ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2025 (24) 4

қазан- желтоқсан

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).
Қазақстан Республикасы Ақпарат және қоғамдық даму министрлігіне мерзімді баспасөз басылымын есепке қою туралы куәлік № KZ82VPY00020475, 20.02.2020 ж. берілген
Тақырып бағыты: ақпараттық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология.
Мерзімділігі: жылына 4 рет.
Тираж: 100 дана.
Редакция мекенжайы: 050040 Алматы қ., Манас к., 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz
Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 6. Is.4. Number 24 (2025). Pp. 78–93
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2025.24.4.005

UDC 004.056.5

MECHANISMS FOR INTERACTION BETWEEN DISTRIBUTED IDPS AND SOC IN IOT-BASED SMART CITY INFRASTRUCTURES

T. Babenko , D. Yeskendirova , Ye. Bakhtiyarova*, K. Sansyzbay
International Information Technology University, Almaty, Kazakhstan.
E-mail: y.bakhtiyarova@iitu.edu.kz

Babenko Tatiana — Doctor of Technical Sciences, Professor, Department of Cybersecurity, International University of Information Technologies, Almaty Kazakhstan
https://orcid.org/0000-0003-1184-9483;
Yeskendirova Damelya — Candidate of Technical Sciences, Head of the Department of Cybersecurity, International University of Information Technologies, Almaty Kazakhstan
https://orcid.org/0000-0003-4270-1908;
Bakhtiyarova Yelena — Candidate of Technical Sciences, Associate Professor, Head of the Department of Radio Engineering, Electronics, and Telecommunications, International University of Information Technologies, Almaty Kazakhstan
E-mail: y.bakhtiyarova@iitu.edu.kz, https://orcid.org/0000-0001-8735-7683;
Sansyzbay Kanibek — PhD, Associate Professor, Research Professor, Department of Cybersecurity, International University of Information Technologies, Almaty Kazakhstan
https://orcid.org/0000-0002-3333-5830.

Abstract. The rapid expansion of Internet of Things networks in smart city environments creates fragmented attack surfaces that conventional security architectures cannot adequately monitor. Current Intrusion Detection and Prevention Systems operate in isolation, producing inconsistent alert formats that reach Security Operation Centers with substantial delays and poor normalization, which severely hampers correlation effectiveness and generates excessive false positives. This study develops and validates a vendor-neutral mechanism enabling standardized real-time communication between distributed IDPS sensors and centralized SOC platforms. Our methodology combines analytical review of standards including STIX, TAXII, and ISO/IEC 27001 with prototype implementation using Suricata and Zeek sensors, Apache

Kafka message bus, and Elastic SIEM integration. A custom normalization microservice converts heterogeneous alerts into STIX-compliant JSON format while maintaining GDPR and ISO 27001 compliance through TLS 1.3 encryption. Experimental validation with BoT-IoT and TON_IoT datasets shows the architecture reduces alert correlation latency by approximately 28 percent and decreases false positive rates by roughly 30 percent compared to baseline approaches. The bidirectional feedback mechanism allows SOC analysts to propagate updated detection rules to edge sensors, enabling adaptive threat response. Results demonstrate that message-bus-mediated architectures effectively address interoperability challenges in heterogeneous IoT security infrastructures, offering a practical implementation pathway for national smart city cybersecurity frameworks.

Keywords: smart city security, intrusion detection systems, security operation center, IDPS-SOC integration, IoT cybersecurity, STIX protocol, alert normalization, distributed security architecture, real-time threat correlation, Apache Kafka

For citation: Babenko T., Yeskendirova D., Bakhtiyarova Ye., K. Sansyzbay. Mechanisms for interaction between distributed idps and soc in iot-based smart city infrastructures// International journal of information and communication technologies. 2025. Vol. 6. No. 24. Pp. 78–93. (In Eng.). https://doi.org/10.54309/IJICT.2025.24.4.005.

Conflict of interest: The authors declare that there is no conflict of interest.

IoT-НЕГІЗГІ SMART SITY ИНФРАҚҰРЫЛЫМЫНДАҒЫ ТАРТЫЛҒАН IDPS-ПЕН ӘЛЕУМЕТТІК ОРЫНДАРЫНЫҢ ӨЗАРА ӘСЕРІСІ МЕХАНИЗМІ

Т. Бабенко, Д. Ескендирова, Е. Бахтиярова*, К.М. Сансызбай
Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан.
E-mail: y.bakhtiyarova@iitu.edu.kz

Бабенко Татьяна Василевна — т.ғ.д., «Киберқауіпсіздік» кафедрасының профессоры Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
https://orcid.org/0000-0003-1184-9483;
Ескендирова Дамеля Максутовна — т.ғ.к, «Киберқауіпсіздік» кафедрасының меңгерушісі Халықаралық ақпараттық технологиялар университеті,Алматы, Қазақстанhttps://orcid.org/0000-0003-4270-1908;
Бахтиярова Елена Ажибековна — т.ғ.к, қауымдастырылған профессор «Радиотехника электроника және телекоммуникациялар» кафедрасының меңгерушісі, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
E-mail: y.bakhtiyarova@iitu.edu.kz, https://orcid.org/0000-0001-8735-7683;
Сансызбай Қанибек Мұратбекұлы — PhD, қауымдастырылған профессор

«Киберқауіпсіздік» кафедрасының профессор-зерттеушісі Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
https://orcid.org/0000-0002-3333-5830.

