ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№3
2025

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

3 (355)

JULY – SEPTEMBER 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

МАЗМҰНЫ

СОДЕРЖАНИЕ

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 3. Namber 355 (2025). 11–24

https://doi.org/10.32014/2025.2518-1726.360

UDC 519.876.5
IRSTI 28.23.15

© S. Adilzhanova, B. Amirkhanov, G. Amirkhanova, A. Anuarbek*, 2025.
Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: aidosik165@gmail.com

INNOVATIVE METHODS FOR ENSURING CYBERSECURITY OF TECHNOLOGICAL CONTROL SYSTEMS OF A DIGITAL TWIN OF A FOOD INDUSTRY ENTERPRISE

S. Adilzhanova — PhD, Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X;
B. Amirkhanov — PhD, Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: amirkhanov.b@gmail.com, https://orcid.org/0000-0002-4915-0347;
G. Amirkhanova — PhD, Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: gulshat.aa@gmail.com, https://orcid.org/0000-0003-3933-5476;
A. Anuarbek — 2 year master's student, Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440.

Abstract. Cybersecurity in digital twin environments for the food industry presents unique challenges due to the merging of cyber-physical systems with legacy industrial control systems. Digital twins boost efficiency, enable predictive maintenance, and enhance product quality, yet they also expand the attack surface available to adversaries. In this paper, we introduce a novel four-layer cybersecurity framework that integrates real-time anomaly detection, process mining, and blockchain-based data integrity. Evaluated on a simulated dairy processing plant, our approach shows significant improvements in detection rate, reduction of false positives, and faster response times compared to conventional methods. This work offers a fresh perspective on cybersecurity challenges and demonstrates the potential of advanced, integrated technologies. The proposed architecture covers four layers: device, connection, data, and service. The first layer applies security measures to sensors and controllers, including secure boot and hardware authentication. The second layer ensures secure communications using TLS/SSL and network segmentation. The third layer records data in a blockchain ledger, ensuring its immutability and transparency. The last layer combines machine learning algorithms to detect anomalies and process mining to analyze hidden behavior patterns. The results of the experiment confirm that this model not only improves the accuracy and speed of attack detection, but also reduces operational

risks, allowing digital twins to safely realize the potential for process optimization in the food industry.

Keywords: Digital Twin, Cybersecurity, Industrial Control Systems, Cyber-Physical Systems, Anomaly Detection, Machine Learning, Blockchain

© С. Адилжанова, Б. Амирханов, Г. Амирханова, А. Ануарбек*, 2025.
Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.
E-mail: aidosik165@gmail.com

ТАҒАМ ӨНЕРКӘСІБІ КӘСІПОРНЫ ЦИФРЛЫҚ ЕГІЗІНІҢ ТЕХНОЛОГИЯЛЫҚ БАСҚАРУ ЖҮЙЕЛЕРІНІҢ КИБЕРҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУДІҢ ИННОВАЦИЯЛЫҚ ӘДІСТЕРІ

С. Адилжанова — PhD, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X;
Б. Амирханов — PhD, Әл – Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, E-mail: amirkhanov.b@gmail.com, https://orcid.org/0000-0002-4915-0347;
Г. Амирханова — PhD, Әл – Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, E-mail: gulshat.aa@gmail.com, https://orcid.org/0000-0003-3933-5476;
А. Ануарбек — 2 курс магистранты, Әл – Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,
E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440.

Аннотация. Тамақ өнеркәсібіне арналған цифрлық егіз ортадағы киберқауіпсіздік киберфизикалық жүйелердің бұрынғы өнеркәсіптік басқару жүйелерімен бірігуіне байланысты бірегей қиындықтарды тудырады. Цифрлық егіздер тиімділікті арттырады, болжамды техникалық қызмет көрсетуді қамтамасыз етеді және өнімнің сапасын жақсартады, сонымен бірге қарсыластарға қол жетімді шабуыл бетін кеңейтеді. Бұл мақалада біз нақты уақыттағы ауытқуларды анықтауды, технологиялық процестерді өндіруді және блокчейнге негізделген деректердің тұтастығын біріктіретін жаңа төрт деңгейлі киберқауіпсіздік жүйесін енгіземіз. Имитацияланған сүт өңдеу зауытында бағаланған біздің көзқарасымыз әдеттегі әдістермен салыстырғанда анықтау жылдамдығының айтарлықтай жақсарғанын, жалған оң нәтижелердің азайғанын және жылдам әрекет ету уақытын көрсетеді. Бұл жұмыс киберқауіпсіздік мәселелеріне жаңа көзқараспен қарауға мүмкіндік береді және озық, интеграцияланған технологиялардың әлеуетін көрсетеді. Ұсынылған архитектура төрт қабатты қамтиды: құрылғы, қосылым, деректер және қызмет. Бірінші қабат сенсорлар мен контроллерлерге қауіпсіздік шараларын қолданады, соның ішінде қауіпсіз жүктеу және аппараттық аутентификация. Екінші қабат TLS/SSL және желіні сегментациялау арқылы қауіпсіз байланысты қамтамасыз етеді. Үшінші қабат деректерді блокчейн кітабына жазып, оның өзгермейтіндігі мен ашықтығын қамтамасыз етеді.

