https://doi.org/10.31891/csit-2026-2-11

UDC 004.9

PROTECTED LOCAL ACCESS BASED ON PHYSICALLY-DETERMINISTIC LINKS

Volodymyr KYSIL
PHD Student of Computer Engineering & Information Systems Department, Khmelnytskyi National University
https://orcid.org/0009-0003-9387-6609
E-mail: vovikusspambox@gmail.com
Tetiana KYSIL
Candidate of Physical and Mathematical Sciences, Associate Professor of Computer Engineering & Information Systems Department, Khmelnytskyi National University
https://orcid.org/0000-0002-4094-3500
E-mail: kysil_tanya@ukr.net

This article proposes an approach to organizing protected local access based on physically-deterministic links for intelligent medical diagnostic systems. The relevance of this study is driven by the necessity of ensuring confidential remote access to local computing resources operating within isolated networks or behind restrictive systems, such as NAT. The developed approach is based on the concept of a "blind" registry and out-of-band key transmission via physical media, such as QR codes or their analogs, enabling a zero-knowledge access model. Information interaction is protected by implementing physically-deterministic links that combine temporary tunnels with a mechanism for local metadata decryption in the user's browser using the Web Crypto API.This approach eliminates the possibility of data compromise at the network infrastructure provider level and ensures confidentiality without requiring centralized key management systems (KMS), which is vital for autonomous nodes and ease of use. The practical significance of the method is integrated into the general concept of automated diagnostic and consultation information technology, providing secure remote calls to neural network models deployed on local computers or servers. The proposed solution is the subject of ongoing research aimed at minimizing hardware requirements while maintaining high levels of access simplicity and setup for patient data access.

The practical significance of the approach is confirmed by its successful integration into information technology for medical consultative diagnostics. The proposed solution allows for the utilization of powerful local resources for medical image processing without the costs of expensive cloud infrastructure. The obtained results demonstrate high system resilience to network constraints (NAT, dynamic IPs) and ensure a high level of security for patient data.

Prospects for further development involve transitioning to direct connections via WebRTC Data Channels using specialized servers for NAT "hole punching" according to the STUN standard. This will allow for the encapsulation of HTTP(s) traffic directly into a P2P channel, where the registry and signaling gateway act exclusively as initial coordination nodes. Such a shift will further enhance the autonomy and speed of consultative-diagnostic processing.

Keywords: Information technology, protected access, physically-deterministic links, blind registry, zero-knowledge

Received: 08/04/2026
Accepted: 20/05/2026
Published: 31/05/2026

Introduction

In the context of intensive digitalization in the healthcare sector, the volume of diagnostic data – specifically fundus images and optical coherence tomography results – is growing exponentially. The dynamics of data accumulation in the central EMR (Electronic Medical Record) database indicate a rapid increase in load: while at the beginning of 2024, the total number of electronic medical records stood at 2.5 billion [**Помилка! Джерело посилання не знайдено.**], by April 2026, this figure reached nearly 5.3 billion [2]. Despite this surge in information, most existing developments in automated diagnostics remain "niche" solutions due to high infrastructure costs and the complexity of integration into existing clinical processes [3]. Consequently, as noted in research regarding sovereign AI and edge computing [4], there is a critical need to create personalized systems that provide automated information processing directly on local capacities with minimal resource expenditure.

The issue of security when providing mass access via open network portals is also of particular importance. It is necessary to develop methods for direct, simplified communication that function outside the boundaries of rigid centralized control. Specifically, in [14], P. Anbil notes that a primary prerequisite for implementing such solutions is the rapid

growth of cyber threats within the Medical Internet of Things (IoMT), requiring network exposure minimization to protect critical medical devices and data. For example, as stated in the U.S. Department of Justice regulations on the protection of bulk sensitive data [15], modern standards for accessing confidential information require the implementation of enhanced protection mechanisms for medical and biometric indicators directly at the architectural level of information systems. In the information context, this necessitates flexible models of confidential interaction, where the architectural "ephemerality" of the connection allows for the separation of technological support from professional specialist work, ensuring balanced management of the parties' responsibilities.