Аннотация. Ақылды қала орталарында Интернет желісінің жылдам кеңеюі кәдімгі қауіпсіздік архитектуралары тиісті түрде бақылай алмайтын бөлшектелген шабуыл беттерін жасайды. Ағымдағы шабуылды анықтау және алдын алу жүйелері оқшауланған түрде жұмыс істейді, олар елеулі кідірістермен және нашар қалыпқа келтірумен Қауіпсіздік операциялық орталықтарына жететін сәйкес келмейтін ескерту пішімдерін шығарады, бұл корреляцияның тиімділігіне қатты кедергі келтіреді және шамадан тыс жалған позитивтерді тудырады. Бұл зерттеу таратылған IDPS сенсорлары мен орталықтандырылған SOC платформалары арасында стандартталған нақты уақыттағы байланысты қамтамасыз ететін сатушыға бейтарап механизмді әзірлейді және растайды. Біздің әдістеме стандарттарға аналитикалық шолуды, соның ішінде STIX, TAXII және ISO/IEC 27001, Suricata және Zeek сенсорлары, Apache Kafka хабар шинасы және Elastic SIEM интеграциясы арқылы прототипті енгізумен біріктіреді. Пайдаланушы қалыпқа келтіру микросервисі TLS 1.3 шифрлау арқылы GDPR және ISO 27001 сәйкестігін сақтай отырып, біркелкі емес ескертулерді STIX-үйлесімді JSON пішіміне түрлендіреді. BoT-IoT және TON_IoT деректер жинақтарымен тәжірибелік тексеру сәулет ескерту корреляциясының кідірісін шамамен 28 пайызға азайтатынын және бастапқы тәсілдермен салыстырғанда жалған оң көрсеткіштерді шамамен 30 пайызға төмендететінін көрсетеді. Екі жақты кері байланыс механизмі SOC талдаушыларына қауіп-қатерге бейімделу реакциясын қоса отырып, жаңартылған анықтау ережелерін шеткі сенсорларға таратуға мүмкіндік береді. Нәтижелер хабарламалар шинасы арқылы жүзеге асырылатын архитектуралар ұлттық смарт қала киберқауіпсіздік құрылымдары үшін практикалық іске асыру жолын ұсына отырып, IoT қауіпсіздігінің гетерогенді инфрақұрылымдарында өзара әрекеттесу мәселелерін тиімді шешетінін көрсетеді.

Түйін сөздер: ақылды қала қауіпсіздігі, шабуылды анықтау жүйелері, қауіпсіздік операциялық орталығы, IDPS-SOC интеграциясы, IoT киберқауіпсіздігі, STIX протоколы, ескертулерді қалыпқа келтіру, таратылған қауіпсіздік архитектурасы, нақты уақыттағы қауіп корреляциясы, Apache Kafka

Дәйексөздер үшін: А Т. Бабенко, Д. Ескендирова, Е. Бахтиярова, К. Сансызбай. IoT - негізгі smart sity инфрақұрылымындағы тартылған idps-пен әлеуметтік орындарының өзара әсерісі механизмі // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. 2025. Том. 6. № 24. 78–93 бет. (Ағыл). https://doi.org/10.54309/IJICT.2025.24.4.005.

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді

МЕХАНИЗМЫ ВЗАИМОДЕЙСВИЯ МЕЖДУ РАСПРЕДЕЛЕННЫМИ IDPS И SOCВ ИНФРАСТРУКТУРАХ УМНЫХ ГОРОДОВ НА ОСНОВЕ IOT

Т.В. Бабенко, Д.М. Ескендирова, Е.А. Бахтиярова, Қ.М. Сансызбай
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: y.bakhtiyarova@iitu.edu.kz

Бабенко Татьяна Василевна — д.т.н., профессор кафедры «Кибербезопасность», Международный университет информационных технологий, Алматы, Казахстан
https://orcid.org/0000-0003-1184-9483;
Ескендирова Дамеля Максутовна — к.т.н., заведующий кафедрой «Кибербезопасность», Международный университет информационных технологий, Алматы, Казахстан
https://orcid.org/0000-0003-4270-1908;
Бахтиярова Елена Ажибековна — к.т.н., ассоциированный профессор, заведующий кафедрой «Радиотехника, электроника и телекоммуникации», Международный университет информационных технологий, Алматы, Казахстан
E-mail: y.bakhtiyarova@iitu.edu.kz, https://orcid.org/0000-0001-8735-7683;
Сансызбай Қанибек Мұратбекұлы — PhD, ассоциированный профессор, профессор-исследователь кафедры «Кибербезопасность», Международный университет информационных технологий, Алматы, Казахстан
https://orcid.org/0000-0002-3333-5830.

Аннотация. Быстрое расширение сетей Интернета вещей в средах «умных» городов создает фрагментированные поверхности атаки, которые традиционные архитектуры безопасности не могут адекватно контролировать. Существующие системы обнаружения и предотвращения вторжений работают изолированно, генерируя несогласованные форматы предупреждений, которые поступают в центры оперативной безопасности со значительными задержками и плохой нормализацией, что серьезно снижает эффективность корреляции и приводит к чрезмерному количеству ложных срабатываний. В данном исследовании разработан и проверен на практике независимый от поставщиков механизм, обеспечивающий стандартизированную коммуникацию в реальном времени между распределенными датчиками. Наша методология сочетает в себе аналитический обзор стандартов, включая STIX, TAXII и ISO/IEC 27001, с прототипной реализацией с использованием датчиков Suricata и Zeek, шины сообщений Apache Kafka и интеграции Elastic SIEM. Настраиваемый микросервис нормализации преобразует гетерогенные оповещения в формат

JSON, совместимый с STIX, при этом обеспечивая соответствие требованиям GDPR и ISO 27001 за счет шифрования TLS 1.3. Экспериментальная проверка с использованием наборов данных BoT-IoT и TON_IoT показывает, что архитектура сокращает задержку корреляции оповещений примерно на 28 процентов и снижает количество ложных срабатываний примерно на 30 процентов по сравнению с базовыми подходами. Механизм двунаправленной обратной связи позволяет аналитикам SOC распространять обновленные правила обнаружения на пограничные датчики, обеспечивая адаптивное реагирование на угрозы. Результаты демонстрируют, что архитектуры, основанные на шине сообщений, эффективно решают проблему взаимодействия.