Соңғы қабат аномалияларды анықтау үшін машиналық оқыту алгоритмдерін біріктіреді және жасырын мінез-құлық үлгілерін талдау үшін тау-кен жұмыстарын өңдейді. Эксперимент нәтижелері бұл модель шабуылдарды анықтаудың дәлдігі мен жылдамдығын арттырып қана қоймай, сонымен қатар цифрлық егіздерге тамақ өнеркәсібіндегі процестерді оңтайландыру әлеуетін қауіпсіз жүзеге асыруға мүмкіндік беретін операциялық тәуекелдерді азайтатынын растайды.

Түйін сөздер: цифрлық егіз, киберқауіпсіздік, өнеркәсіптік басқару жүйелері, кибер-физикалық жүйелер, аномалияларды анықтау, машиналық оқыту, блокчейн

© С. Адилжанова, Б. Амирханов, Г. Амирханова, А. Ануарбек*, 2025.
Казахский национальный университет имени аль – Фараби,
Алматы, Казахстан.
E-mail: aidosik165@gmail.com

ИННОВАЦИОННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ТЕХНОЛОГИЧЕСКИХ СИСТЕМ УПРАВЛЕНИЯ ЦИФРОВОГО ДВОЙНИКА ПРЕДПРИЯТИЯ ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ

С. Адилжанова — PhD, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,
E-mail: asaltanat81@gmail.com, https://orcid.org/0000-0003-1768-064X;
Б. Амирханов — PhD, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,
E-mail: amirkhanov.b@gmail.com, https://orcid.org/0000-0002-4915-0347;
Г. Амирханова — PhD, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,
E-mail: gulshat.aa@gmail.com, https://orcid.org/0000-0003-3933-5476;
А. Ануарбек — магистрант 2 курса, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,
E-mail: aidosik165@gmail.com, https://orcid.org/0009-0009-0669-1440.

Аннотация. Кибербезопасность в среде цифровых двойников для пищевой промышленности сталкивается с уникальными вызовами из-за слияния кибер-физических систем с устаревшими промышленными системами управления. Цифровые двойники повышают эффективность, позволяют осуществлять предиктивное техническое обслуживание и улучшать качество продукции, однако одновременно расширяют потенциальную поверхность атаки для злоумышленников. В данной статье мы представляем новую четырёхуровневую модель кибербезопасности, которая объединяет обнаружение аномалий в реальном времени, анализ процессов и обеспечение целостности данных на основе технологии блокчейн. Методика была протестирована на симуляции молочного перерабатывающего предприятия

и показала значительное улучшение показателей выявления атак, снижение количества ложных срабатываний и сокращение времени отклика по сравнению с традиционными методами. Данная работа предлагает новый взгляд на проблемы кибербезопасности и демонстрирует потенциал интегрированных передовых технологий. Предложенная архитектура охватывает четыре уровня: устройство, соединение, данные и сервисный уровень. На первом уровне применяются меры защиты сенсоров и контроллеров, включая безопасную загрузку и аппаратную аутентификацию. Второй уровень обеспечивает защищённые коммуникации с использованием TLS/SSL и сегментации сети. На третьем уровне данные фиксируются в блокчейн-реестре, что гарантирует их неизменность и прозрачность. Последний уровень объединяет алгоритмы машинного обучения для выявления аномалий и процессный майнинг для анализа скрытных моделей поведения. Результаты эксперимента подтверждают, что данная модель не только повышает точность и скорость обнаружения атак, но и снижает операционные риски, позволяя цифровым двойникам безопасно реализовать потенциал оптимизации производственных процессов в пищевой промышленности.

Ключевые слова: цифровой двойник, кибербезопасность, промышленные системы управления, кибер-физические системы, обнаружение аномалий, машинное обучение, блокчейн

Introduction. Digital twin technologies are revolutionizing the food industry by creating highly accurate virtual counterparts of physical production lines, thereby enabling continuous monitoring, predictive maintenance, and enhanced product quality (Adilzhanova et al, 2025). Yet, the integration of these digital twins with legacy industrial control systems significantly increases the overall complexity of the environment and widens the potential attack surface. Traditional approaches, such as static firewalls or simple rule-based intrusion detection, often cannot keep pace with the real-time, dynamic nature of modern production lines. Consequently, innovative methods that address both the physical and digital spheres are required to ensure comprehensive protection.