The general problem in deploying local diagnostic nodes is ensuring the security of open access points and the difficulty of configuring them to establish a direct connection. Common architectures face several formalized obstacles, such as the use of dynamic IP addresses, servers operating behind NAT mechanisms, and strict firewall settings. These factors prevent direct network visibility of a local computing server from external networks, requiring the development of alternative approaches to addressing and traffic routing in distributed information systems.

The primary goal of this work is the scientific substantiation of the autonomy of local medical servers and the development of new remote access methods adapted for use by personnel without specialized technical training. The emphasis shifts toward ensuring "operational intuitiveness," where the complexity of cryptographic and network manipulations is entirely hidden from the end-user, allowing them to focus on the diagnostic process and providing consultative assistance. This work builds upon previous research in ML-diagnostics [16] and the construction of decentralized architectures for medical records [17].

Related works

At the current stage of network technology development, a significant number of solutions for providing remote access exist; however, most of them have substantial limitations when implemented in autonomous medical systems. Specifically, as P. Anbil argued in [14], traditional connection models for Medical Internet of Things (IoMT) devices often ignore the necessity of network exposure minimization. This creates critical vulnerabilities to modern cyber threats, as broad attack vectors on medical infrastructure make standard remote access methods insufficiently reliable for protecting sensitive patient data. Consideration of common tunneling tools such as Cloudflare Tunnel, ngrok, and zrok demonstrates their effectiveness for rapid publication of local services, but in the context of free tiers, they create obstacles for mass use. In particular, bandwidth limitations and mandatory interstitial pages for browser verification, characteristic of free tiers of popular tunneling services, create significant barriers to the stable operation of diagnostic interfaces. As noted in [5], the complexity of initial configuration and the need to administer third-party access tokens form a high technical threshold for personnel without specialized training. This leads to a "usability gap," where the excessive complexity of network setup negates the advantages of the technology itself. Given current trends toward simplifying communication architectures through the transition to P2P connections [6], the use of third-party tunneling solutions remains only a partial workaround that does not satisfy the requirements for full autonomy of local medical nodes. Moreover, direct dependence on the stability of a third-party provider contradicts the requirements for operational autonomy, which are necessary for the availability of local computing nodes in this manner. Therefore, for this system, it is necessary to create an approach that can leverage the advantages of existing systems and ignore their disadvantages, with the possibility of transitioning to maximum autonomy, which is a logical development of previous research in the field of intelligent medical diagnostics [16].

Analysis of Zero-Knowledge methods and approaches to "blind" addressing opens possibilities for creating systems with a high level of access granularity. Specifically, as argued in the regulations on the protection of bulk sensitive data [7], the implementation of reinforced architectural security measures for medical and biometric indicators is crucial for preventing unauthorized access at the infrastructure level. This allows for the realization of a model where authority verification occurs without disclosing the content of the data themselves, ensuring compliance with requirements for minimizing the transmission of sensitive information in the clear. Unlike classic models, where the server address is a publicly known stable point, an approach using encrypted metadata in public registries allows for the implementation of the concept of separation of responsibilities [9]. In such a model, access to secret keys and addresses becomes possible only in the presence of a physically-deterministic link, which acts as a trusted channel for connection initialization. Specifically, as M. Garcia argued in [8] using the example of the QWBP protocol (QR-WebRTC Bootstrap Protocol), the use of a QR code as an out-of-band means for transmitting signaling parameters effectively allows for hiding the internal network structure from external adversaries. This ensures the establishment of a direct P2P connection even in isolated or "air-gapped" environments, maintaining low infrastructure overhead. The economic justification for such an approach lies in the use of free public resources (KV-storages, Gist) as blind intermediaries, ensuring zero infrastructure costs while maintaining a professional level of security.

