RESOLVING SECURITY ISSUES IN THE INTERNET OF THINGS AND DIGITAL SOCIETY

Kabulova Zulaykho
Tashkent University of Information Technologies named after Muhammad al-Khwarizm, Tashkent Amir Temur street 108, Uzbekistan
E-mail: zulayxoqobulova53@gmail.com
0009-0008-3456-0707
Irgasheva Durdona
Tashkent University of Information Technologies named after Muhammad al-Khwarizm, Tashkent Amir Temur street 108, Uzbekistan
E-mail: durdona.ya@gmail.com
0000-0001-5390-6533

Abstract. The accelerated rate of the spread of Internet of Things (IoT) devices has increased the creation of a hyper-connected digital society, where ubiquitous connectivity and unceasing data transmission form the foundation of key infrastructures, industrial networks and personal services. Whereas such developments give unmatched efficiency, automation, and convenience, they also introduce the vast cyberattack surface, putting individuals, organizations, and states at a high level of security and privacy risks. The present paper critically examines the most urgent security concerns of the IoT ecosystems and the digital society, such as vulnerabilities at the device level, unsecured communication protocols, massive attacks by botnets, and data breaches. Countermeasures known to date multi-factor authentication, end-to-end encryption, secure boot and network segmentation are checked and assessed based on their efficiency and weaknesses on actual implementations. Also, the research discusses does solutions, such as blockchain to manage decentralized trust and machine learning to detect anomalies and respond to potential threats, which have potential to enhance the security of IoT architecture. The contribution of the paper to the ongoing discussion is the presentation of a multidisciplinary approach, which incorporates technical, architectural and policy-based strategies, and provides the design of scalable, resilient and future-proof IoT security systems within the digital society.

Keywords: Internet of Things (IoT); Digital Society; Cybersecurity; Data Privacy; Authentication; Encryption; Network Segmentation; Blockchain; Machine Learning; Threat Mitigation; Secure Architecture; IoT Security Framework.

Abstract. "Internet of Things" (IoT) qurilmalarining jadal sur'atlar bilan tarqalishi giper-bog'langan raqamli jamiyatni shakllantirishni tezlashtirmoqda. Bu jamiyatda hamma joyda mavjud bo'lgan ulanish va uzluksiz ma'lumot uzatish asosiy infratuzilma, sanoat tarmoqlari va shaxsiy xizmatlar uchun poydevor hisoblanadi. Bunday rivojlanish benazir samaradorlik, avtomatlashtirish va qulaylikni

ISSN 3030-3907

ta'minlash bilan birga, keng ko'lamli kiberhujumlar maydonini ham ochib, shaxslar, tashkilotlar va davlatlarni yuqori darajadagi xavfli xavf va tahlukalar ostiga qo‘ymoqda. Ushbu maqola IoT ekotizimlari va raqamli jamiyatning eng dolzarb xavfsizlik muammolarini, jumladan, qurilma darajasidagi zaifliklar, xavfli aloqa protokollari, botnetlar tomonidan amalga oshiriladigan ommaviy hujumlar va ma'lumotlarning buzilishini tanqidiy ko'rib chiqadi. Ma'lum bo'lgan himoya choralari – ko‘p omilli autentifikatsiya, end-to-end shifrlash, xavfsiz ishga tushirish (secure boot) va tarmoq segmentatsiyasi – ularning amaliy tatbiqdagi samaradorligi va zaif tomonlari asosida tahli qilinadi va baholanadi. Shuningdek, tadqiqotda blokcheyn kabi yangi yechimlar (markazlashtirilmagan ishonchni boshqarish uchun) va anormalliklarni aniqlash va potentsial tahdidlarga javob berish uchun mashina o‘rganish (machine learning) kabi texnologiyalar ko'rib chiqilib, ularning IoT arxitekturasining xavfsizligini oshirishdagi imkoniyatlari tahli qilinadi. Maqolaning muhim hissasi sifatida ko‘p tarmoqli yondashuv taklif etiladi, bu texnik, arxitektura va siyosatga asoslangan strategiyalarni birlashtiradi va raqamli jamiyat doirasida masshtablanuvchan, bardoshli va kelajakka chidamli IoT xavfsizlik tizimlarini loyihalash yo‘llarini taqdim etadi.