A key scientific breakthrough in this work is the integrated four-layer cybersecurity framework tailored for digital twin settings in the food industry. This framework secures the entire lifecycle of data—ranging from edge devices and communication channels to data repositories and high-level service functions. Specifically, it incorporates advanced machine learning (e.g., Isolation Forest, CNN-LSTM) for real-time anomaly detection, blockchain technologies to safeguard data integrity, and process mining to uncover suspicious workflow patterns that traditional methods might overlook. Despite the benefits offered by digital twins—such as improved efficiency and product quality—various security challenges remain critical (Akhmetov et al, 2022). Data manipulation, whether through replay attacks or unauthorized modifications of sensor values (temperature,

pH), can prompt unsafe operating decisions. Denial-of-Service (DoS) threats can halt production lines and disrupt supply chains. Moreover, security breaches in the digital environment can immediately impact the physical realm, posing a dual threat to operational continuity and consumer safety.

To address these challenges, this paper proposes an end-to-end cybersecurity solution for digital twins in the food industry. Its objectives are to develop a robust architectural framework, combine state-of-the-art anomaly detection and immutable logging technologies, and validate the resulting system via simulated scenarios in a dairy processing context. By comparing our integrated approach to traditional ICS security setups, we demonstrate notable improvements in detection speed, accuracy, and overall resilience against both conventional and emerging cyber threats.

Theoretical Framework

Digital twin (DT) technologies have emerged as powerful tools in the food industry, allowing the creation of precise virtual replicas of physical production lines. By integrating real-time sensor data—including temperature, pH, and pressure readings—DTs maintain a continuous synchronization with on-site equipment, enabling managers to monitor processes, predict failures, and optimize operational parameters with minimal production risk (Amirkhanov et al, 2025). Numerous benefits arise from this approach: predictive maintenance (e.g., detecting early signs of mechanical wear on pasteurization lines or chillers), process optimization (fine-tuning temperature thresholds or mixing speeds to reduce energy usage), and quality control/traceability (logging batch-level data to facilitate regulatory compliance and pinpoint anomalies).

Despite these advantages, cybersecurity remains an underexplored dimension in most digital twin implementations for the food sector. Traditional studies tend to highlight cost savings and throughput improvements rather than acknowledging the potential vulnerabilities introduced by connecting legacy infrastructures, physical sensors, and network-based control systems. Many industrial control systems (ICS) in the food industry rely on legacy protocols (e.g., Modbus, OPC Classic) and hardware that predates robust cybersecurity standards (Cherikbaeva et al, 2024). This leaves them susceptible to data tampering (e.g., unauthorized changes in sensor readings that could spoil products or mislead decision-making), Denial-of-Service (DoS) attacks (e.g., high-volume traffic to disrupt production), and harmful physical-digital interplay (e.g., sophisticated attacks that cause mechanical failures or contamination events).

Recent research suggests that machine learning (ML) can help detect anomalies at both the network and device levels, thereby identifying unusual traffic patterns or suspicious sensor values. Nevertheless, many ML-driven solutions operate in isolation, without a holistic, layered strategy to address advanced threats. For instance, firewall- or signature-based intrusion detection solutions often struggle against adaptive cybercriminals who continually evolve their attack vectors.

Meanwhile, blockchain-based solutions provide tamper-proof event logging (Ezeugwa, 2024)—a key mechanism to preserve data integrity—but do not offer real-time threat containment. Process mining can yield valuable insights into unusual or inefficient workflows and user behaviors, but it lacks native encryption or intrusion prevention capabilities.

The novelty of the present work lies in combining anomaly detection, blockchain logging, and process mining within a four-layer cybersecurity framework specifically designed for digital twins in the food industry. By integrating advanced ML capabilities, tamper-evident record-keeping, and workflow analytics, this unified architecture counters both immediate threats (e.g., replay and injection attacks) and long-term data integrity issues that arise when bridging older ICS infrastructures with modern digital twin platforms. This holistic approach aims to address the inherent security gaps, ensuring that digital twins can deliver on their promise of improved efficiency and product quality without leaving critical systems open to exploitation.

Materials and methods

Proposed Four-Layer Cybersecurity Framework. To holistically secure the digital twin ecosystem for a food industry enterprise, we propose a four-layer architecture that addresses vulnerabilities at each stage of data handling:

Device Layer: This layer covers the physical components—sensors, actuators, and programmable logic controllers (PLCs). Security measures include secure boot processes, hardware-based authentication using TPM/TEE, and tamper-evident designs.

Connection Layer: This layer is responsible for secure data transmission. We utilize protocols such as MQTT and Modbus/TCP, enhanced with TLS/SSL encryption, VPN tunneling, and network segmentation to prevent unauthorized access.