When compared to centralized Key Management Systems (KMS), such as solutions from AWS or Google Cloud, their architectural vulnerability in the context of providing decentralized access becomes apparent. This was clearly illustrated by events in the Middle East in March 2026, when a kinetic attack on Amazon Web Services (AWS) data centers in the UAE and Bahrain [10] paralyzed the operation of numerous banking and government systems. As argued in [11], this incident demonstrated the failure of standard cloud redundancy mechanisms (Multi-AZ) to withstand the physical destruction of infrastructure nodes, leading to large-scale disruptions in civil services [12]. Thus, full dependence on centralized KMS makes information systems vulnerable to global-level physical threats,

justifying the transition to autonomous local key management models. Centralized KMS require a constant internet connection for credential verification and often rely on expensive Hardware Security Modules (HSM), which are absent in typical clinical or educational environments. Instead, the proposed approach is oriented toward decentralized management, where decryption keys are generated and stored exclusively locally. This ensures system resilience to external failures and guarantees the privacy of medical data in accordance with modern regulatory standards. Specifically, in [15], it is argued that the protection of bulk sensitive data requires the implementation of architectural tools that prevent unauthorized access to biometric and medical indicators at the infrastructure level. Such an approach allows for the implementation of an autonomous functioning model without dependence on cloud services. As described in [17], the use of decentralized physician-oriented architectures with local cryptographic protection is critical for ensuring the authenticity and confidentiality of records in Electronic Health Record (EHR) systems operating outside of centralized cloud control.

Methodology

The developed methodology for constructing the information technology is based on a combination of ephemeral tunneling methods and physically-deterministic addressing. In contrast to common remote access solutions, such as cloud tunnels (e.g., Cloudflare Tunnel or ngrok) and traditional VPN gateways [5, 6], the proposed approach involves the complete elimination of a centralized Key Management System (KMS). Identification, decryption, and session management functions are transferred directly to the client side, which architecturally ensures high autonomy for local computing stations. This model enables the implementation of secure external access without dependence on the status of third-party authentication services, which is critical for the stable operation of systems in dynamic or isolated network environments.

System Requirements

The primary requirement for building the system is the necessity to provide remote access to a local computing node for users (physicians and patients) who do not have specialized technical training. Taking into account the specifics of medical data and the architectural constraints of local networks, several requirements have been established for the direct local access system: the "blind" registry requirement, requirements for the physical local link, and physical constraints.

"Blind" Registry Requirement: The public registry must function as a passive intermediary for indirect addressing. The core parameter is the complete lack of access by the registry to decryption keys or open server addresses. The registry must only accept encrypted objects (ciphertext), access to which is possible exclusively through an encrypted session hash or a key generated on the server side and transmitted to the patient through an out-of-band channel.

Physical Local Link Concept: A physical key carrier – a QR code (or any other method of physical information encoding) – is used to provide access. The primary requirement for this mechanism is the implementation of the "user simplicity" principle. The decryption key K must be integrated into the link such that it never leaves the patient's device when interacting with the public infrastructure. This enables physical delegation of access directly in the physician's office, establishing a trusted interaction loop.

The general structural diagram of the interaction between the information system components during the implementation of the proposed approach is shown in Fig. 1.

Technical Constraints and Network Isolation: The system must operate stably in the absence of a fixed public IP address and function at near-zero cost. The main constraint is working behind multi-level NAT mechanisms and active firewalls that block any incoming requests. The methodology stipulates that the server acts exclusively as the initiator of outbound connections, independently forming ephemeral access routes and publishing current metadata in the registry only for the duration of the active session. Additionally, the frequency of data updates in the registry must be limited to comply with free-tier limits provided by public platforms for automated access and editing operations.

Concept of the Proposed Information Technology

The logical structure of the proposed technology is based on the dynamic separation of signaling and transport channels. The primary architectural feature is the role of the local computing server as the active initiator of all network transactions, which allows bypassing inbound traffic restrictions without altering the network equipment configuration. Interaction between system components (server, "blind" registry, and client device) is implemented through a multi-level mechanism of indirect addressing (Fig. 2). This organization is aimed at automating diagnostics while maintaining low solution costs and providing mass access.

