КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.900
UDC 004.056.53:004.94

Volodymyr Avsiievych
Master's degree, Student of Information Technologies Faculty
Khmelnytskyi National University, Khmelnytskyi, Ukraine
ORCID ID: 0009-0004-2040-8756
avsiievychvr@gmail.com

Olga Pavlova
PhD, Associate Professor, Head of the Department of Computer Engineering and Informational Systems
Khmelnytskyi National University, Khmelnytskyi, Ukraine
ORCID ID: 0000-0001-7019-0354
pavlovao@khmnu.edu.ua

Ihor Mykhalchuk
Assistant Lecturer of Computer Engineering and Informational Systems Department
Khmelnytskyi National University, Khmelnytskyi, Ukraine
ORCID ID: 0009-0002-5162-5986
mykhalchukiv@khmnu.edu.ua

SECURITY FRAMEWORK FOR CYBER-PHYSICAL SMART PARKING SYSTEMS WITH AUTOMATED LICENSE PLATE RECOGNITION

Abstract. Smart parking systems with automated license plate recognition (ALPR) are getting more popular in cities, but they have serious cybersecurity problems. This study analyzes security threats in smart parking infrastructure and offers ways to reduce them via vulnerability assessments and improved security designs. We analyzed various attacks such as protocol exploits and data interception risks in cyber-physical parking systems. Our research studies RTSP camera communication vulnerabilities, REST API security problems, and cloud service integration risks in license number recognition systems using computer vision technologies. Our approach includes vulnerability testing, threat modeling with STRIDE framework, penetration testing, and security analysis. We studied problems of RTSP camera protocol, HTTP/HTTPS communications, Laravel REST API setup, and Google Cloud Vision API integration. Results show that smart parking systems may have data interception risks, unauthorized access, API security problems and system integrity threats, which need multi-layered security approaches. We designed a cyber-physical parking system prototype with improved security measures in all components. The prototype has good license plate recognition accuracy while applying security methods without major performance reduction. Important security factors include secure communication protocols, encrypted transmission of data, authentication frameworks, input validation, rate limiting, and logging systems. This research helps to understand cybersecurity facets in IoT-based parking systems and offers methods for secure automated vehicle recognition setup in smart cities. This work is truly relevant for Ukrainian smart city projects, showing methodology applicable by IT companies for critical infrastructure protection.

Keywords: cybersecurity; cyber-physical systems; smart parking; automated license plate recognition; computer vision; IoT security; threat modeling; vulnerability assessment.

INTRODUCTION

Nowadays, urban infrastructure depends heavily on cyber-physical systems (CPS) that connect physical processes with computational elements through networked communication systems. Smart parking systems represent a critical area where cybersecurity becomes important — considering how sensitive vehicle identification data is and potential system abuse [14], [16], [17].

When automated license plate recognition (ALPR) technology is integrated with parking management systems, new attack surfaces appear that require thorough security analysis.

This research becomes relevant for Ukrainian smart city development projects. Critical infrastructure and cybersecurity have become a national priority during wartime conditions. Ukrainian cities actively apply digital transformation projects, including smart parking solutions. This makes setting up strong security frameworks from early deployment stages essential. Protecting civilian infrastructure systems such as transportation and parking management contributes to overall national cybersecurity strength.

Current smart parking systems often value functionality more than security factors, creating vulnerabilities that malicious actors can exploit. These vulnerabilities enable unauthorized access to vehicle data, manipulation of parking information, or complete system operation disruption. The combination of IoT devices, computer vision systems, and cloud-based services in smart parking architecture requires a serious cybersecurity approach addressing security measures.

Problem statement. This research is mainly related to the cybersecurity of smart parking systems and how to make efficient and secure infrastructure of these systems.

Analysis of recent research and publications. Looking at recent cybersecurity work on autonomous and connected vehicles, there's clearly growing worry about smart city infrastructure vulnerabilities [4]–[6]. Smart parking systems face unique security challenges — researchers have noted this is because of their distributed nature and how they depend on multiple communication protocols [7]–[10]. The problem is that systems often focus on making things work better while overlooking critical protection aspects.

Take Radiuk et al. [1] — they showed how well convolutional neural networks work for parking slot detection but completely missed data processing protection effects. It's the same story with automated license plate recognition studies [9], [10]. They focus mostly on accuracy improvements without thinking about cybersecurity — which is bad when you consider how sensitive license plate data is.

Earlier IoT protection framework research [31] gives us basic principles for securing networked infrastructures. But specialized approaches for parking facilities? Still not much there. Computer vision API integration [15] in smart parking brings additional concerns that need dedicated analysis [26]–[28]. This gap between making things work and making them secure keeps showing up in the literature.

Article aims. What we want to do in this research is develop and analyze cybersecurity measures for cyber-physical smart parking systems with automated license plate recognition. We are focusing on threat modeling, vulnerability assessment, and secure architecture design. Basically, we want to bridge that gap between making things work and making them secure in smart parking infrastructure.