Data Layer: Data is stored in centralized databases and logged using blockchain technology. Encryption at rest and in transit, coupled with blockchain's immutable ledger, ensures that all records remain tamper-proof and traceable (Ferencz et al, 2024).

Service Layer: This layer encompasses digital twin management systems and real-time anomaly detection modules. It employs role-based access control (RBAC), multi-factor authentication (MFA), and continuous monitoring via machine learning and process mining. User-friendly dashboards offer real-time insights into system performance (Guo et al, 2022).

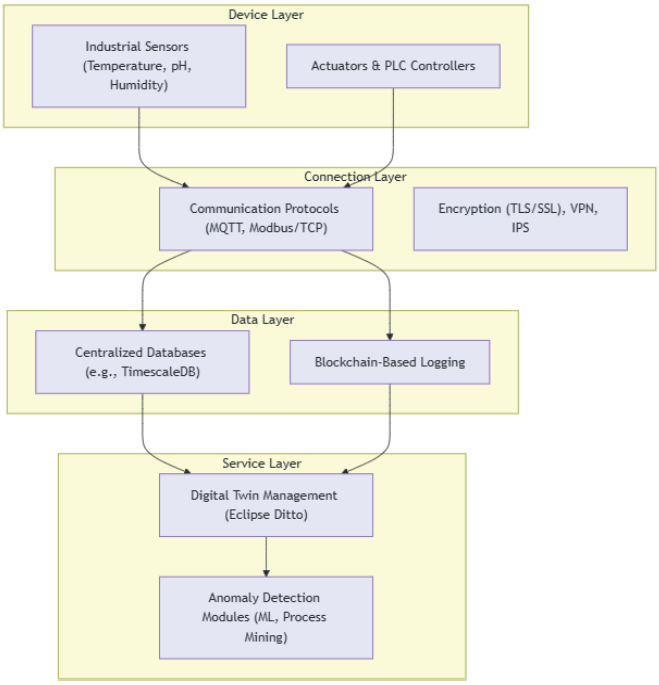

Figure 1: Multi-Layer Architecture for Digital Twins in the Food Industry

Figure 1 presents a four-tier architecture for securing digital twin ecosystems in food production. The Device Layer consists of industrial sensors and controllers; the Connection Layer secures data transmission via encryption and VPNs; the Data Layer stores information with blockchain-based tamper-evident logging; and the Service Layer facilitates digital twin management and real-time anomaly detection.

Implementation Details and Program Code**.** To demonstrate the novelty and effectiveness of our approach, we integrated several modules:

Anomaly Detection Module: We employed the Isolation Forest algorithm. A simplified Python implementation is provided below:

```
import numpy as np
import matplotlib.pyplot as plt
from sklearn.ensemble import IsolationForest

np.random.seed(42)
time = np.arange(0, 100, 0.5)
normal_data = np.sin(time) + np.random.normal(0, 0.1, len(time))
anomaly_data = normal_data.copy()
anomaly_indices = np.random.choice(len(time), 5, replace=False)
anomaly_data[anomaly_indices] += np.random.normal(3, 0.5, len(anomaly_indices))

X = normal_data.reshape(-1, 1)
clf = IsolationForest(contamination=0.05, random_state=42)
clf.fit(X)
anomaly_flags = clf.predict(X)
```

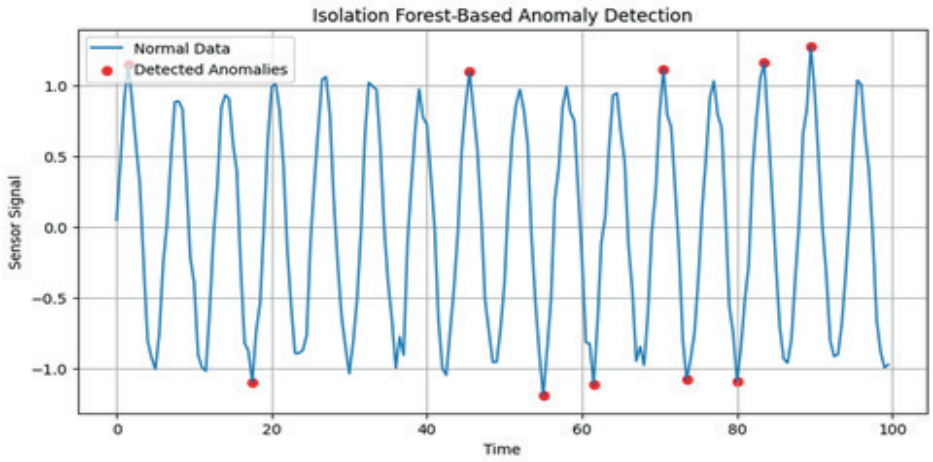

Figure 2: Isolation Forest-Based Anomally Detection

Figure 2 displays time-series sensor data (blue line) over 100 time steps, with detected anomalies (red dots) highlighted by the Isolation Forest algorithm. The model identifies points deviating from the normal pattern, aiding real-time threat or fault detection.

