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

# AN ADAPTIVE ZERO TRUST-BASED NETWORK SECURITY MODEL FOR CYBER-RESILIENT 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 zamonaviy raqamli infratuzilmalarda kiberxavfsizlikni ta’minlash uchun Zero Trust tamoyillariga asoslangan adaptiv tarmoq xavfsizligi modeli taklif etiladi. Bugungi kunda bulutli hisoblash, IoT qurilmalari, edge computing va taqsimlangan tarmoqlarning kengayishi an’anaviy xavfsizlik yondashuvlarini yetarli bo‘lmay qolishiga olib kelmoqda. Tadqiqotda firewall, intrusion detection system, shifrlash, multi-factor authentication, role-based access control va sun’iy intellekt asosidagi tahdidlarni aniqlash mexanizmlari yagona modelda birlashtiriladi. Taklif etilgan model har bir foydalanuvchi, qurilma va so‘rovni doimiy tekshirish orqali tarmoq barqarorligini oshirishga qaratilgan. Natijalar adaptiv, ko‘p qatlamli va Zero Trust asosidagi yondashuv tarmoq hujumlariga qarshi samarali himoya yaratishini ko‘rsatadi.

**Kalit so‘zlar.** tarmoq xavfsizligi, Zero Trust, firewall, IDS, sun’iy intellekt, shifrlash, MFA, access control, IoT xavfsizligi, kiberbarqarorlik.

**Аннотация**. В данной статье предлагается адаптивная модель сетевой безопасности, основанная на принципах Zero Trust, для обеспечения киберустойчивости современных цифровых инфраструктур. Расширение облачных вычислений, IoT-устройств, edge computing и распределенных сетей приводит к тому, что традиционные подходы к безопасности становятся недостаточными. В исследовании объединяются firewall, intrusion detection system, шифрование, multi-factor authentication, role-based access control и механизмы обнаружения угроз на основе искусственного интеллекта в единую модель. Предложенная модель направлена на повышение устойчивости сети за счет постоянной проверки каждого пользователя, устройства и запроса. Результаты показывают, что адаптивный многоуровневый подход на основе Zero Trust обеспечивает эффективную защиту от сетевых атак.

**Ключевые слова.** сетевая безопасность, Zero Trust, firewall, IDS, искусственный интеллект, шифрование, MFA, контроль доступа, безопасность IoT, киберустойчивость.

**Abstract**. This article proposes an adaptive Zero Trust-based network security model for ensuring cyber resilience in modern digital infrastructures. The rapid expansion of cloud computing, Internet of Things devices, edge computing, and distributed networks makes traditional perimeter-based security approaches

insufficient. The study integrates firewalls, intrusion detection systems, encryption, multi-factor authentication, role-based access control, and artificial intelligence-driven threat detection into a unified framework. The proposed model aims to improve network resilience by continuously verifying every user, device, and access request. The results show that an adaptive, multi-layered, and Zero Trust-based approach can provide effective protection against evolving network attacks.

**Keywords**. network security, Zero Trust, firewall, IDS, artificial intelligence, encryption, MFA, access control, IoT security, cyber resilience.

## INTRODUCTION.

The rapid digitalization of modern society has increased the importance of network security for organizations, governments, financial institutions, healthcare systems, and individual users. Digital infrastructures now rely on cloud platforms, Internet of Things devices, edge computing, mobile applications, and distributed communication systems. These technologies improve efficiency and connectivity, but they also expand the attack surface and create new cybersecurity risks [1].

Traditional network security models were mainly based on perimeter protection. In this approach, users and devices inside the network were often considered trusted, while external traffic was treated as suspicious. However, this model is no longer sufficient because modern attacks can originate both outside and inside the network. Compromised user accounts, infected IoT devices, insider threats, misconfigured cloud services, and advanced persistent threats can bypass traditional perimeter defenses.