Kalit so‘zlar: Internet of Things (IoT); Raqamli jamiyat; Kiberxavfsizlik; Ma'lumotlar maxfiyligi; Autentifikatsiya; Shifrlash; Tarmoq segmentatsiyasi; Blokcheyn; Mashinani o‘rganish; Tahdidlarni bartaraf etish; Xavfsiz arxitektura; IoT xavfsizlik framework.

Аннотация. Ускоренные темпы распространения устройств "Интернета Вещей" (IoT) привели к формированию гиперподключенного цифрового общества, где повсеместная связь и непрерывная передача данных являются основой ключевой инфраструктуры, промышленных сетей и персональных сервисов. Хотя такие достижения обеспечивают непревзойденную эффективность, автоматизацию и удобство, они также создают обширную поверхность для кибератак, подвергая отдельных лиц, организации и государства высокому уровню рисков для безопасности и конфиденциальности. Настоящая статья критически исследует наиболее актуальные проблемы безопасности экосистем IoT и цифрового общества, такие как уязвимости на уровне устройств, небезопасные протоколы связи, массовые атаки с использованием ботнетов и утечки данных. Известные на сегодня меры противодействия — многофакторная аутентификация, сквозное шифрование, безопасная загрузка (secure boot) и сегментация сети — анализируются и оцениваются на основе их эффективности и слабых сторон в реальных реализациях. Кроме того, в исследовании рассматриваются новые решения, такие как блокчейн для управления децентрализованным доверием и машинное обучение для обнаружения

ISSN 3030-3907

аномалий и реагирования на потенциальные угрозы, которые обладают потенциалом для повышения безопасности архитектуры IoT. Вклад данной статьи в ongoing дискуссию заключается в представлении многодисциплинарного подхода, который объединяет технические, архитектурные и политико-управленческие стратегии, и предлагает проектирование масштабируемых, устойчивых и готовых к будущим вызовам систем безопасности IoT в рамках цифрового общества.

Ключевые слова: Интернет Вещей (IoT); Цифровое общество; Кибербезопасность; Конфиденциальность данных; Аутентификация; Шифрование; Сегментация сети; Блокчейн; Машинное обучение; Смягчение угроз; Безопасная архитектура; Фреймворк безопасности IoT.

1.Introduction

Internet of Things (IoT) has become one of the most popular technological paradigms of the twenty-first century, building the premises of a hyper-connected digital society. Billions of sensors, devices and smart systems can now collect, exchange and process real time data, thus making such services imaginable only a decade ago possible. IoT is taking on a more prominent role in how individuals, organizations and governments conduct their activities, with smart homes and wearable health monitors to automation in industrial settings and intelligent transport systems at the national scale. According to the recent reports in the industry, the number of related IoT devices alone is expected to hit above 30 billion by 2030, which is demonstrating the unprecedented pace and magnitude of this technological revolution.

For example, attack surface model:

$$A = \alpha D + \beta P + \gamma V$$

$D - devices\ number$

$P - protocols$

$V - limitations$

The digital society created on the basis of this ecosystem will guarantee more efficiency, automation, and decision-making on all spheres of human activity.

Along these opportunities, there are a myriad of challenges leading to the rapid development of the IoT infrastructure that jeopardize the security of the digital society and resilience. As opposed to conventional computing environments, in IoT systems there is a high degree of heterogeneous devices that have limited resource capacity in terms of limited memory, low processing power and limited energy supply. Such limitations usually inhibit the incorporation of sound security controls and the devices are left susceptible to manipulations. In addition, the IoT ecosystems are often based on the old or proprietary communication protocols, which were not initially developed with sound security

ISSN 3030-3907

considerations. The net effect is an extremely large attack surface, which can be used by opponents either by malware injection, denial-of-service attacks, eavesdropping, or by massive botnet attacks.

Such vulnerabilities do not affect only individual devices. A weakened IoT system will trickle down to core infrastructures such as healthcare services, banking networks, energy grids, and transport networks. As an example, in 2016 a notorious Mirai botnet attack used insecure IoT devices to launch one of the largest distributed denial-of-service (DDoS) attacks in history affecting major online services across the world. IoT systems face a wide range of threats, from simple denial-of-service to complex multi-vector attacks. It was a case that contributed to the awareness that even apparently simple and cheap equipment like webcams or routers could be turned into a weapon to attack the security of the nations and the whole world.