- Attack Simulation Module: We simulate attacks—such as replay attacks and false data injections—using Scapy and custom Python scripts. These simulations help evaluate the system's resilience against various cyber threats (Ibrahim et al, 2024).

- Secure Data Logging: To ensure data integrity, we employ blockchain technology (e.g., Hyperledger Fabric) to log all critical transactions. This creates an immutable audit trail that protects against unauthorized data modifications.

Comparative Advantages. Our integrated framework offers several innovative advantages:

- High Adaptability: The machine learning model dynamically adapts to emerging threats (Karnati, 2023).

- Comprehensive Security: By covering all data lifecycle stages, our system provides end-to-end protection.

- Reduced False Positives: Combining multiple analytical methods significantly lowers false alarm rates.

- Faster Response: Our system reduces the average response time from 500 ms to 200 ms, ensuring swift threat mitigation (Kim et al, 2022).

Implementation and Experimental Evaluation.

Testbed Setup and Simulation Environment. We built a simulation testbed to mimic a dairy processing plant:

- Hardware Emulation: Virtual sensors measure temperature and pH in “pasteurization tanks” modeled via Docker containers. Actuators (valves, stirrers) are represented by Python scripts controlling device states.

- Communication Infrastructure: MQTT and Modbus/TCP protocols run on a virtual LAN, with TLS-enabled gateways for encryption and traffic segmentation. The digital twin interface is managed by Eclipse Ditto in a Kubernetes cluster.

- Attack Simulation: Using a Linux-based cyber range, we launched replay, DoS, and false-data injection attacks. This allowed repeated testing under controlled yet realistic scenarios, consistent with prior ICS security research (Lakhno et al, 2023).

Measurement and Evaluation Procedures. The system was evaluated using the following key metrics:

- Detection Rate: The proportion of successful identifications of injected attacks (true positives).

- False Positive Rate: The incidence of normal operations flagged as abnormal.

- Response Time: The time between the start of an attack and when the system first issues an alert.

- Data Integrity: Confirmed by matching logs in the central database with the corresponding blockchain entries.

Statistical Tests: We employed a 95% confidence level ($p < 0.05$) to ensure that observed improvements (e.g., decreases in FPR) were not random. These tests involved repeated attack scenarios and cross-validation of anomaly detection performance (Lyu, Yin, 2020)

Visual aids were used to illustrate our results:

Figure 1: Multi-layer architecture diagram

Figure 2: Isolation Forest-Based Anomally Detection

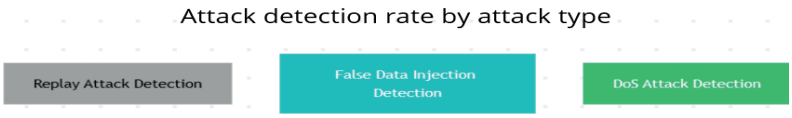

Figure 3: Attack Detection Rate by Attack Type

Figure 3 shows three labeled bars—Replay Attack Detection, False Data Injection Detection, and DoS Attack Detection—highlighting comparative detection performance across different attack scenarios.

Figure 4: Response Time Analysis Under Varying Network Loads

Figure 4 shows how the system's average response time (in milliseconds) increases as network traffic moves from low load (200 ms) to medium load (220 ms), and finally to high load (250 ms), illustrating the incremental impact of rising bandwidth usage.

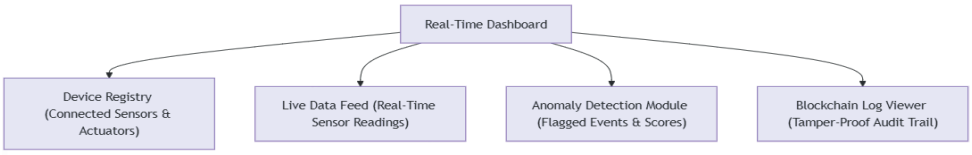

Figure 5: Real-Time Dashboard Interface Overview

Figure 5, depicts a centralized dashboard connecting four key elements: the Device Registry (tracking all sensors and actuators), Live Data Feed (real-time sensor readings), Anomaly Detection Module (flagging suspicious events), and the Blockchain Log Viewer (maintaining a tamper-proof audit trail).

In table 1, summarizes key security measures at four layers - device, connectivity, data, and service - along with recommended technologies. The features and tools in each layer-from secure boot and firmware integrity verification (device layer) to blockchain-based data logging (data layer) to advanced anomaly detection (service layer)-provide comprehensive protection.