The uploaded IEEE article emphasizes that modern network security requires a comprehensive strategy combining preventive measures, detection mechanisms, response processes, firewalls, intrusion detection systems, encryption, access control, multi-factor authentication, Zero Trust Architecture, artificial intelligence, blockchain, cloud security, and IoT protection. This article continues that research direction by proposing a new adaptive Zero Trust-based network security model.

The main purpose of this study is to develop a multi-layered network security model that continuously evaluates users, devices, traffic behavior, and contextual risk factors before granting access to digital resources. The scientific novelty of the article is the integration of adaptive firewall rules, AI-based IDS, hybrid encryption, MFA, RBAC, and automated incident response into a unified Zero Trust architecture.

## LITERATURE REVIEW.

Network security is a broad field that includes technologies, policies, and practices designed to protect networks from unauthorized access, misuse, data


ISSN 3030-3907

leakage, and service disruption. The source article defines network security as a multi-layered defense mechanism that protects both hardware and software components and ensures confidentiality, integrity, and availability of data.

Firewalls are one of the oldest and most important components of network defense. They control incoming and outgoing traffic according to predefined security rules. Modern next-generation firewalls can perform deep packet inspection, application-level filtering, and dynamic rule enforcement. However, firewalls alone cannot detect all types of advanced attacks, especially those that use legitimate credentials or encrypted channels [2].

Intrusion Detection Systems are used to monitor network traffic and identify suspicious behavior. Network-based IDS analyzes packets across network segments, while host-based IDS monitors logs and system activities on individual devices. Recent research has shown that machine learning can improve IDS accuracy by detecting unknown attacks and reducing false positives [3], [4].

Encryption techniques are essential for protecting data confidentiality and integrity. Symmetric encryption provides high speed, while asymmetric encryption improves key distribution security. Hybrid encryption combines the advantages of both methods and is widely used in secure communication systems [5]. In cloud and IoT environments, encryption must also be optimized for performance, latency, and resource consumption.

Authentication and access control are also central to network security. Password-based authentication is still widely used, but it is vulnerable to phishing, credential theft, and brute-force attacks. Multi-factor authentication improves security by requiring several verification factors, such as password, token, biometric data, or device identity. Access control models such as Role-Based Access Control and Discretionary Access Control are used to regulate user permissions [6].

Zero Trust Architecture has become an important security paradigm for modern networks. Its main principle is “never trust, always verify.” In a Zero Trust model, every request must be authenticated, authorized, and continuously evaluated regardless of whether it comes from inside or outside the network. This approach is especially useful for cloud computing, IoT ecosystems, remote work environments, and critical infrastructure [7].

The literature shows that isolated security tools are not enough to protect modern distributed networks. Therefore, an integrated model is required. Such a model should combine prevention, detection, encryption, authentication, access control, monitoring, and automated response mechanisms.


ISSN 3030-3907

Table 1

**Main network security components and their functions**

| Component | Main function | Advantage | Limitation |
|---|---|---|---|
| Firewall | Filters network traffic | Prevents unauthorized access | Limited against insider threats |
| IDS | Detects suspicious activity | Identifies known and unknown attacks | May generate false positives |
| Encryption | Protects data confidentiality | Secures data in transit and at rest | Requires key management |
| MFA | Verifies user identity | Reduces credential-based attacks | May affect usability |
| RBAC | Controls user permissions | Simplifies access management | Less flexible for dynamic systems |
| Zero Trust | Continuous verification | Strong adaptive protection | Requires complex implementation |

## RESEARCH METHODOLOGY.

The methodology of this study is based on structural modeling and comparative analysis of modern network security mechanisms. The proposed model integrates several security layers into one adaptive Zero Trust framework. The model consists of five main layers:

1. Identity verification layer

This layer verifies users and devices using multi-factor authentication, device fingerprinting, and behavioral context.

2. Access control layer

This layer uses role-based and context-aware access control to define permissions according to user role, device status, location, and risk level.

3. Network protection layer

This layer includes adaptive firewalls and segmentation mechanisms. It blocks unauthorized traffic and isolates suspicious devices.