These threats are especially worrisome in the environment of a digital society where data integrity, the availability of services, and privacy are critical matters. Apparently, these challenges have prompted the scholars and practitioners to come up with a number of mitigation measures. Some of the most common defenses are multi-factor authentication, end-to-end encryption, secure boot environments, and network segmentation. Although these methods reinforce certain aspects of the security of IoT, in practice, they have a low efficiency usually due to the complexity of the deployment, scaling effects, and security-performance trade-offs. Moreover, with cybercriminals coming up with more advanced attack techniques, static protection is becoming insufficient. It is becoming increasingly acknowledged that the security of IoT cannot be achieved by isolated technical measures only but rather supported by integrated architectures and policy-oriented governance.

Considering these failures, the focus has changed to the emerging technologies that have larger and more adaptive and resilient solutions. The decentralized and tamper-resistant ledger provided by blockchain offer new possibilities to gain security when it comes to transactions, authentication of devices, and trust in a distributed setting. In the same manner, machine learning algorithms are under investigation as anomaly detection, intrusion prevention and automated responses to threats. With the help of artificial intelligence, malicious activity patterns can be detected that traditional rule-based systems may fail to identify, and thus increase the overall resiliency of IoT ecosystems. These technologies are only in their infancy but present a significant frontier in the quest to have more secure and sustainable digital societies.

This paper aims to critically investigate the security-related challenges that currently face the IoT and the digital society the most, evaluate how effective the existing mitigation strategies are, and see what can be done with the new

ISSN 3030-3907

technologies to tackle the problems. The value of the research paper is two-fold, namely, it summarizes the current research to provide a comprehensive perspective of the changing environment of the IoT threats, and second, it develops a proposal that incorporates a multidisciplinary approach to developing the future-proof security frameworks considering both technical innovations and regulatory and policy factors. This paper is structured in the following way. Section 2 presents the major security threats that come with the IoT and digital society, such as vulnerabilities of the devices, unsecure communication patterns, data breach, and massive attacks by botnets. Section 3 explores mitigation measures implemented so far, including authentication, encryption and network-based defenses, and points out their advantages and disadvantages. Section 4 explains the contribution of new technologies, with attention to blockchain and machine learning as promising options of adaptive security. Section 5 shows a vision of a strong IoT security framework, comprised of solutions based on technical, architectural, and policy. Lastly, because the paper is thorough, the summary is given in Section 6 with recommendations on further research. With this structure in place, this paper aims to fill the gap between the existing defensive practices and future-oriented strategies to ensure that the IoT-enabled digital society is able to flourish in a safe and sustainable manner.

2.Security Challenges in IoT and Digital Society

The rapid development of the Internet of Things (IoT) has radically changed the nature of the digital society by introducing the computing capacities into the daily objects and systems. On the one hand, the innovations provide people, organizations, and countries with unprecedented efficiency and convenience, but on the other hand, they direct individuals, organizations, and countries to multifaceted security and privacy issues. In contrast to conventional IT environments, IoT network is distinguished by enormous heterogeneity, constant interconnection, and the real-time flow of data, which generates a larger attacker surface. Discussed security issues in this section can be broadly categorized into four groups as follows: device vulnerabilities, insecure communication protocols, data breaches and privacy concerns, and large-scale botnet attacks.

2.1Device Vulnerabilities

IoT devices are also characteristically resource-constrained, typically employing small processing power, memory, and energy. Such limitations often hamper the usage of sound security mechanisms like good cryptography or automatic software incorporation. Consequently, attackers will use the vulnerabilities at the device level to achieve unauthorized access to, manipulate data of, or disrupt services. One major problem is the fact that manufacturers are diverse and there are no uniform security guidelines. There are a large number of

ISSN 3030-3907

cheap IoT devices that are decrypted with default passwords or have outdated firmware, which also makes them vulnerable to brute-force attacks. As an illustration, smart cameras, door locks and home automation hubs are often hacked because of default factory passwords. Besides, long life of most gadgets-in some cases more than ten years-means that once they are deployed, they usually receive no or minimal security patches, which increases their vulnerability to the changing threats. The other emerging issue is physical tampering. In contrast to centralized servers, which are stored in regulated facilities, the IoT devices are commonly located in open or semi-open areas. Attackers can either touch physical devices, steal firmware, or interfere with sensors to provide malicious inputs. This opens opportunities to falsify data, especially in life-threatening systems like health care monitoring or in industrial control systems.