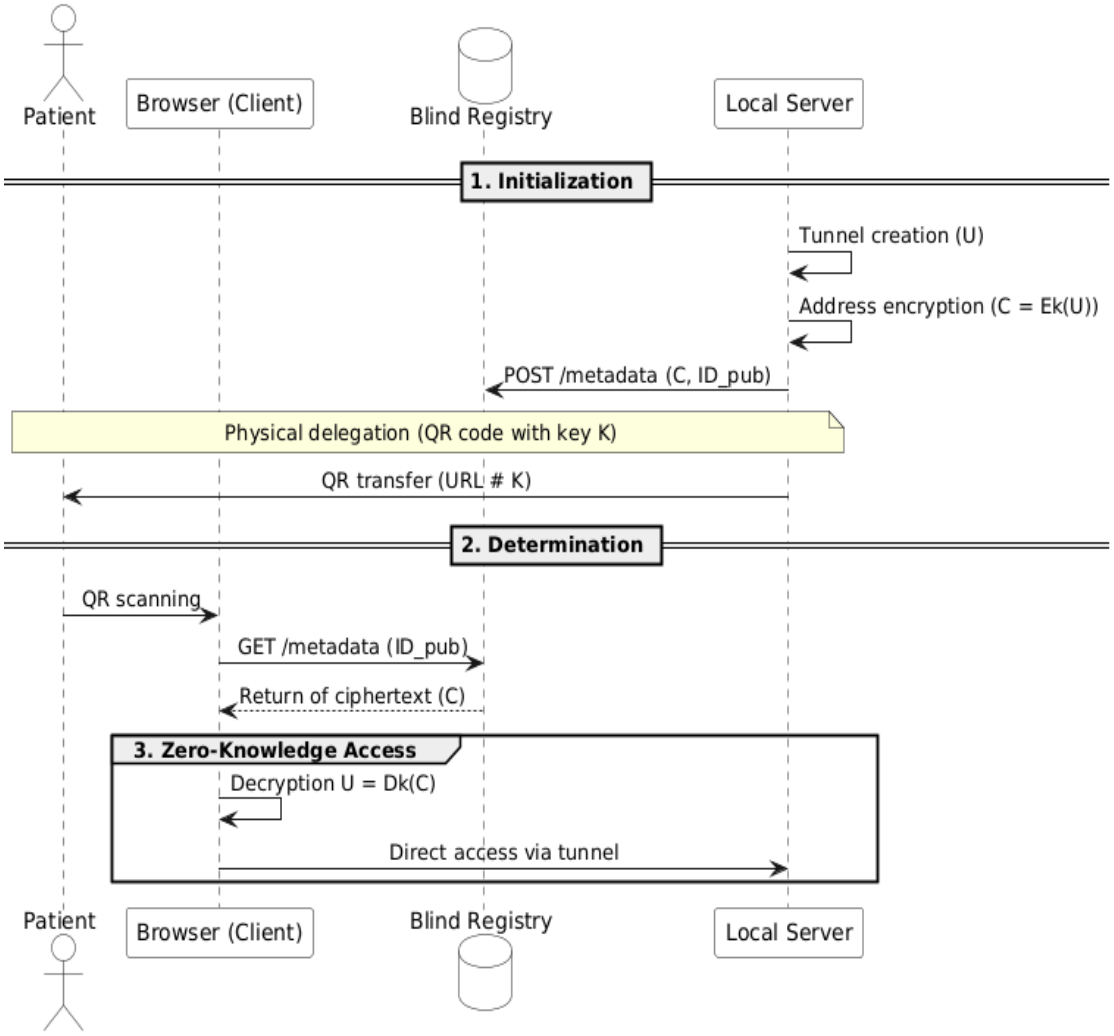

Fig. 1. Architectural model of secure access based on physically-deterministic links in a diagnostic system

The functioning method of the information technology includes four sequential steps:

Step 1. **Generation**: The server initiates the creation of an ephemeral tunnel via a third-party relay service, obtaining a temporary access address. This allows for hiding the real local IP address and providing a secure TLS channel for the transmission of medical images and other data.

Step 2. **Metadata Publication**: The obtained tunnel URL is encrypted using a symmetric algorithm with a session key K. The ciphertext is placed in a public registry under an identifier that is a salted hash of the server's unique token. In this process, the registry acts exclusively as a passive storage for binary data.