4. Threat detection layer

This layer uses IDS and artificial intelligence-based anomaly detection to identify suspicious traffic patterns.

5. Incident response layer


ISSN 3030-3907

This layer automatically responds to detected threats by blocking sessions, isolating devices, updating firewall rules, and sending alerts to administrators.

Mathematical model

The risk score of each access request can be calculated as follows:

$$R = \omega_1 I + \omega_2 D + \omega_3 B + \omega_4 L + \omega_5 T$$

where:

$R$

is the total risk score;

$I$

is the identity risk factor;

$D$

is the device trust factor;

$B$

is the behavioral anomaly factor;

$L$

is the location-based risk factor;

$T$

is the traffic anomaly factor;

$\omega_1, \omega_2, \omega_3, \omega_4, \omega_5$

are weight coefficients.

The access decision is made according to the following rule:

$$A = \begin{cases} Allow, & R < \theta_1 \\ Verify, & \theta_1 \leq R < \theta_2 \\ Block, & R \geq \theta_2 \end{cases}$$

where:

$A$

is the access decision;

$\theta_1$

is the verification threshold;

$\theta_2$

is the blocking threshold.

This formula allows the system to make adaptive security decisions. If the risk score is low, access is allowed. If the risk score is medium, additional verification is required. If the risk score is high, the request is blocked.


ISSN 3030-3907

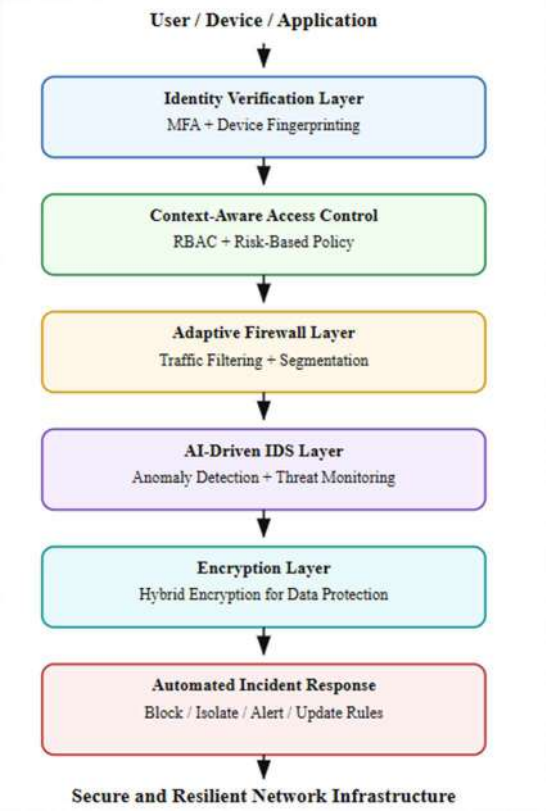



**Figure 1. Architecture of the adaptive Zero Trust-based network security model [1].**

The figure illustrates the proposed multi-layered security workflow. First, the system verifies the identity of the user and device. Then, access control policies evaluate the request according to role and risk level. After that, the adaptive firewall filters network traffic, while the AI-driven IDS monitors suspicious behavior. Encryption protects data during transmission and storage. Finally, the incident response module blocks, isolates, or reports malicious activity.

## RESULTS AND DISCUSSION.

The proposed model improves network security by combining several protection mechanisms into one coordinated architecture. Unlike traditional perimeter-based systems, the Zero Trust model does not automatically trust internal users or devices. Every access request is evaluated continuously.

The first advantage of the model is stronger identity protection. Multi-factor authentication reduces risks related to stolen passwords and phishing attacks. When combined with device fingerprinting and behavioral analysis, MFA becomes more effective because the system can detect abnormal login attempts.

The second advantage is adaptive traffic control. Firewalls are no longer limited to static rules. In the proposed model, firewall rules can be updated dynamically according to IDS alerts and risk scores. This improves response speed and reduces the time between threat detection and threat containment.