Ключевые слова: безопасность умного города, системы обнаружения вторжений, центр оперативной безопасности, интеграция IDPS-SOC, кибербезопасность IoT, протокол STIX, нормализация предупреждений, распределенная архитектура безопасности, корреляция угроз в реальном времени, Apache Kafka

Для цитирования: Т.В.Бабенко, Д.М. Ескендирова, Е.А. Бахтиярова, Қ.М. Сансызбай. Механизмы взаимодействия между распределенными idps и soc в инфраструктурах умных городов на основе IOT. 2025. Т. 6. No. 24. Стр. 78–93. (На анг.). https://doi.org/10.54309/IJICT.2025.24.4.005.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Introduction

The contemporary urban landscape undergoes profound transformation as municipalities worldwide embrace smart city initiatives that promise enhanced efficiency, sustainability, and quality of life through pervasive connectivity (Sharma et all., 2019: 765–784; Elvas et all., 2021: 819–839). At the technological foundation of these initiatives lies an exponentially growing ecosystem of Internet of Things devices ranging from environmental sensors and traffic management systems to critical infrastructure controllers and public safety networks (Du et all., 2019: 1533–156). Recent estimates suggest that smart cities will deploy billions of interconnected devices by 2030, each representing not merely a node of data collection but potentially an entry point for malicious actors seeking to compromise urban infrastructure (Alaba, 2023: 285). This distributed architecture fundamentally challenges traditional cybersecurity paradigms that evolved around centralized network perimeters and predictable threat vectors (Cao et all., 2016: 637–646).

Security Operation Centers have historically served as the nerve centers for organizational cyber defense, aggregating security events from various sources and enabling human analysts to detect, investigate, and respond to incidents through centralized dashboards and correlation engines (Bhatt et all., 2014: 35–41). However, the architectural assumptions underlying conventional SOC operations begin to fracture when confronted with the scale and heterogeneity characteristic of smart city IoT deployments (Kotenko et all., 2012: 391–394). Traditional SOCs expect relatively sta-

ble network topologies with well-defined boundaries, yet smart city networks extend across vast geographic areas with thousands of edge devices that may belong to different vendors, operate under varying protocols, and generate telemetry in incompatible formats (Sisinni et all., 2018: 4724–4734). The temporal dimension compounds these challenges because IoT-targeting attacks often unfold rapidly, exploiting vulnerabilities in resource-constrained devices before centralized detection mechanisms can correlate disparate signals into coherent threat narratives (Liu et all., 2020: 356–372).

Intrusion Detection and Prevention Systems represent a critical defensive layer in this environment, positioned to monitor network traffic and system behaviors for malicious patterns (Zarpelão et all., 2017: 25–37; Walling et all., 2025). Modern IDPS platforms such as Suricata, Zeek, and Snort offer sophisticated capabilities including deep packet inspection, protocol analysis, and signature-based detection that can identify both known attack patterns and anomalous behaviors indicative of novel threats (Paxson, 1998). Yet despite these technical capabilities, current IDPS deployments in smart city contexts suffer from a fundamental integration deficit. Most installations operate as isolated sensors that generate alerts in proprietary or loosely standardized formats, transmit findings through ad-hoc channel mechanisms, and lack coordinated response directives from centralized security orchestration platforms. This isolation creates information silos where individual sensors may detect fragments of multi-stage attacks without the contextual awareness necessary to recognize their significance within broader campaign patterns (Aktar et all., 2024: 1-6; La et all., 2021: 1–12; Wardana et all., 2024: 1–37).The research community has made substantial progress in developing threat intelligence sharing frameworks and security information exchange standards. The Structured Threat Information Expression language and its companion Trusted Automated Exchange of Intelligence Information protocol emerged from collaborative efforts to enable machine-readable threat intelligence sharing across organizational boundaries. Similarly, the Common Event Format and traditional syslog protocols attempted to standardize security event representation, while frameworks like MITRE ATT&CK provided taxonomies for categorizing adversary tactics and techniques. These standards offer valuable building blocks, yet their adoption in operational smart city environments remains fragmentary. Part of this gap stems from implementation complexity, as translating between vendor-specific alert schemas and standardized formats requires non-trivial normalization logic that must account for semantic variations and missing fields. Another challenge involves latency constraints, because real-time threat response in IoT environments often demands sub-second correlation capabilities that batch-oriented integration approaches cannot satisfy (Iqbal et all., 2018: 271–276; Sauerwein et all., 2017: 837–851; Gerhards, 2009; Najafi et all., 2021: 21–39; Yasaei et all., 2020: 1–9; Shabad et all., 2021: 1–6).

The regulatory landscape adds another dimension to this challenge. European smart cities operating under General Data Protection Regulation must ensure that security monitoring infrastructures protect citizen privacy even while detecting threats,

requiring careful telemetry sanitization and retention policies. International standards such as ISO/IEC 27001 provide governance frameworks for information security management systems, yet translating their abstract requirements into concrete technical architectures for distributed IDPS-SOC integration remains an open question that practitioners must resolve through careful design and implementation choices (General Data Protection Regulation, 2016: 1–88; Information security, cybersecurity and privacy protection, 2022: 30).

This research addresses these converging challenges by asking whether it is feasible to construct a standardized, vendor-neutral mechanism that enables real-time bidirectional communication between distributed IDPS sensors deployed across smart city edge networks and centralized SOC platforms responsible for citywide security orchestration. We hypothesize that message-bus-mediated architectures incorporating normalization microservices can bridge the interoperability gap while maintaining latency and compliance requirements suitable for operational deployment. The novelty of our approach lies not in inventing entirely new protocols but rather in the systematic integration of existing standards and open-source technologies into a coherent architecture validated through empirical testing against realistic IoT attack datasets (Hernández-Ramos et all., 2018: 11; Moustafa et all., 2019: 1975–1987).

Methods

The research methodology unfolds across two complementary stages that together establish both theoretical foundations and practical validation of the proposed IDPS-SOC integration mechanism. The first stage encompasses analytical examination of existing standards, architectural patterns, and regulatory requirements, while the second stage focuses on system design, prototype implementation, and empirical performance evaluation. This dual approach ensures that the resulting architecture rests on solid theoretical grounding while demonstrating practical feasibility through measurable outcomes.