Step 3. **Physical Delegation:** A QR code is generated based on the key K and the address of a static decryptor website. This step is pivotal for establishing trust, as the transfer of access rights occurs during direct contact between the physician and the patient or the patient and a physical key located near the physician (e.g., on a door, which does not prevent the use of the link after its acquisition). This ensures transparency and the possibility of notification regarding data access.

Step 4. **Determination and Redirection**: After scanning the QR code, the client device loads a static JS interface that automatically requests the ciphertext from the registry. Using the key from the URL fragment (the key never leaves the device at all), the browser performs decryption of the actual tunnel address and proceeds to the diagnostic interface. This does not eliminate the need for user identification and protection of the system itself but rather complements these systems.

The reliability of the proposed approach is ensured by a multi-level protection system, where the mathematical justification for using URL fragments to transmit session keys occupies a central place. Since the part of the link following the fragment symbol (#key) is not transmitted by the client to the server during the metadata request, this guarantees full isolation of the key K from the registry's network logs, which corresponds to the concept of cryptographic "dead drops". Thus, the Zero-Knowledge principle is implemented using built-in and common browser tools for secure data decryption on the client side[13].

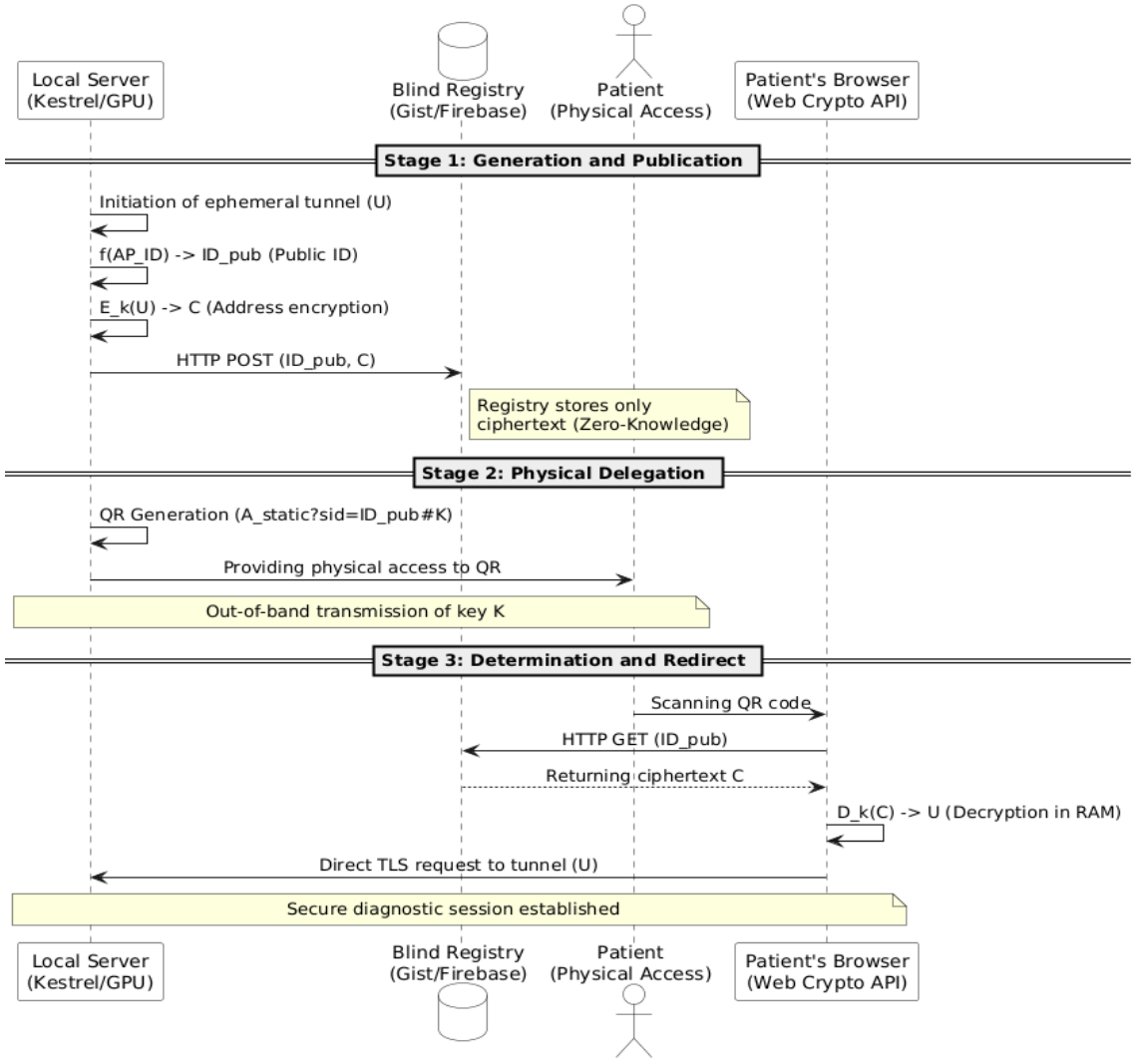

Fig. 2. Component interaction algorithm during connection establishment

Mathematical Formalization of the Process

To provide a formal description of the security of information interaction, let us introduce a set of basic notations. Let *U* be the ephemeral tunnel address, AP_{ID} be the unique internal identifier of the server's access point, and *K* be the symmetric session encryption key (AES-GCM). The process of establishing a secure connection involves three main stages:

1. Formation of a secure record in the registry (Server side).

The local computing node performs a unique cryptographic transformation f over the access point identifier to obtain the public session identifier ID_{pub}:

$$ID_{pub} = f(AP_{ID})$$

Next, the current tunnel address U is encrypted using the key K:

$$C = E_K(U)$$

where E is the encryption function, and C is the resulting ciphertext, which is uploaded to the registry under the key ID_{pub}:

$$Registry[ID_{pub}] \leftarrow C$$

2. Generation of a physically-deterministic link.