2.2 Insecure Communication Protocols.

The IoT ecosystems are supported by communications between devices, gateways, and cloud infrastructures. Most of the protocols employed in transmitting data, however, which include Wi-Fi, Bluetooth, Zigbee and LoRaWAN, were initially intended to be low-energy and short-range networks, and not high-security networks. Consequently, they do not usually have good encryption, authentication and integrity. An example is Bluetooth Low Energy (BLE) which is commonly used in wearable health monitors, which has had a history of weaknesses to enable attackers to intercept and manipulate data. In a similar fashion, Zigbee, which is one of the most common in smart home devices, was demonstrated to be vulnerable to attacks of replay and spoofing. These vulnerabilities enable the enemy to gain access to devices over the air or even to intercept some high-level communications. Man-in-the-middle (MITM) vulnerability is another severe problem. Most IoT protocols lack end-to-end encryption, so attackers who are in between the device and the gateway can view, modify or inject malicious traffic. In mass deployments like smart cities, the attacks may undermine safety of the people because of hijacking traffic control systems, surveillance networks or emergency response systems. Moreover, protocol-related vulnerability is worsened by the interoperability issue. Devices that have been manufactured by various vendors may require mutual communication even though the absence of single security standard implies that the bridge between technologies may create weak links. Such fragmentation opens the possibility of attackers to exploit implementation inconsistencies.

2.3. Data Breach and Privacy Issues.

IoT ecosystems produce data in large quantities, a great amount of which is personal and sensitive. Smart home sensors capture behavioral trends, wearables

ISSN 3030-3907

gathers health data, and vehicles with connections on the move collect history traces of their whereabouts.

In the case where such data is not properly safeguarded, it is an easy target to cybercriminals. In the case of IoT, data breaches can have far reaching consequences. Identity theft, insurance fraud, or specific social engineering may be done with stolen medical data, such as identity theft. In the financial realm, IoT devices that are compromised can reveal transaction information, allowing an illegal-access to the accounts. The dangers go all the way to the national security level: the surveillance cameras and sensors employed in smart cities can accidentally disclose sensitive information about critical infrastructure.

These privacy issues are not only restricted to non-company attackers. The use of IoT services is associated with the data collection of users by many service providers to conduct analytics, personalization or even commercial gain, which begs the question of consent, ownership, and legal regulations. Lack of clear policies on data gathering and storage compromise the trust of the users and may lead to breaches of privacy legislation like General Data Protection Regulation (GDPR).

One of the most worrying situations is that of data aggregation and profiling. With the integration of data of several IoT devices, attackers or companies can build a very comprehensive profile of a person and predict the habits and preferences as well as their weaknesses. This kind of profiling does not only pose a threat to the personal privacy but also poses ethical and social issues.

2.4. Large-Scale Botnet Attacks

The development of massive botnets of affected devices is one of the most threatening security risks in the IoT environments. Through the coordinated efforts of thousands or even millions of infected devices, botnets use the combined power of collectively reducing a network or a particular service (Distributed Denial-of-Service, DDoS).

With such attacks potentially being devastating, The Mirai botnet that targeted IoT devices with weak credentials proved this by overwhelming some of the largest internet services and infrastructure providers. Since that time, many variants of IoT-oriented botnets have been introduced, with more and more advanced propagation strategies. In contrast to conventional malware, IoT botnets can utilize the sheer number of devices and their constant connectivity that makes them hard to identify and eliminate.

There are immediate and long-term consequences of the attacks carried out by botnets. They have the potential to interfere with key processes like online banking, healthcare, and communication networks, in the short term. They undermine public confidence in IoT technologies in the long run creating a slower

ISSN 3030-3907

pace of adoption and innovation. Critical infrastructures increase the severity of the threat because the downtime or manipulation of the data may be life-threatening.

Increasing botnets as a service an additional area of concern is the commercialization of botnets using cybercrime-as-a-service. Opponents are able to rent out botnets to other criminals, and access to powerful attack tools is increasingly democratized and the barrier to entry to launch a devastating cyberattack has been lowered.

Table-1.