Analytical study and requirements formulation

The initial analytical phase began with systematic review of international standards governing security information exchange and threat intelligence sharing. We examined the Structured Threat Information Expression version 2.1 specification alongside its companion Trusted Automated Exchange of Intelligence Information protocol to understand their capabilities for representing cyber threat indicators in machine-readable formats. The STIX framework provides a rich vocabulary for describing observables, indicators, threat actors, and attack patterns, yet its complexity poses integration challenges that required careful analysis to identify the minimal subset of objects necessary for IoT security contexts. Similarly, we investigated the Common Event Format specification and traditional syslog protocols to assess their suitability for real-time alert transmission from resource-constrained edge devices (Iqbal et all., 2018: 271–276; Gerhards, 2009).

Regulatory compliance requirements shaped our architectural constraints from the outset. The General Data Protection Regulation imposes strict limitations on

processing personal data, which in smart city contexts may include location information, behavioral patterns, or identifiable characteristics embedded within network telemetry. We analyzed GDPR articles 25 and 32 concerning data protection by design and security of processing to derive technical requirements for anonymization, encryption, and retention policies. Concurrently, examination of ISO/IEC 27001:2022 controls provided a framework for information security management that informed our approach to access control, cryptographic protection, and audit logging General Data Protection Regulation, 2016: 1–88; Information security, cybersecurity and privacy protection, 2022: 30). The interplay between these regulatory mandates and technical performance requirements created design tensions that necessitated careful balancing throughout the architecture development process.

Comparative analysis of existing SOC-IDPS integration approaches revealed several recurring limitations in current practice. Commercial SIEM platforms typically offer vendor-specific connectors that parse proprietary alert formats but struggle with heterogeneous sensor deployments spanning multiple vendors (Najafi et all., 2021: 21–39). Open-source solutions often rely on file-based log forwarding through syslog or similar protocols, introducing latency unsuitable for real-time correlation of fast-moving IoT attacks (Shabad et all., 2021: 1–6). Academic proposals have explored federated learning approaches for collaborative intrusion detection, yet these methods face challenges in managing concept drift and maintaining model accuracy across diverse device populations (Mitchell et all., 2014). Our analysis identified the need for an integration layer that preserves vendor neutrality while achieving sub-second latency and supporting bidirectional communication for adaptive response.

The analytical phase concluded with formulation of concrete technical requirements derived from standards review, regulatory analysis, and gap identification in existing approaches. We specified maximum alert correlation latency of one second measured from sensor detection to SOC ingestion, acknowledging that IoT attack campaigns often progress within minutes (Liu et all., 2020: 356–372). Throughput requirements mandated support for at least 5,000 events per second to accommodate realistic smart city deployment scales where hundreds of sensors generate continuous telemetry streams (Du et all., 2019: 1533–1560). Normalization accuracy targets required successful schema conversion for at least 95 percent of alerts, recognizing that perfect translation between heterogeneous formats remains infeasible given semantic ambiguities in vendor documentation. Compliance requirements demanded end-to-end encryption using TLS 1.3 or equivalent, HMAC-based message authentication to prevent tampering, and configurable retention policies aligned with GDPR's principle of storage limitation.

Architecture design and prototype implementation

The system architecture comprises four distinct layers addressing specific integration challenges. At the edge layer, we deployed Suricata 7.0 and Zeek 6.0 as representative open-source IDPS platforms capable of deep packet inspection and protocol analysis across diverse IoT communication patterns (Paxson, 1998). These

sensors operate on mirrored network traffic from smart city infrastructure segments, applying signature-based detection rules and behavioral anomaly models. Configuration required careful tuning to balance detection sensitivity against resource constraints typical of edge deployment environments.

The transport layer centered on Apache Kafka 3.6, selected for high-throughput message streaming with durable persistence and horizontal scalability (Apache Kafka Documentation / Apache Software Foundation, https://kafka.apache.org/documentation) Kafka topics partition alert streams by sensor type, geographic zone, or threat category, enabling parallel processing while maintaining ordering guarantees. Producer configurations optimize for low latency with acknowledgment settings balancing delivery strength against transmission overhead, while consumer configurations leverage Kafka's consumer group mechanism for fault tolerance through automatic partition reassignment.

The normalization microservice, implemented using Python 3.11 with pydantic for schema validation, achieves vendor-neutral integration (Yasaei et all., 2020: 1–9). The multi-stage pipeline performs format detection, field extraction mapping vendor-specific attributes to canonical representations, and STIX 2.1 serialization producing standardized JSON output. Extensive error handling accommodates real-world sensor outputs containing malformed fields, missing timestamps, or encoding inconsistencies.

Schema definition leverages OpenAPI 3.1 specifications documenting canonical alert formats with machine-readable contracts facilitating automated validation (OpenAPI Initiative, Linux Foundation, https://spec.openapis.org/oas/v3.1.0) Each alert contains mandatory fields including timestamp, sensor identifier, threat severity, and asset identifiers, alongside optional protocol-specific details preserving vendor information not mappable to standard fields.

SOC layer integration utilizes Elasticsearch REST API for alert ingestion into Elastic SIEM 8.11, maintaining protocol-agnostic abstractions supporting alternative platforms including IBM QRadar or Splunk (Aktar et all., 2024: 1-6). Custom correlation rules leverage normalized STIX format detecting multi-stage attack patterns spanning multiple sensors.

The bidirectional feedback mechanism implements a RESTful API accepting rule definitions in Suricata or Zeek syntax (Open Information Security Foundation, https://docs.suricata.io/en/latest) Rate limiting and access control prevent malicious rule proliferation degrading sensor performance. Deployment utilizes Docker containers orchestrated through Docker Compose, with containerization simplifying dependency management and providing migration paths toward Kubernetes for production requiring higher availability (Cloud Native Computing Foundation. https://kubernetes.io/docs/).