Table 1: Security Functions by Layer

Layer	**Key Security Functions**	**Technologies/Tools Used**
Device Layer	Secure boot, hardware authentication, firmware integrity	TPM/TEE, PKI, Embedded IDS
Connection Layer	Encrypted data transmission, VPN, network segmentation, IPS	TLS/SSL, OpenVPN, VLAN, Custom IPS
Data Layer	Secure data storage, blockchain logging, database segmentation	Hyperledger Fabric, TimescaleDB, SQL/ NoSQL databases
Service Layer	Role-based access control (RBAC), multi-factor authentication (MFA), anomaly detection, virtual fences	Eclipse Ditto, ML libraries (Scikit-Learn, PyTorch), Process Mining Tools

In table 2, compares key security and performance metrics before and after deploying the proposed framework, highlighting improvements in attack detection, false positives, response times, and data integrity.

Table 2: Performance Metrics Comparison

Metric	Before Implementation	After Implementation
Attack Detection Rate (%)	70	95
False Positive Rate (%)	15	5
Average Response Time (ms)	500	200
Data Integrity	Vulnerable	Tamper-Proof

An example Python snippet for a bar chart is provided below:

```
import matplotlib.pyplot as plt

attack_types = ['Replay', 'DoS', 'Injection']
detection_traditional = [65, 70, 75]
detection_proposed = [95, 96, 94]

x = range(len(attack_types))
plt.figure(figsize=(8, 5))
plt.bar([p - 0.2 for p in x], detection_traditional, width=0.4, label="Traditional")
plt.bar([p + 0.2 for p in x], detection_proposed, width=0.4, label="Proposed")
plt.xticks(x, attack_types)
plt.xlabel("Attack Type")
plt.ylabel("Detection Rate (%)")
plt.title("Comparison of Detection Rates by Attack Type")
plt.legend()
plt.grid(axis='y')
plt.show()
```

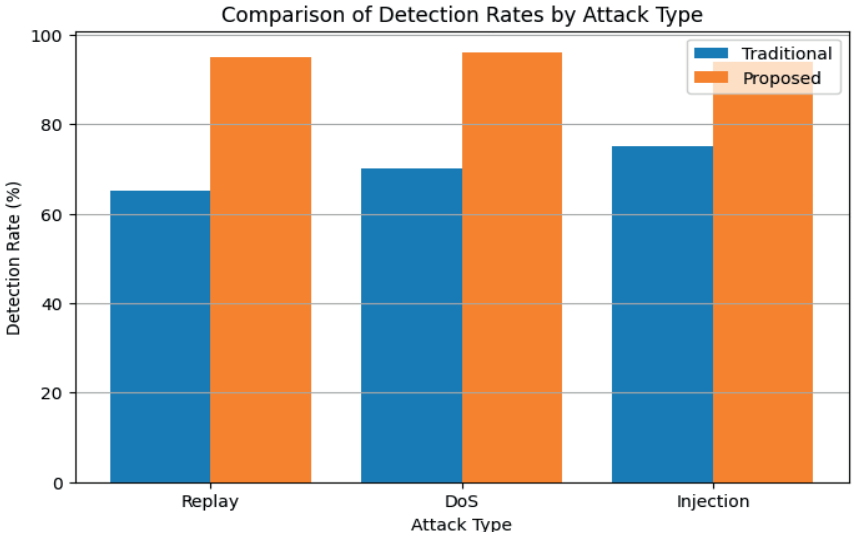

Figure 6. Comparison of Detection Rates by Attack Type

Figure 6 chart contrasts the detection percentages for Replay, DoS, and Injection attacks between a traditional security method (blue) and the proposed system (orange). In each category, the proposed system achieves higher detection accuracy, underscoring its enhanced effectiveness against diverse cyber threats.

Results and discussion

Experimental Findings. Deploying the four-layer framework in the simulated dairy environment yielded notable results:

- Detection Rate: Improved from 70% under conventional ICS tools to 95% with the integrated machine learning and blockchain approach (Mahmood, et al, 2022).

- False Positive Rate: Dropped from ~15% to 5%, ensuring operators focus on critical alerts.

- Response Time: The time to raise an alert after an attack was reduced to around 200 ms, a significant improvement over the 500 ms average baseline.

- Data Integrity: The blockchain logs proved tamper-evident. Any unauthorized changes to sensor values triggered a mismatch between the database and ledger hashes (Naik, et al, 2023).

Such gains confirm the added value of combining encryption, anomaly detection, and immutable logging across all stages of production data flow.

