaneously. However, firewalls alone are not enough because attackers may use legitimate ports, stolen credentials, or encrypted channels. Therefore, IDPS, encryption, segmentation, and continuous monitoring must support firewall protection.

The IDPS layer strengthens protection by detecting suspicious behavior that may bypass the firewall. It can identify unusual traffic volumes, malware communication, scanning attempts, and policy violations. When connected to the risk analysis module, IDPS alerts become more useful because the system can prioritize serious threats and reduce unnecessary alerts.

The encryption layer ensures that data remains confidential even if traffic is intercepted. Hybrid encryption is suitable for modern networks because it combines the speed of symmetric encryption with the secure key distribution advantages of asymmetric encryption. This is particularly important for cloud, edge, and IoT systems where sensitive data is transmitted between many different devices.

The segmentation layer limits the spread of attacks. For example, if an IoT device is compromised, the attacker cannot easily access database servers or administrative systems. This is important because IoT devices often have weaker built-in security than traditional computing systems.

The SOC layer ensures that detected incidents are monitored, analyzed, documented, and resolved. A mature SOC can improve response coordination by combining technical alerts with human expertise and operational procedures. When automation is integrated with SOC processes, the response time can be reduced and repeated tasks can be handled more efficiently.

Table 2

Expected impact of the proposed model

Evaluation criterion	Traditional defense	Proposed risk-aware model

ISSN 3030-3907

Traffic filtering	Static firewall rules	Adaptive firewall and NGFW rules
Threat detection	Basic IDS alerts	IDPS with risk-based prioritization
Data protection	Optional encryption	Mandatory hybrid encryption
Attack containment	Limited	Network segmentation
Incident response	Manual	Automated monitor, alert, block, isolate
SOC integration	Partial	Continuous centralized monitoring
Suitability for IoT/5G	Medium	High

The main advantage of the proposed model is risk awareness. Instead of treating all alerts equally, the system calculates a risk score by considering threat severity, asset value, vulnerability level, detection confidence, and potential impact. This improves decision-making and helps security teams focus on the most dangerous incidents.

The model also supports proactive defense. Regular updates, firewall audits, IDPS tuning, encryption key management, user education, and SOC monitoring remain important. The source document emphasizes that proactive and adaptive cybersecurity practices are necessary to maintain resilience against evolving threats. Similar conclusions are also supported by studies on network security best practices and advanced security strategies.

However, implementation challenges remain. First, integrating several security technologies may increase system complexity. Second, IDPS tuning requires high-quality traffic data. Third, encryption key management must be carefully designed. Fourth, SOC operations require trained specialists and continuous monitoring. Fifth, IoT and edge environments may have limited processing and memory resources, which requires lightweight and optimized security mechanisms.

ISSN 3030-3907

Despite these challenges, the proposed model is suitable for organizations that operate distributed networks, IoT environments, cloud platforms, 5G infrastructures, and industrial control systems.

CONCLUSION AND RECOMMENDATIONS.

This article proposed a risk-aware multi-layered network defense model for protecting IoT and 5G-enabled digital infrastructures. The model was developed based on the ideas of multi-layered network defense, firewalls, IDPS, encryption, proactive defense, and cyber resilience discussed in the uploaded source document.

The study showed that modern networks require integrated security architectures rather than isolated tools. Firewalls provide traffic filtering, IDPS detects and prevents threats, encryption protects data, segmentation limits attack movement, and SOC ensures continuous monitoring and incident management.

The proposed mathematical model allows the system to calculate risk scores and select response actions according to threat severity. This approach improves response efficiency and reduces the impact of cyber incidents. In addition, the model supports IoT and 5G security by combining adaptive traffic filtering, real-time detection, hybrid encryption, segmentation, and automated incident response.

It is recommended that organizations implement multi-layered defense gradually. First, they should deploy properly configured firewalls and NGFWs. Second, they should integrate IDPS with real-time monitoring. Third, they should apply hybrid encryption for sensitive data. Fourth, they should segment IoT, user, and server zones. Fifth, they should establish SOC-based incident response processes. Sixth, they should regularly assess risks and update security policies according to new threats.

Future research should focus on testing the model in real IoT and 5G environments, applying machine learning for risk scoring;optimizing encryption for resource-constrained devices, and integrating automated response mechanisms with SOC platforms.

REFERENCES

1. I. M. Karimova, “Multi-layered network defense: Integrating firewalls, IDPS, and encryption to counter evolving cyber threats,” submitted manuscript, Information Security Department, Urgench State University named after Abu Rayhan Biruni, Urgench, Uzbekistan, 2025.
2. M. A. Anderson, M. E. Ahmed, E. E. El-Sayed, and A. Arora, “An introduction of a modular framework for securing 5G networks and beyond,” MDPI, 2022.
3. B. Davis, F. Vega, G. Moreno, and R. Smith, “Automation for network security configuration: State of the art and research trends,” ACM, 2024.

ISSN 3030-3907

4. J. Doe and Y. Evans, “The Critical Role of NIDS/NIPS in Protecting Internet Infrastructure,” SCHOLINK INC., 2023.
5. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
6. G. M. Hughes, “Exploring Secure Methods for Ensuring Data Integrity: A Theoretical Analysis of Cryptographic and Detection Techniques,” CSUSB ScholarWorks, 2025.
7. E. Carson, “Process, Technology and Human Aspects of a Security Operations Center,” Middle East Technical University, Faculty of Architecture, 2024.
8. A. Zhang, “Industry Briefing: IoT in the Supply Chain and Control Systems Sector,” PETRAS National Centre of Excellence for IoT Systems Cybersecurity, 2021.
9. H. Abdullah, T. S. Ishikawa, M. Y. Ibrahim, and others, “Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities,” IEEE, 2020.
10. M. M. Karimov, I. M. Karimova, and T. T. Turdiyev, “Advanced Strategies for Network Security: Ensuring Resilience in a Digital World,” 2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM), pp. 2040–2044, 2025, doi: 10.1109/EDM65517.2025.11096644.

ISSN 3030-3907