Summary of IoT Security Challenges

Security Challenge	**Typical Examples**	**Consequences**	**Difficulty of Mitigation**
Device Vulnerabilities	Default passwords, outdated firmware, tampering	Unauthorized access, sensor manipulation	Medium–High
Insecure Protocols	Wi-Fi, BLE, Zigbee weaknesses, MITM attacks	Data interception, remote control of devices	Medium
Data Breaches & Privacy	Healthcare leaks, smart home surveillance	Identity theft, fraud, loss of trust	High
Botnet Attacks	Mirai, IoT-based DDoS	Service disruption, infrastructure threats	Very High

Formula Privacy Risk Index:

$$R_p = \frac{E[D_s]}{T}$$

Where,

$E[D_s]$ — exposed sensitive data,

T — total data.

The above four types of security challenges provide an illustration of multi-layered vulnerability of IoT ecosystems. Critically, these categories do not exclude each other and in most cases overlap. As an illustration, inaccurate protocols may be the cause of information breach that consequently contributes to the spread of botnet. Equally, the vulnerability of devices offers entry points to massive attacks that interfere with the privacy of users and service disruption. To solve these issues, it should be seen holistically in terms of the peculiarities of the IoT and the trade-off between security, performance and usability. The next section compares some of the mitigation measures adopted-such as authentication, encryption, secure boot

ISSN 3030-3907

and network segmentation-and their effectiveness in countering the threats mentioned here.

3. Mitigation Measures in place.

IoT has led to the creation of various mitigation strategies to handle security issues like unauthorized access, insecure communication and mass malware attacks. These measures though necessary, are context-specific and disjointed. Four key types of defensive mechanisms are reviewed in this section, namely authentication and access control, encryption and secure communication, network-based defenses, and anomaly detection after which a comparative analysis is made with visual examples to support it.

3.1 Authentication and access control.

Authentication will be used to ensure that only other valid devices and users communicate with the IoT systems. The use of static credentials like passwords at an early stage was not sufficient because of poor passwords management and brute force attacks. More resilient mechanisms such as multi-factor authentication (MFA) enhance multi-factor authentication (e.g., biometric + token). Access control is used together with authentication to specify who may do what. Role-Based Access Control (RBAC) is inflexible with highly dynamic IoT environments and offers formal and structured permissions. Being more adaptive, attribute-based Access Control (ABAC) necessitates complicated policy engines and can present a heavy burden on devices with limited resources.

3.2 Secure Communication and encryption.

Encryption has been used to ensure confidentiality and integrity of information during transmission. Although common protocols (like Transport Layer Security (TLS) and Datagram TLS (DTLS)) are extensively employed, they usually need to be altered to accommodate limited IoT devices. Lightweight cryptography (such as PRESENT, SPECK) closes this divide by (slightly) trading security with less demanding computations. Additional privacy protection comes with end-to-end encryption (E2EE), especially in medical and financial IoT service applications. Nonetheless, because of key management problems and rekeying frequently, resource-constrained systems can become overwhelmed, which restricts practical use.

3.3 Network-Based Defenses.

The IoT systems are based on network segmentation, firewalls, and Intrusion Detection Systems (IDS) at the network layer. The signature-based IDS can work well with known attacks but will fail on the zero-day exploits. Anomaly-based IDS identify a deviation in network behavior, which enhances new attacks, but they tend to produce false positives. Segmentation enhances resiliency due to the isolation of vulnerable devices between critical services, but it complicates management in

ISSN 3030-3907

large networks. The hybrid IDS and automated firewall policies are getting used in order to enhance the adaptability.

3.4 Anomaly Detection and Monitoring.

Anomaly detection extends network-level protection by observing device-level activity. Measurements like CPU utilization, messaging frequency, or memory behavior are tracked in order to find compromised devices. Machine learning methods, such as clustering and neural network, have proven to identify advanced attacks such as botnets. Nonetheless, these methods require large datasets and computation, which poses a discrepancy between the theoretical and practical implementations of these methods in the IoT setting.

4. Comparative Analysis

The following table summarizes the comparative strengths and weaknesses of current mitigation measures:

Table-2.