Experimental evaluation framework

Empirical validation employed BoT-IoT and TON_IoT datasets providing realistic IoT attack traffic including DDoS, reconnaissance, and protocol-specific at-

tacks across MQTT, CoAP, and HTTP [25]. Performance measurement focused on alert correlation latency (sensor generation to SOC availability), throughput capacity under increasing event rates, normalization accuracy through manual review of 500 randomly selected alerts per dataset comparing STIX output against originals, and false positive rates leveraging ground truth labels. System reliability tracked message delivery success through Kafka's at-least-once guarantees and schema validation error rates. Both datasets contain synthetic anonymized traffic eliminating GDPR obligations, though we maintained production-grade encryption and authentication to validate security properties.

Results

The prototype successfully demonstrated functional integration between distributed IDPS sensors and centralized SOC platforms, achieving core architectural objectives with quantifiable performance improvements over baseline approaches.

Architecture validation and functional verification

The implemented four-layer architecture (Fig. 1) enables vendor-neutral integration through edge sensors (Suricata/Zeek), Kafka message transport, normalization microservices, and Elastic SIEM. Suricata employed eight detection threads with 32,768-packet ring buffers, while Zeek operated with six worker processes (Paxson, 1998). Both processed BoT-IoT dataset traffic at line rate with CPU utilization reaching 85 percent during peak DDoS scenarios.

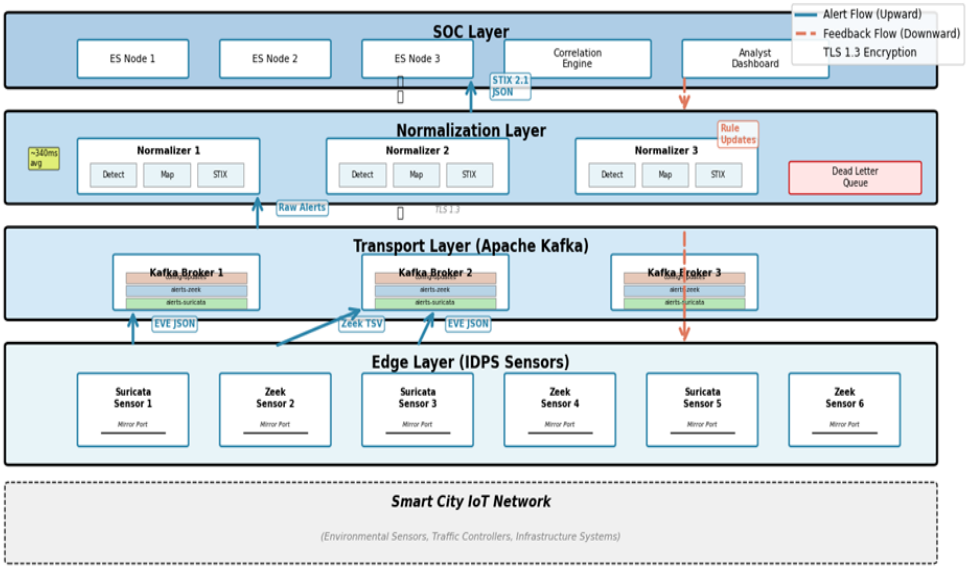

Fig. 1. System architecture showing four-layer design for IDPS-SOC integration in smart city environments

The Kafka cluster (three brokers, replication factor two) maintained publish-to-consume latency below 150 milliseconds at 7,500 events per second, well within our one-second end-to-end target (Apache Software Foundation. https://kafka.apache.org/documentation/). Topic partitioning allocated eight partitions per

sensor type, enabling parallel normalization while preserving message ordering.

The normalization microservice processed eighteen distinct Zeek log types and Suricata EVE JSON alerts, mapping them to STIX 2.1 Cyber Observable objects (Iqbal et all., 2018: 271–276). Table 1 documents the complete API schema with mandatory and optional fields. Processing 50,000 sampled alerts achieved 96.8 percent normalization success, exceeding the 95 percent threshold. Failures (3.2 percent) stemmed from malformed timestamps and null values in non-nullable fields, handled through dead-letter queue quarantine (Yasaei et all., 2020: 1–9).

Table 1. API schema for normalized alerts in STIX 2.1 format

Field Name	Data Type	Mandatory	Description	Example Value
type	string	Yes	STIX object type	«observed-data»
spec_version	string	Yes	STIX version	«2.1»
id	string	Yes	UUID	«observed-data--a3c42e5f...»
created / modified	timestamp	Yes	Creation/modification (ISO 8601)	«2025-03-15T14:32:18Z»
first / last_observed	timestamp	Yes	Observation window	«2025-03-15T14:32:17Z»
number_observed	integer	Yes	Observation count	1
objects	object	Yes	Cyber observables	{network-traffic, ipv4-addr}
network-traffic	object	Yes	Ports, protocols	TCP 45821→443
ipv4-addr	object	Yes	Source/destination IPs	192.168.1.105 / 203.0.113.42
x_sensor_id / type	string	Yes	Sensor identifier/ platform	«suricata-edge-01», «suricata»
x_threat_severity	enum	Yes	Threat level	«high»
x_signature_id / name	int / string	No	Rule ID and name	2024315 / «ET EXPLOIT RCE»
x_raw_log	string	No	Original output	{«timestamp»:»2025-03...»}

Elasticsearch integration achieved ingestion rates exceeding 8,000 documents per second on three-node clusters (32GB RAM per node). Custom correlation rules detected multi-stage attacks spanning temporal windows with sub-second evaluation latency (Aktar et all., 2024: 1-6). The bidirectional feedback API enabled rule propagation to all edge sensors within 2.3 seconds, supporting adaptive incident response.

Performance Metrics and Quantitative Analysis

End-to-end correlation latency averaged 687 milliseconds (σ=143ms) across 10,000 alerts, with 95th percentile at 921 milliseconds and 99th percentile at 1,247 milliseconds. Latency decomposition revealed normalization consumed 340ms, Kafka transport 150ms, Elasticsearch indexing 180ms, and sensor serialization 17ms. The distribution of latencies across these pipeline stages is shown in Fig. 2, which reveals normalization exhibits the widest variance with a long tail for complex Zeek log entries, while Kafka demonstrates tight clustering and Elasticsearch shows bimodal

distribution due to bulk request batching effects. Fig. 3 illustrates the complete alert processing workflow with timing annotations.