THEORETICAL FOUNDATIONS OF RESEARCH

Cyber-physical systems in smart parking infrastructure bring together physical sensors, cameras, and actuators with computational processing and network communication capabilities [13]. When you're designing secure CPS, the theoretical foundations rely on defense-in-depth principles — multiple security layers that provide complete protection against different attack vectors. This makes sense because no single security measure will be enough in complex, interconnected systems.

Security assessment frameworks for CPS environments usually use risk analysis methods. They consider system components, potential vulnerabilities, and threat scenarios [29], [30]. A systematic approach means identifying critical system components $S = \{s_1, s_2, \ldots, s_n\}$ and potential vulnerabilities $V = \{v_1, v_2, \ldots, v_m\}$. Where components and vulnerabilities intersect, you get a risk matrix that guides security setup priorities.

You can formulate risk assessment mathematically:

$$R = \sum_{i=1}^{n} \sum_{j=1}^{m} P(v_j|s_i) \times I(v_j) \times L(s_i) \quad (1)$$

R represents overall system risk, $P(v_j|s_i)$ is the probability of vulnerability v_j being exploited given system component s_i, $I(v_j)$ represents impact severity of vulnerability v_j, and $L(s_i)$ indicates likelihood of component s_i being targeted.

Security effectiveness evaluation happens through complete testing and analysis of applied countermeasures. You can measure effectiveness like this:

$$E = 1 - \prod_{i=1}^{k} (1 - E_i) \quad (2)$$

Where E stands for overall security effectiveness and E_i is effectiveness of individual security control i across k total controls.

RESEARCH METHODOLOGY

Our research approach includes assessing vulnerabilities, modeling threats, and designing protection architecture for smart parking infrastructures. The experimental setup uses a new cyber-physical parking facility with multiple components that need evaluation.

Firstly, we need to do a network infrastructure analysis. We examine RTSP camera protocols, HTTP/HTTPS communications, and APIs. This analysis will show weak points in the communication system that could allow unauthorized access or data interception.

Threat modeling is the second component. We use the STRIDE method to find potential attack vectors. This means that we examine Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege threats in all components.

Thirdly, we do vulnerability testing. Penetration testing of interfaces includes camera access points, server APIs, and client applications [28]. This testing finds problems that a theoretical analysis might miss.

Finally, we'll determine the method of calculating metrics. We can use mathematical models to measure how well protection improvements work.

The experimental environment has a Hikvision DS-2CD1021-I camera [18], a Laravel REST API server [19], [21], and React Native mobile client [22], [23]. Each part of the system was tested on its own and as part of the whole to find problems that were either separate or affected the entire system.

Research was done at Khmelnytskyi National University using commonly available technologies and cloud services.

Fig. 1 shows the system architecture — how hardware components (CCTV camera), software components (Laravel REST API, Python OpenCV API), and client applications (React Native mobile app, web browser interface) interact. Each interaction point can be a potential attack surface that needs security consideration.

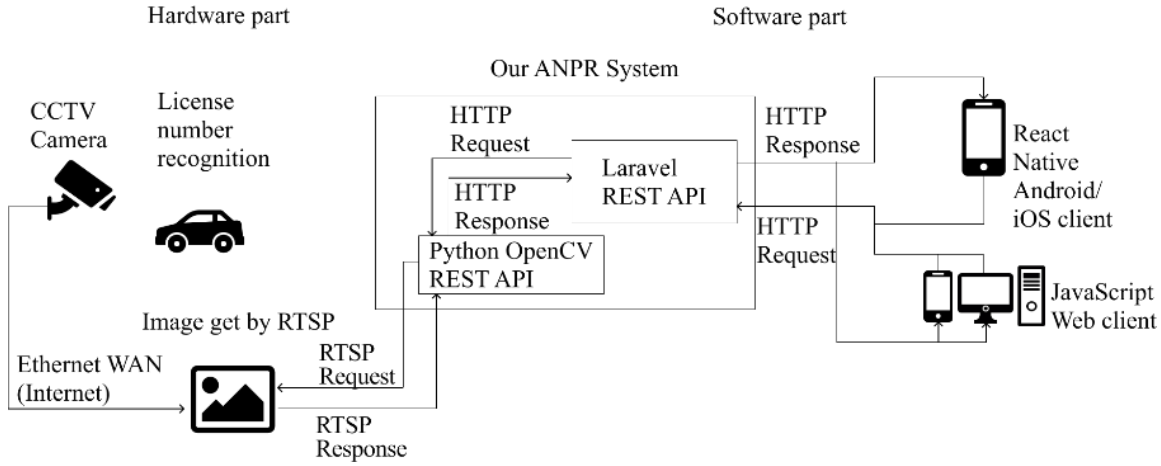

Fig. 1. Cyber-physical smart parking system architecture with ALPR capabilities

RESEARCH RESULTS

Security assessment of smart parking components

When we tested our cyber-physical smart parking system, we found several security factors in different system layers. Each layer of the system has unique vulnerabilities that need right security measures.