The physical link L, which is encoded into a QR code, is mathematically represented as the concatenation of the static gateway address A_{static}, the query parameter with the encrypted session identifier, and the link fragment with the key *K*:

$$L = A_{static} // \# // ID_{pub} // : // K$$

Due to the HTTP protocol specifications, when accessing address L, the values ID_{pub} and *K* do not appear in the network request:

$$\forall request \rightarrow A_{static}, keyK \notin HTTP\_Header, keyID_{pub} \notin HTTP\_Header$$

3. Determination of Access Address (Client Side).

After scanning the QR code, the patient's browser navigates to A_{static}. A script on the client side extracts ID_{pub} from the query parameters and sends a request to the registry to obtain C. Subsequently, decryption D is performed locally, utilizing the key K extracted from the URL fragment:

$$U = D_K(C) = D_K(E_K(U))$$

Due to the properties of the symmetric algorithm, the patient gains access to the diagnostic interface U. Simultaneously, for any external observer (including the registry and tunnel providers), the zero-knowledge condition is met:

$$P(revealU|accesstoRegistry) = P(revealU)$$

The use of built-in browser capabilities eliminates the need to load third-party cryptographic libraries, which increases trust in the system. The session key exists exclusively in the device's random access memory (RAM) for the duration of the active connection. The server's internal infrastructure is protected by limiting the access rights of the server-station (e.g., based on Kestrel) to the registry to Write-Only mode, preventing token leakage. The integrity of the session circuit is further controlled through mechanisms similar to previously developed hash chains and the addition of a separate actor/server for monitoring; however, this falls outside the scope of the current method.

Conclusions

This work proposes and scientifically substantiates an approach to organizing secure remote access to local computing nodes based on physically-deterministic links. The scientific novelty of the solution lies in the decentralized orchestration of ephemeral transport channels through out-of-band key transmission and unambiguous cryptographic transformation of identifiers. This alignment with the principles of modern initialization protocols via physically isolated channels enables a Zero-Knowledge model without the involvement of complex key management systems.

The practical significance of the approach is confirmed by its successful integration into information technology for medical consultative diagnostics. The proposed solution allows for the utilization of powerful local resources for medical image processing without the costs of expensive cloud infrastructure. The obtained results demonstrate high system resilience to network constraints (NAT, dynamic IPs) and ensure a high level of security for patient data.