ISSN 3030-3907

The third advantage is intelligent threat detection. AI-driven IDS can analyze traffic patterns and detect anomalies that may not match known attack signatures. This is useful for identifying zero-day attacks, insider threats, and multi-stage attacks. The source article also highlights the importance of machine learning in improving intrusion detection accuracy.

The fourth advantage is improved data protection. Hybrid encryption ensures confidentiality and integrity of transmitted data. This is important for cloud platforms, IoT communication, healthcare systems, e-commerce, and financial services.

**Table 2**

**Comparison between traditional security and proposed Zero Trust model**

| Criterion | Traditional network security | Proposed adaptive Zero Trust model |
|---|---|---|
| Trust principle | Internal network is trusted | No user or device is trusted by default |
| Access control | Static permissions | Context-aware and risk-based permissions |
| Firewall operation | Predefined rules | Adaptive rule updates |
| Threat detection | Signature-based IDS | AI-assisted anomaly detection |
| Authentication | Password or 2FA | MFA + device and behavior analysis |
| Incident response | Mostly manual | Automated block, isolate, and alert actions |
| Suitability for IoT/cloud | Limited | High |


ISSN 3030-3907

The proposed model is especially useful for distributed environments. In IoT networks, many devices have limited computing power and weak built-in security. In cloud environments, workloads move dynamically between different servers and regions. In such conditions, a static security perimeter is ineffective. Adaptive Zero Trust control can provide continuous verification and segmentation.

However, the model also has several implementation challenges. First, collecting and analyzing contextual data may increase system complexity. Second, AI-driven IDS requires high-quality training data. Third, excessive verification may reduce user convenience. Fourth, automated incident response must be carefully configured to avoid blocking legitimate activity.

Despite these challenges, the proposed model provides a practical direction for improving cyber resilience. It combines prevention, detection, protection, authentication, and response mechanisms in one coordinated architecture.

**CONCLUSION AND RECOMMENDATIONS.**

This article proposed an adaptive Zero Trust-based network security model for cyber-resilient digital infrastructures. The model was developed based on the ideas of multi-layered network security, firewall protection, IDS monitoring, encryption, MFA, access control, artificial intelligence, and Zero Trust Architecture discussed in the uploaded source article.

The study showed that traditional perimeter-based security is no longer sufficient for modern cloud, IoT, edge computing, and distributed network environments. A more effective approach requires continuous verification of users, devices, access requests, traffic behavior, and contextual risk factors.

The proposed model integrates identity verification, context-aware access control, adaptive firewall rules, AI-driven IDS, hybrid encryption, and automated incident response. This layered architecture improves confidentiality, integrity, availability, and resilience against advanced cyber threats.

It is recommended that organizations implement Zero Trust gradually. First, they should identify critical assets and users. Second, they should deploy MFA and role-based access control. Third, they should integrate IDS with firewall systems. Fourth, they should use encryption for sensitive data. Fifth, they should introduce automated response mechanisms and continuous monitoring.

Future research should focus on experimental implementation of the proposed model in cloud-IoT environments, optimization of AI-based anomaly detection, development of lightweight Zero Trust mechanisms for IoT devices, and integration of blockchain-based audit logs for incident traceability.


ISSN 3030-3907

## REFERENCES

1. 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.
2. P. Prandini and M. Ramilli, “Knowledge is power: Social engineering in cyber security,” in Computer and Information Security Handbook, 3rd ed., Elsevier, pp. 427–440, 2017.
3. K. H. M. Al-Baldawi, M. Ghani, and S. A. Aljunid, “Machine learning approaches for intrusion detection: A review,” International Journal of Engineering and Technology, vol. 7, no. 4, pp. 437–441, 2018.
4. T. T. Di, P. Ning, P. M. Le, and Y. Du, “Specification-based intrusion detection for the industrial Internet of Things,” Proceedings of IEEE Conference on Communications and Network Security, pp. 9–16, 2017.
5. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
6. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.


ISSN 3030-3907