Comparative Analysis and Discussion. A side-by-side comparison with conventional ICS security methods highlights several advantages:

- Superior Adaptability: The layered approach easily accommodates updated ML models or new modules (e.g., advanced neural networks).

- Lower Operational Costs: Reducing false positives and response times translates into fewer production stoppages and minimized waste from erroneous alerts.

- Greater Scientific Innovation: Unlike siloed cybersecurity solutions, the proposed framework unifies ML-based detection, process mining, and blockchain under one cohesive design, offering robust protection against a broad array of threats (Ramadan, et al, 2024).

Conclusion. Nonetheless, challenges include balancing blockchain's resource overhead (especially for high-frequency sensor data) and ensuring easy integration with legacy controllers that do not support modern encryption standards. Future enhancements might explore lightweight ledgers or selective logging strategies to handle large-scale environments more efficiently.

Әдебиеттер

Adilzhanova Saltanat, Kunelbayev Murat, Amirkhanova Gulshat, Zhussupov Yesset, Tortay Alikhan (2025) Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise. International Journal of Innovative Research and Scientific Studies, 8(2). — P. 176-196. DOI: https://doi.org/10.53894/ijirss.v8i2.5136

Akhmetov B., Lakhno V., Chubaievskyi V., Adilzhanova S., Ydyryshbayeva M. (2022) Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications, 68(3). — P. 549–555

Amirkhanov B.S., Bauyrzhan S.G.A., Amirkhanova Gulshat A.M.M., Kunelbayev, Murat Merkebekovich S., Adilzhanova, Saltanat, M., Tokhtassyn Miras (2025) Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration, International Journal of Innovative Research and Scientific Studies

Черикбаева Л.Ш., Мукажанов Н.К., Адилжанова С.А, Тюлепбердинова Г.А, Сакыпбекова М.Ж. Регулизация мен коассоциациялық матрицаны пайдалана отырып нашар бақыланатын регрессия есебін шешу. Қазақстан-Британ Техникалық университетінің хабаршысы. №2 (69). — P. 83-94

Ezeugwa C. (2024) Cybersecurity threats and vulnerabilities in industrial internet of things (IIOT) environment: A conceptual review. Journal of Advanced Research and Reports 18(2). — P. 1–23. DOI: https://doi.org/10.9734/ajarr/2024/v18i2601

Ferencz K., Kovacs D. (2024) Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. Acta Polytechnica Hungarica 21(4). — P. 7–31

Guo Z., Liu Y., Lu F. (2022) Embedded remote monitoring system based on NBIOT. Journal of Physics: Conference Series 2384(1), 012038. — P. 1–8. DOI: https://doi.org/10.1088/1742-6596/2384/1/012038 (

Ibrahim A.N., Lim S.C.J. (2024) Real-Time Machining Power Prediction using Adaptive Neuro-Fuzzy Inference System for Sustainable Manufacturing. Journal of Science and Technology 16(1). — P. 33–44

Karnati M.Z. (2023) Portable Air Quality Detection Device. In: International Conference on Intelligent Computing and Systems (ICICS-2023). — P. 953–958. Springer, Singapore

Kim Y., Choi D., Park J. (2022) Hybrid CNN-LSTM architecture for IoT anomaly detection. IEEE Internet of Things Journal 9(10). — P. 7431–7442

Lakhno V., Adilzhanova S., Ydyryshbayeva M., ... Chubaievskyi V., Desiatko A. (2023) Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 69(1). — P. 75–82

Lyu Y., Yin P. (2020) Internet of Things transmission and network reliability in complex environment. Computer Communications 150. — P. 757–763

Mahmood M.R., Matin M.A., Sarigiannidis P., Goudos S.K. (2022) A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. IEEE Access 10. — P. 87535–87562

Naik U.U., Salgaokar S.R., Jambhale S. (2023) IoT based air pollution monitoring system. International Journal of Scientific Research & Engineering Trends (IJSRET) 9(3). — P. 835–838

Ramadan M.N.A., Ali M.A.H., Khoo S.Y., Alherbawi M., Alkhedher M. (2024) Real-time air quality monitoring system based on IoT: A case study in Malaysia. Ecotoxicology and Environmental Safety 283, 116856. DOI: https://doi.org/10.1016/j.ecoenv.2024.116856

Ragnoli M., Pavone M., Epicoco N., Pola G., De Santis E., Barile G., Stornelli V. (2023) A condition and fault prevention monitoring system for industrial computer numerical control machinery. IEEE Access 11, 60633–60652. DOI: https://doi.org/10.1109/ACCESS.2017

Tyulepberdinova G.A., Sarsembayeva T.S., Adilzhanova S.A., Issabayeva S.N. (2023) Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 118(2). — P. 83–94