Prospects for further development involve transitioning to direct connections via WebRTC Data Channels using specialized servers for NAT "hole punching" according to the STUN standard. This will allow for the encapsulation of HTTP(s) traffic directly into a P2P channel, where the registry and signaling gateway act exclusively as initial coordination nodes. Such a shift will further enhance the autonomy and speed of consultative-diagnostic processing.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

The authors' contributions are as follows: V. Kysil proposed the methodology for the decentralized doctor-centric architecture, designed the algorithms, and carried out the software implementation; T. Kysil supervised the study and determined the results validation strategy.

DECLARATION ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS

During the preparation of this work, the author(s) used Gemini for the purposes of translation, checking grammar and spelling, general formatting, and searching for relevant news for reference. After using this service, the author(s) reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

1. eHealth Ukraine. Про працездатність ЦБД ЕСОЗ: аналіз навантаження на систему. Офіційний портал eHealth, Січень 2024. URL: https://ehealth.gov.ua/2024/01/15/zvit-esoz-2023-summary/

2. eHealth Ukraine. В ЕСОЗ кількість електронних медичних записів сягнула понад 5 млрд. Офіційний портал eHealth, Квітень 2026. URL: https://ehealth.gov.ua/2026/04/09/v-esoz-kilkist-elektronnyh-medychnyh-zapysiv-syagnula-ponad-5-mlrd/

3. Anbil, P. Tackling Cybersecurity Threats in IoMT: The Case for Network Exposure Minimization. Medical Device & Diagnostic Industry, 2026. URL: https://www.mddionline.com/medical-iot/cybersecurity-threats-to-medical-devices-navigating-the-evolving-threat-landscape

4. Petronella Technology Group. Sovereign AI: Data Residency as Competitive Edge and Edge Computing for Sensitive Workloads. Petronella Blog, 2026. URL: https://petronellatech.com/blog/sovereign-ai-turning-data-residency-into-a-competitive-edge/

5. Sahani, A. Building Real-Time P2P Communication: A Deep Dive into WebRTC, ICE, STUN, and TURN. Medium Engineering, 2026. URL: https://akashsahani2001.medium.com/building-real-

time-p2p-communication-a-deep-dive-into-webrtc-ice-stun-and-turn-e645492230c5

6. Alakkad, S. 7 WebRTC Trends Shaping Real-Time Communication in 2026: From AI Integration to Media over QUIC. DEV Community, 2026. URL: https://dev.to/alakkadshaw/7-webrtc-trends-shaping-real-time-communication-in-2026-1o07

7. Blockchain Commons. Hubert: A Cryptographic Dead-Drop Architecture for Trustless Metadata Exchange. BCR-2025-006, 2025. URL: https://github.com/BlockchainCommons/Research/blob/master/papers/bcr-2025-006-hubert.md

8. Garcia, M. Breaking the QR Limit: QWBP (QR-WebRTC Bootstrap Protocol). magarcia.io, 2026. URL: https://magarcia.io/air-gapped-webrtc-breaking-the-qr-limit/

9. Al-Dallal, H. R. H., & Al Mukhtar, W. N. M. (2023). A QR code used for personal information based on multi-layer encryption system. International Journal of Interactive Mobile Technologies (iJIM), 17(9), 44–56. DOI: doi.org/10.3991/ijim.v17i09.38777

10. Data Centre Magazine. AWS Data Centre in UAE Hit in Iranian Strikes: Impact on Cloud Sovereignty. Data Centre Magazine, Березень 2026. URL: https://datacentremagazine.com/news/aws-data-centre-in-uae-hit-in-iranian-strikes

11. InfoQ. War in Iran Damages Multiple AWS Data Centers: Analysis of Multi-AZ Infrastructure Failure. InfoQ News, Березень 2026. URL: https://www.infoq.com/news/2026/03/aws-multiaz-conflict-outage/

12. MLQ.ai. AWS Outages from Drone Attacks Disrupt UAE and Bahrain Banking Services. Infrastructure & Security Report, 2026. URL: https://mlq.ai/news/aws-outages-from-drone-attacks-disrupt-uae-and-bahrain-banking-services/