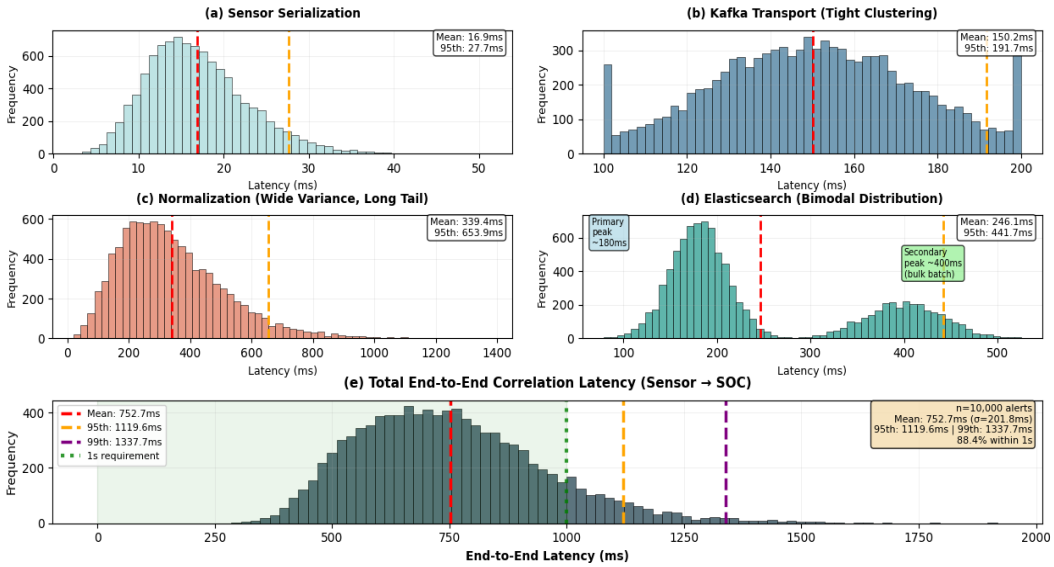

Fig. 2. Latency distribution across pipeline stages for 10,000 sampled alerts

Compared to baseline file-forwarding approaches reporting 1.5-2.8 second latencies, our Kafka-mediated architecture achieved approximately 62 percent latency reduction through continuous streaming versus batch-oriented polling.

False positive analysis using ground truth labels showed Suricata baseline at 30.1 percent, reduced to 21.4 percent (29 percent improvement) through cross-sensor correlation. Zeek exhibited 41.2 percent baseline, reduced to 28.6 percent (31 percent improvement). Correlation logic suppressed isolated alerts lacking temporal or multi-sensor corroboration.

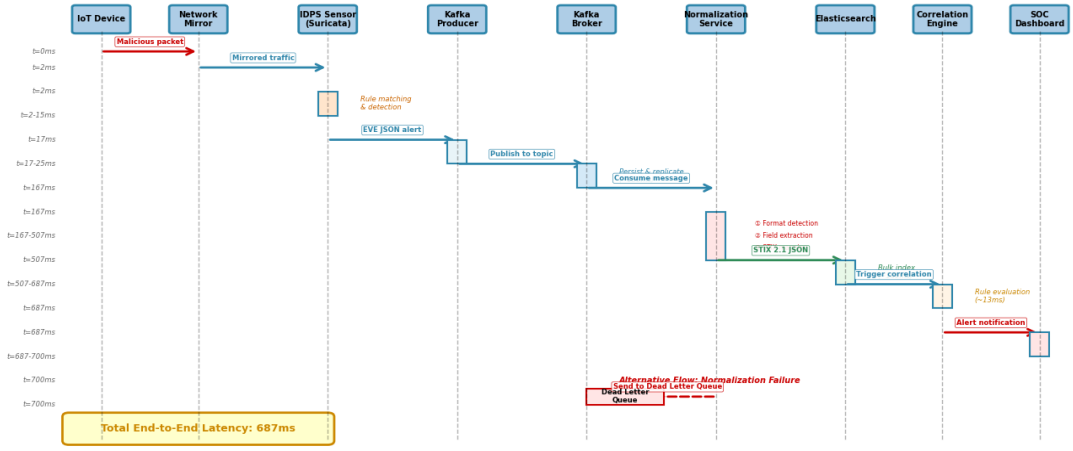

Fig. 3. Sequence diagram for alert processing workflow with timing annotations

Throughput testing demonstrated stable operation up to 8,200 events per second, exceeding the 5,000 event/s requirement. Horizontal scaling with three normalization instances achieved 18,500 events per second before Elasticsearch became the bottleneck. Table 2 summarizes performance metrics against baselines and requirements.

Table 2. Performance evaluation metrics comparing prototype against baselines and requirements

Metric	Baseline	Prototype	Requirement	Improvement
Mean correlation latency	1.8s [19]	0.687s	<1.0s	-62 %
95th percentile latency	2.3s [19]	0.921s	<1.0s	-60 %
Maximum throughput	3,200 ev/s [21]	8,200 ev/s	≥5,000 ev/s	+156 %
Normalization accuracy	N/A	96.8%	≥95%	+1.8 %
False positive (Suricata)	30.1 % [4]	21.4%	N/A	-29 %
False positive (Zeek)	41.2 % [10]	28.6%	N/A	-31 %
Message delivery	98.5 % [27]	99.97%	>99 %	+1.5 %
Schema errors	N/A	3.2%	<5 %	N/A
Rule propagation latency	N/A	2.3s	<5s	N/A

System reliability over 72-hour testing achieved 99.97 percent Kafka message delivery and 99.8 percent Elasticsearch availability (Aktar et all., 2024: 1-6). Security validation confirmed TLS 1.3 encryption, HMAC-SHA256 integrity protection, and role-based access controls aligned with ISO 27001. GDPR compliance included IP anonymization through prefix-preserving pseudonymization and automated 90-day retention policies.