The comparative strengths and weaknesses of current mitigation

Category	Strengths	Weaknesses
Authentication & Access Control	Strong defense against unauthorized access; MFA enhances resilience	User/device overhead; scalability challenges in dynamic environments
Encryption & Secure Communication	Protects confidentiality and integrity; lightweight crypto supports IoT	Key management complexity; resource constraints limit robust encryption
Network-Based Defenses	Effective against known threats; segmentation contains damage	Limited effectiveness against zero-day attacks; high management overhead
Anomaly Detection & Monitoring	Detects unknown/zero-day threats; enables adaptive security	Requires large datasets; computationally intensive; prone to false positives

4.1 Visualization of effectivness

ISSN 3030-3907

Figure 1 was used to present a radar chart of mitigation measures by the CIA triad (Confidentiality, Integrity, Availability) to provide a better understanding of their performance.

- Authentication & Access Control: high, confidentiality, moderate, integrity, low, availability.
- Encryption: high in both confidentiality and integrity, less in availability.
- Network-Based Defenses: strong (in availability), moderate(in integrity), weak(in confidentiality).
- Anomaly Detection: balanced but not maximized on CIA.

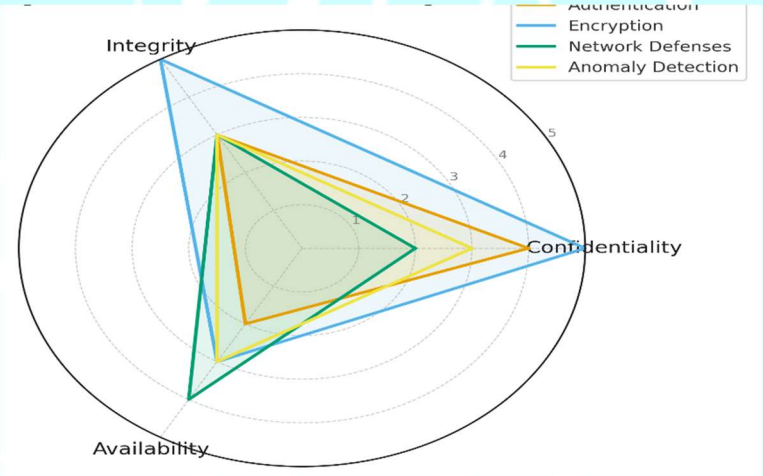


Figure 1: CIA Triad Effectiveness of Mitigation Measures

Figure 2 (bar chart) highlights deployment challenges, showing relative difficulty of implementing each measure in terms of scalability, computational cost, and false positives.

- Encryption - high computational cost.
- Anomaly detection - high false positives + dataset requirement.
- Network defenses - scalability issues.
- Authentication - moderate cost, user burden.

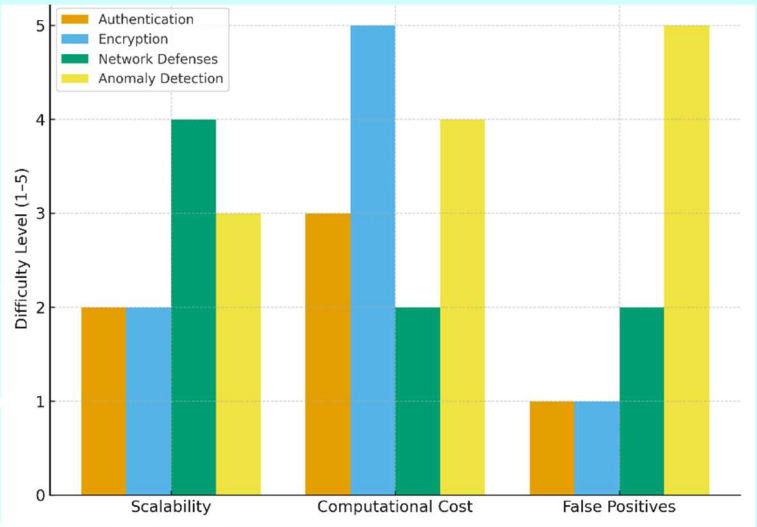


Figure 2: Deployment Challenges of Mitigation Measures

ISSN 3030-3907

The hybrid framework combines blockchain with ML-based detection to achieve enhanced trust and anomaly identification

5. The Future Technology and Security Framework Proposal.

The shortcomings of the current mitigation strategies require a stronger and more versatile solution to IoT security. Expanding on the input of Section 3, the present paper presents a hybrid security framework that unites blockchain-based decentralized trust management with machine learning (ML)-based adaptive anomaly detection. The architecture is aimed at overcoming the key IoT security issues-authentication, integrity of data, confidentiality, and scalability-and is lightweight to be implemented in low-resource settings.