13. MDN Web Docs. Web Crypto API: Symmetric encryption and decryption in the browser environment. [Online].

14. Anbil, P. Tackling Cybersecurity Threats in IoMT: The Case for Network Exposure Minimization. Medical Device & Diagnostic Industry, 2026. URL:https://www.mddionline.com/medical-iot/cybersecurity-threats-to-medical-devices-navigating-the-evolving-threat-landscape

15. U.S. Department of Justice. Regulatory Framework for Bulk Sensitive Data (Health & Biometric Data) Protection. Federal Register, 2025. URL:https://www.federalregister.gov/documents/2025/04/15/2025-07241/protection-of-sensitive-personal-data

16. Kysil, V., Popov, P., et al. Concept of Information Technology for Diagnosis and Prognosis of Glaucoma Based on Machine Learning Methods. CEUR Workshop Proceedings, Vol. 3675, pp. 171-181,2024.

17. KYSIL, V., & KYSIL, T. (2025). APPROACH TO A DECENTRALIZED PHYSICIAN-ORIENTED EHR ARCHITECTURE WITH CRYPTOGRAPHIC PROTECTION. Computer Systems and Information Technologies, (4), 18–26.URL: https://doi.org/10.31891/csit-2025-4-2

Володимир КІСІЛЬ, Тетяна КИСІЛЬ
Хмельницький національний університет

ЗАХИЩЕНИЙ ЛОКАЛЬНИЙ ДОСТУП НА ОСНОВІ ФІЗИЧНО-ШИФРОВАНИХ ПОСИЛАНЬ

У статті запропоновано підхід до організації захищеного локального доступу на основі фізично-детермінованих посилань для систем інтелектуальної медичної діагностики. Актуальність дослідження зумовлена необхідністю забезпечення конфіденційного дистанційного доступу до локальних обчислювальних ресурсів, які функціонують в умовах ізольованих мереж або за обмежувальними системами, зокрема NAT. Розроблений підхід базується на концепції «сліпого» реєстру та позаканальної передачі ключів через фізичні носії такі як QR-коди або аналоги, що дозволяє реалізувати модель доступу з нульовим розголошенням.

Захист інформаційної взаємодії забезпечується шляхом впровадження фізично-детермінованих посилань, що поєднують тимчасові тунелі з механізмом локального дешифрування метаданих у браузері користувача за допомогою Web Crypto API. Такий підхід виключає можливість компрометації даних на рівні провайдера мережевої інфраструктури та забезпечує конфіденційність без необхідності залучення централізованих систем керування ключами, що є важливим для автономних вузлів та простоти використання. Практична значущість методу включена в загальну концепцію інформаційної технології автоматизованої діагностики та консультування, де забезпечується безпечний віддалений виклик нейромережевих моделей, розгорнутих на локальних обчислювальних комп'ютерах або северах. Запропоноване рішення є об'єктом поточного дослідження та спрямоване на мінімізацію апаратних вимог при збереженні високого рівня простоти доступу та налаштування доступу до даних пацієнтами.

Практичну значущість підходу підтверджує його успішна інтеграція в інформаційні технології медичної консультативної діагностики. Запропоноване рішення дозволяє використовувати потужні локальні ресурси для обробки медичних зображень без витрат на дорогу хмарну інфраструктуру. Отримані результати демонструють високу стійкість системи до мережевих обмежень (NAT, динамічні IP-адреси) та забезпечують високий рівень безпеки даних пацієнтів.

Перспективи подальшого розвитку передбачають перехід до прямих з'єднань через канали даних WebRTC з

використанням спеціалізованих серверів для "hole punching" NAT за стандартом STUN. Це дозволить інкапсулювати HTTP(s) трафік безпосередньо в P2P канал, де реєстр та сигнальний шлюз виступатимуть виключно як початкові вузли координації. Такий перехід ще більше підвищить автономність та швидкість консультативно-діагностичної обробки.

Ключові слова: Інформаційні технології, захищений доступ, фізично-детерміновані посилання, сліпий реєстр, нульове розголошення.