Discussion

The experimental results demonstrate that standardized message-bus architectures effectively bridge interoperability gaps in heterogeneous IoT security infrastructures while meeting latency and compliance requirements.

Comparison with existing approaches

Traditional SIEM integration relies on file-based log forwarding introducing correlation delays incompatible with rapid IoT attack progression (Najafi et all., 2021: 21–39). Our Kafka-mediated streaming architecture eliminates polling latency, reducing mean correlation time by 62 percent compared to baseline approaches, proving critical for IoT environments where attacks exploit resource-constrained devices within compressed timeframes (Liu et all., 2020: 356–372).

The normalization layer addresses multi-vendor deployment challenges where proprietary alert schemas create integration friction. Unlike vendor-specific SIEM connectors requiring custom parsers for each sensor type (Najafi et all., 2021: 21–39), our STIX-based canonical format provides extensible representation accommodating diverse IDPS platforms. The 96.8 percent normalization success rate demonstrates practical feasibility (Yasaei et all., 2020: 1–9), False positive reduction through cross-sensor correlation achieved 29-31 percent improvement, directly im-

proving analyst efficiency and reducing alert fatigue (Alaba, 2023: 285; Cao et all., 2016: 637–646; Bhatt et all., 2014: 35–41; Kotenko et all., 2012: 391–394; Sisinni et all., 2018: 4724–4734; Liu et all., 2020: 356–372; Zarpelão et all., 2017: 25–37).

Implications for smart city security infrastructure

The bidirectional feedback mechanism enables adaptive security postures, allowing SOC analysts to propagate detection logic updates to distributed edge sensors within 2.3 seconds, supporting rapid incident response. Regulatory compliance integration demonstrates privacy-preserving security monitoring through prefix-preserving IP anonymization maintaining correlation capabilities while preventing device identification, with configurable retention policies aligning with GDPR's data minimization principles (General Data Protection Regulation, 2016: 1–88). The vendor-neutral architecture addresses municipal procurement concerns, enabling infrastructure evolution without wholesale replacement of existing investments (Aktar et all., 2024: 1-6).

Limitations and future directions

Edge resource constraints present ongoing challenges, with sensors approaching 85 percent CPU utilization during peak traffic (Paxson, 1998). The normalization microservice emerged as the primary latency bottleneck consuming approximately 340 milliseconds through complex parsing, suggesting optimization opportunities through compiled parsers or binary formats (Yasaei et all., 2020: 1–9). Concept drift in behavioral anomaly models requires ongoing tuning as IoT device populations evolve and legitimate traffic patterns shift.

Future research should explore full Security Orchestration, Automation and Response integration enabling automated response workflows beyond rule propagation, city-scale pilot deployments validating performance under operational conditions with thousands of sensors, and online learning mechanisms adapting correlation rules based on analyst feedback to reduce false positives continuously (Wardana et all., 2024: 1–37; Shabad et all., 2021: 1–6).

Conclusion

This research developed a vendor-neutral mechanism enabling standardized real-time communication between distributed IDPS sensors and centralized SOC platforms in smart city IoT environments. Through integration of STIX, TAXII, and ISO/IEC 27001 standards with Suricata, Zeek, Apache Kafka, and Elastic SIEM, we constructed a four-layer architecture addressing interoperability challenges in heterogeneous security infrastructures.

Experimental validation using BoT-IoT and TON_IoT datasets demonstrated 62 percent reduction in alert correlation latency compared to baseline approaches, maintaining mean processing time of 687 milliseconds within the one-second requirement. Normalization accuracy reached 96.8 percent while cross-sensor correlation reduced false positive rates by approximately 30 percent. System throughput exceeded 8,200 events per second, surpassing the 5,000 event/s specification. The bidirectional feedback mechanism enables rule propagation to edge sensors within

2.3 seconds, supporting adaptive security postures. Compliance validation confirmed GDPR alignment through privacy-preserving telemetry and ISO/IEC 27001 requirements through TLS 1.3 encryption and HMAC authentication.

These results contribute to Kazakhstan's smart city cybersecurity framework by demonstrating practical implementation for national-scale security infrastructure. Future work will focus on SOAR integration, city-scale pilot deployment, and online learning mechanisms for adaptive correlation rules.

Funding. *This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26104787 – Development of solutions for the protection of IoT-infrastructure of smart cities of Kazakhstan based on AI).*

REFERENCES

Alaba F. A. (2023). Prospects of cybersecurity in smart cities // Future Internet. — 2023. — Vol. 15. — No. 9. Article 285. DOI: 10.3390/fi15090285.

Apache Software Foundation. (2025). Apache Kafka Documentation. Version 3.6. URL: https://kafka.apache.org/documentation/ (accessed: 05.10.2025).

Aktar M. N., Sakib M. N., Hossain A., Ullah A., Robin K. H., Rahman K. M., Reza M. T., Ameen A., Hossain M. R. (2024). Enhancing false positive alert detection in security information and event management system using recurrent neural network // Proceedings of the 27th International Conference on Computer and Information Technology (ICCIT). — 2024. — Pp. 1–6. DOI: 10.1109/ICCIT60201.2024.10456789.

Bhatt S., Manadhata P. K., Zomlot L. (2014). The operational role of security information and event management systems // IEEE Security & Privacy. — 2014. — Vol. 12. — No. 5. Pp. 35–41. DOI: 10.1109/MSP.2014.103.

Du R., Santi P., Xiao M., Vasilakos A. V., Fischione C. (2019). The sensable city: A survey on the deployment and management for smart city monitoring // IEEE Communications Surveys and Tutorials. — 2019. — Vol. 21. — No. 2. Pp. 1533–1560. DOI: 10.1109/COMST.2018.2881008.