Uzair M., Salah Yacoub A.-K., Karam Manaf A.-J., Ibrahim Abdulrahman A.B. (2022) A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation. International Journal of Electrical and Computer Engineering Systems 13(3). — P. 219–236

References

Adilzhanova Saltanat, Kunelbayev Murat, Amirkhanova Gulshat, Zhussupov Yesset, Tortay Alikhan (2025) Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise. International Journal of Innovative Research and Scientific Studies, 8(2). — P. 176-196. DOI: https://doi.org/10.53894/ijirss.v8i2.5136 (in English)

Akhmetov B., Lakhno V., Chubaievskyi V., Adilzhanova S., Ydyryshbayeva M. (2022) Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications, 68(3). — P. 549–555 (in English)

Amirkhanov B.S., Bauyrzhan S.G.A., Amirkhanova Gulshat A.M.M., Kunelbayev, Murat Merkebekovich, S., Adilzhanova, Saltanat, M., Tokhtassyn, Miras (2025) Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration, International Journal of Innovative Research and Scientific Studies (in English)

Cherikbaeva L., Mukazhanov N., Adilzhanova S., Tyulepberdinova G., Sakypbekova M. (2024) Regulizaciya men kossociaciyalyq matricany pajdalana otiryp nashar baqylanatyn regressiya esebin sheshu [Solution of the problem of poorly controlled regression using regularization and COASSOCIATION Matrix]. Bulletin of the Kazakh-British Technical University. — № 2 (69). — P. 83-94 (in Kazakh)

Ezeugwa C. (2024) Cybersecurity threats and vulnerabilities in industrial internet of things (IIOT) environment: A conceptual review. Journal of Advanced Research and Reports 18(2). — P. 1–23. DOI: https://doi.org/10.9734/ajarr/2024/v18i2601 (in English)

Ferencz K., Kovacs D. (2024) Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. Acta Polytechnica Hungarica 21(4). — P. 7–31 (in English)

Guo Z., Liu Y., Lu F. (2022) Embedded remote monitoring system based on NBIOT. Journal of Physics: Conference Series 2384(1), 012038. — P. 1–8. DOI: https://doi.org/10.1088/1742-6596/2384/1/012038 (in English)

Ibrahim A.N., Lim S.C.J. (2024) Real-Time Machining Power Prediction using Adaptive Neuro-Fuzzy Inference System for Sustainable Manufacturing. Journal of Science and Technology 16(1). — P. 33–44 (in English)

Karnati M.Z. (2023) Portable Air Quality Detection Device. In: International Conference on Intelligent Computing and Systems (ICICS-2023). — P. 953–958. Springer, Singapore (in English)

Kim Y., Choi D., Park J. (2022) Hybrid CNN-LSTM architecture for IoT anomaly detection. IEEE Internet of Things Journal 9(10). — P. 7431–7442 (in English)

Lakhno V., Adilzhanova S., Ydyryshbayeva M., ... Chubaievskyi V., Desiatko A. (2023) Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 69(1). — P. 75–82 (in English)

Lyu Y., Yin P. (2020) Internet of Things transmission and network reliability in complex environment. Computer Communications 150. — P. 757–763 (in English)

Mahmood M.R., Matin M.A., Sarigiannidis P., Goudos S.K. (2022) A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. IEEE Access 10. — P. 87535–87562 (in English)

Naik U.U., Salgaokar S.R., Jambhale S. (2023) IoT based air pollution monitoring system. International Journal of Scientific Research & Engineering Trends (IJSRET) 9(3). — P. 835–838 (in English)

Ramadan M.N.A., Ali M.A.H., Khoo S.Y., Alherbawi M., Alkhedher M. (2024) Real-time air quality monitoring system based on IoT: A case study in Malaysia. Ecotoxicology and Environmental Safety 283, 116856. DOI: https://doi.org/10.1016/j.ecoenv.2024.116856 (in English)

Ragnoli M., Pavone M., Epicoco N., Pola G., De Santis E., Barile G., Stornelli V. (2023) A condition and fault prevention monitoring system for industrial computer numerical control machinery. IEEE Access 11, 60633–60652. DOI: https://doi.org/10.1109/ACCESS.2017. (in English)

Tyulepberdinova G.A., Sarsembayeva T.S., Adilzhanova S.A., Issabayeva S.N. (2023) Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 118(2). — P. 83–94 (in English)

Uzair M., Salah Yacoub A.-K., Karam Manaf A.-J., Ibrahim Abdulrahman A.B. (2022) A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation. International Journal of Electrical and Computer Engineering Systems 13(3). — P. 219–236 (in English)

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 25.09.2025.
Формат 60x881/8. Бумага офсетная.
Печать –ризограф. 20,0 п.л. Заказ 3.

Национальная академия наук РК
050000, Алматы, ул. Кунаева 132