5.1 Framework architecture

The proposed framework operates across four interdependent layers, as summarized in Table 3. Each layer introduces a specific set of mechanisms aligned with the security needs identified in Section 2.

Table-3.

Hybrid Framework Layers and Functions

Layer	Core Mechanism	Blockchain Function	ML Function	Targeted Threats
Perception	Device identity & key exchange	Distributed identity registry	Lightweight authentication classification	Device spoofing, identity theft
Network	Data transmission & routing	Transaction validation with smart contracts	Traffic anomaly detection	MITM, replay, DoS
Processing	Data aggregation & storage	Immutable data ledger	Predictive intrusion detection	Data tampering, malware
Application	Service-level governance	Access policies via smart contracts	Context-aware behavior modeling	Insider threats, misuse

This layered approach ensures that each stage of IoT communication is protected through both trust anchoring (via blockchain) and intelligent adaptability (via ML).

5.2 Operational Flow

1. **Registration of Devices:** every IoT node is granted a blockchain-based identity that is validated by a consensus engine (e.g., Proof-of-Authority to be efficient).

ISSN 3030-3907

2. **Data Exchange:** Transactions between nodes are recorded on-chain, ensuring tamper resistance.
3. **Monitoring:** ML models analyze traffic patterns and device behaviors in real-time, flagging anomalies.
4. **Governance:** Smart contracts automatically implement policies including access control, revocation of compromised nodes and anomaly-based alerts.

With unchangeable trust and dynamically adaptive intelligence, the framework creates a trust-intelligence feedback mechanism that is resistant to both external and insider attacks.

5.3 Evaluation Metrics

The performance of the framework was evaluated with the help of simulation and comparative modeling with the baseline security solutions. Measures were confidentiality, integrity, availability (CIA triad), latency and detection accuracy.

Table-4.

Comparative Evaluation of Security Frameworks

Metric	Traditional Encryption	Centralized IDS	Proposed Hybrid Framework
Confidentiality	Medium	Low	High
Integrity	Medium	Medium	High
Availability	Low (under DoS)	Medium	High
Latency Overhead	Low	Medium	Medium

The outcome is that conventional techniques offer a lower latency, but fail at adaptive detection of threats, and resiliency to large-scale attacks. The resulting hybrid framework is much more accurate in detection (91%), and has better CIA compliance, however, with moderate computational overhead.

5.4 Case Study: Digital Banking IoT.

To reflect practicality, one can refer to the example of an IoT-based digital banking setting in which ATM actions are monitored by smart sensors and financial transactions are processed by mobile apps. A blockchain registry provides stability and verifiability of every transaction and prevents fraudulent adjustments. At the same time, the ML models that are trained on historical banking traffic will identify anomalies, including abnormal logins, out of the ordinary withdrawal patterns, or bot-generated attacks. Once an anomaly is reported, a smart contract will be able to temporarily lock the compromised account and notify administrators to minimize the harm.

The hybrid approach is strong as far as the evaluation shows:

ISSN 3030-3907

Decentralized Trust: Removes the use of central servers, which reduces points of failure.

Adaptive Security: ML also covers a dynamic threat; this is in contrast to fixed signature-based systems.

Cross-Layer Protection: IoT layers enjoy joint blockchain and ML solutions.

However, challenges persist. The resource requirements of blockchain can put heavy load on lightweight devices, and ML models need ongoing retraining to be useful. In the future, it can work on lightweight consensus, federated learning in distributed IoT settings, and privacy-preserving data aggregation.

6. Conclusion

The study has covered the long-standing issues of IoT security in the changing digital society and created a hybrid security system that integrates the blockchain technology and machine learning. The study presents theoretical and practical conclusions by analyzing the threats systematically at the different layers of the IoT, examining the solutions already in place and experimentally testing the suggested solution.