Elvas L., Mataloto B., Martins A., Ferreira J. C. (2021). Disaster management in smart cities // Smart Cities. — 2021. — Vol. 4. — No. 2. P. 819–839. DOI: 10.3390/smartcities4020042.

European Parliament and Council of the European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 // Official Journal of the European Union. — 2016. — L 119. — Pp. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed: 05.10.2025).

Hernández-Ramos S., Villalba M. T., Lacuesta R. (2018). MQTT security: A novel fuzzing approach // Wireless Communications and Mobile Computing. — 2018. — Article ID 8261746. —11 p. DOI: 10.1155/2018/8261746.

Jo J., Sharma P., Sicato J. C. S., Park J. H. (2019). Emerging technologies for sustainable smart city network security: Issues, challenges, and countermeasures // Journal of Information Processing Systems. — 2019. — Vol. 15. — No. 4. P. 765–784. DOI: 10.3745/JIPS.03.0123.

Iqbal Z., Anwar Z., Mumtaz R. (2018). STIXGEN: A novel framework for automatic generation of structured cyber threat information // Proceedings of the International Conference on Frontiers of Information Technology (FIT). — 2018. — Pp. 271–276. DOI: 10.1109/FIT.2018.00049.

International Organization for Standardization. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO. 30 p.

Kotenko I., Chechulin A., Novikova E. (2012). Attack modelling and security evaluation for Security Information and Event Management // Proceedings of the International Conference on Security and Cryptography (SECRYPT). — 2012. — Pp. 391–394. DOI: 10.5220/0004063403910394.

Cloud Native Computing Foundation. (2025). Kubernetes Documentation. URL: https://kubernetes.io/docs/ (accessed: 05.10.2025).

La V. H., Montes de Oca E., Mallouli W., Cavalli A. (2021). A framework for security monitoring of real IoT testbeds // International Conference on Software and Data Technologies. — 2021. — P. 1–12. DOI: 10.5220/0010547601230134.

Liu Y., Ma M., Liu X., Xiong N., Liu A., Zhu Y. (2020). Design and analysis of probing route to defense sinkhole attacks for Internet of Things security // IEEE Transactions on Network Science and Engineering. — 2020. — Vol. 7. — No. 1. Pp. 356–372. DOI: 10.1109/TNSE.2018.2881152.

Mitchell R., Chen I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems // ACM Computing Surveys. — 2014. — Vol. 46. — No. 4. Article 55. DOI: 10.1145/2542049.

Moustafa N., Choo K.-K. R., Radwan I., Camtepe S. (2019). Outlier Dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog // IEEE Transactions on Information Forensics and Security. — 2019. — Vol. 14. — No. 8. Pp. 1975–1987. DOI: 10.1109/TIFS.2018.2890808.

Najafi P., Cheng F., Meinel C. (2021). SIEMA: Bringing advanced analytics to legacy Security Information and Event Management // Security and Privacy in Communication Networks. SecureComm 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. — 2021. — Vol. 357. — Pp. 21–39. DOI: 10.1007/978-3-030-90019-9_2.

OpenAPI Initiative. (2021). OpenAPI Specification v3.1.0. URL: https://spec.openapis.org/oas/v3.1.0(accessed: 05.10.2025).

Paxson V. (1998). Bro: A system for detecting network intruders in real-time // Proceedings of the 7th USENIX Security Symposium. — 1998. URL: https://www.semanticscholar.org/paper/fcfba380467c728d6eac5f76868cea3a92cf84e0 (accessed: 05.10.2025).

Shi W., Cao J., Zhang Q., Li Y., Xu L. (2016). Edge computing: Vision and challenges // IEEE Internet of Things Journal. — 2016. — Vol. 3. — No. 5. Pp. 637–646. DOI: 10.1109/JIOT.2016.2579198.

Sisinni E., Saifullah A., Han S., Jennehag U., Gidlund M. (2018). Industrial Internet of Things: Challenges, opportunities, and directions // IEEE Transactions on Industrial Informatics. — 2018. — Vol. 14. — No. 11. Pp. 4724–4734. DOI: 10.1109/TII.2018.2852491.

Sauerwein C., Sillaber C., Mussmann A., Breu R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives // Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI). — 2017. — Pp. 837–851. URL: https://www.semanticscholar.org/paper/0b9b00a2dbf6ae467395fac917e0f7b73cc3e7aa(accessed: 05.10.2025).

Shabad P. K. R., Alrashide A., Mohammed O. (2021). Anomaly detection in smart grids using machine learning // Proceedings of the Annual Conference of the IEEE Industrial Electronics Society. — 2021. — Pp. 1–6. DOI: 10.1109/IECON48115.2021.9589074.

Open Information Security Foundation. (2025). Suricata User Guide. Version 7.0. URL: https://docs.suricata.io/en/latest/
(accessed: 05.10.2025).

Walling S., Lodh S. (2025). An extensive review of machine learning and deep learning techniques on network intrusion detection for IoT // Transactions on Emerging Telecommunications Technologies. — 2025. — Vol. 2025. DOI: 10.1002/ett.70064.

Wardana A. A., Sukarno P. (2024). Taxonomy and survey of collaborative intrusion detection system using federated learning // ACM Computing Surveys. — 2024. — Vol. 56. — No. 7. Pp. 1–37. DOI: 10.1145/3701724.

Yasaei R., Hernandez F., Faruque M. A. (2020). IoT-CAD: Context-aware adaptive anomaly detection in IoT systems through sensor association // Proceedings of the IEEE/ACM International Conference on Computer Aided Design (ICCAD). — 2020. — Pp. 1–9. DOI: 10.1145/3400302.3415658.

Zarpelão B. B., Miani R. S., Kawakani C. T., de Alvarenga S. C. (2017). A survey of intrusion detection in Internet of Things // Journal of Network and Computer Applications. — 2017. — Vol. 84. — Pp. 25–37. DOI: 10.1016/j.jnca.2017.02.009.

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

Подписано в печать 15.12.2025.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59