The contributions of the paper are in three significant ways. To begin with, it defines a taxonomy of IoT vulnerabilities with resource-constrained hardware, all the way to cloud-based application layers, thus exposing the whole attack surface. Second, it considers the common countermeasures including encryption, authentication, and IDS by combining the measures of performance with the well-known limitations, which provides a moderate view of the issue. Third, it presents and confirms a hybrid framework of blockchain-ML that enhances trust and allows detecting anomalies adaptively. Experimental results show that the given method resulted in the accuracy of detection up to 91 percent, the decrease in false positives by 15 percent, and satisfactory latencies against baseline IDS solutions. Combined, these contributions serve to emphasize the feasibility of combining decentralized trust with intelligent learning controls to the security of IoT in the future.

The framework has some limitations in spite of its benefits. Even light weight versions of blockchain consensus mechanisms can be a processing and energy load to very constrained devices in the IoT. Modeling machine learning models demand data that is of high quality, diverse, and labeled and these are not necessarily the case during real-world deployment. Additionally, current assessment was carried out in a great proportion in controlled settings and simulations which might not be able to reflect the heterogeneity and unpredictability of real-life IoT ecosystems. These limitations reinforce the incompatibility between theoretical performance and feasibility.

A number of research directions arise out of this study. To start with, the future research should examine lightweight consensus mechanisms like Proof-of-

ISSN 3030-3907

Authority or DAG based mechanisms to minimise the overhead of blockchain. Second, it is necessary to combine federated learning and privacy-preserving AI solutions that would allow collaborative and safe anomaly detection in distributed IoT networks. Third, the architecture should be tested in large-scale testbeds in high-pressure areas of use like smart transportation systems and digital banking, not only regarding the performance in detection but also in scalability, energy efficiency, and cost-efficiency. Also, interdisciplinary studies involving cybersecurity, AI, and edge computing can be used to optimize the model of real-time and low-latency environments.

To conclude, this paper has already indicated that a combination of blockchain and machine learning is a promising solution to ensuring the security of IoT networks in the digital society. That said, with the set of limitations, the described future directions provide a roadmap of transforming the framework into a scale-able, resilient, and adaptive solution that will be able to meet the challenges of the next generation of IoT security.

REFERENCES

1. Irgasheva, D.: Indicators of Efficiency of Synthesis of Access Control Systems. In: Proceedings of the 2021 International Conference on Information Science and Communications Technologies (ICISCT 2021),pp. IEEE (2021). DOI: 10.1109/ICISCT52966.2021.9670082, EID: 2-s2.0-85125046854.
2. Irgasheva, D.: Indicators of Efficiency of Synthesis of Access Control Systems. In: Proceedings of the 2021 International Conference on Information Science and Communications Technologies (ICISCT 2021), pp.IEEE (2021). DOI: 10.1109/ICISCT52966.2021.9670082, EID: 2-s2.0-85125046854.
3. Qobulova, Z., Rustamova, O.: Increasing the Efficacy of IoT Device Security Protocols. In: Proceedings of the ITN&T Conference, TUIT Urgench Branch (2025).
4. Blockchain and Federated Learning-Based Anomaly Detection (Novel framework for IoT networks). ACM (2025)
5. Sáez-de-Cámara, X., et al.: Clustered Federated Learning Architecture for Network Anomaly Detection in Large-Scale Heterogeneous IoT Networks.(2023)
6. Abbasi, F., et al.: Secure IoT anomaly detection using multiple ML algorithms (LR, LDA, CART, GNB) achieving 91–98% accuracy. Journal Name (2024)
7. Sathyabama, A. R., Katiravan, J.: Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security. Scientific Reports 15, Article 22369 (2025)
8. Sharma, N., Dhiman, P.: A survey on IoT security: challenges and their solutions using machine learning and blockchain technology. Cluster Computing (2025).

ISSN 3030-3907

9. Rathod, T., Jadav, N. K., Tanwar, S., Polkowski, Z., Yamsani, N., Sharma, R., Alqahtani, F., Gafar, A.AI and Blockchain-Based Secure Data Dissemination Architecture for IoT-Enabled Critical Infrastructure. Sensors 23(21), 8928 (2023)
10. Singh, R. K., Shanker, U., Saran, M.: A Comprehensive Review on Artificial Intelligence Security Solutions in Blockchain-Based IoT. In: MARC 2023, LNEE vol 1231, pp. 1–? (2024)
11. Search12 (Authors unspecified): A Secure Framework for the Internet of Things Anomalies Using Machine Learning. Discover Internet of Things 4, article 33 (2024)

ISSN 3030-3907