Looking at component interaction diagram (Fig. 2), we can see multiple communication endpoints that need security evaluation. HTTP connections between web/mobile clients and server hosting environments are especially important. The complexity of multi-component interaction in our system increases potential attack surfaces exponentially.

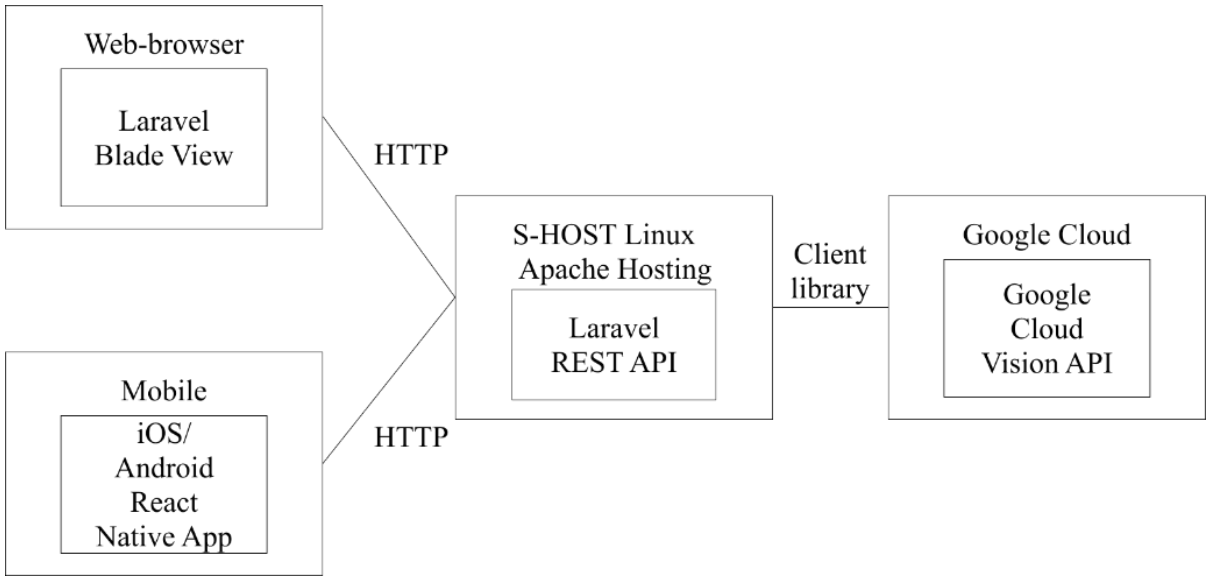

Fig. 2. Component interaction diagram

Camera network layer security

Usually, we use RTSP (Real-Time Streaming Protocol) for accessing camera feed. RTSP communications are significantly risky because of protocol characteristics. When we analyzed camera authentication methods, we found that default credentials and unencrypted data transmission create exploitable vulnerabilities. Many smart parking setups just don't bother changing default camera credentials — this creates easily exploitable entry points.

RTSP using devices must have strong authentication and encrypted data transfer to prevent unrestricted camera feed access. We can calculate the probability of unauthorized RTSP access like this:

$$P(UA) = f(P(DC), P(NA), P(PE)) \quad (3)$$

Where P(DC) stands for probability of default credentials being unchanged, P(NA) indicates network accessibility probability, and P(PE) is protocol-level exploit probability. Relation f needs to be figured out experimentally. Studies show that IoT systems with cameras often keep default credentials, creating major vulnerabilities [11], [12].

API protection factors

We tested REST API setup using Laravel framework [19]–[21] for common web application issues. Our results show multiple vulnerability categories that need attention.

One of the most common measures that is used in these types of systems is token-based authentication. These tokens with strong encryption [25] provide secure session management while preventing unrestricted access. Developers need to carefully implement token generation, validation, and expiration policies.

We can't neglect input validation for image data. Processing this data prevents injection attacks and abuse. Validation includes file type verification, size limits, content analysis, and malware scanning. Sure, we know that data should be coming only from our local requests, but this can't be ignored if there is even the smallest possibility of something going wrong.

Rate limiting factors for external API calls of Google Cloud Vision API [15], [24] prevent denial-of-service attacks and excessive resource consumption.

These measures together provide serious protection against most common web application threats. We can determine combined effectiveness using standard evaluation method:

$$CE = 1 - \prod_{i=1}^{n}(1 - IE_{\text{i}}) \quad (4)$$

where IE_{i} is individual effectiveness of measure i.

Following established guidelines like OWASP recommendations [31] can greatly improve API protection posture. But generic recommendations need adaptation to specific smart parking needs.

Data processing protection

Google Cloud Vision API integration brings factors related to external service dependencies. Data processing protection means careful attention to data transmission, storage, and processing practices to minimize potential exposure risks. License plate data sensitivity needs particular attention to privacy and protection factors.

The image processing workflow (Fig. 3) shows data flow from clients through all system parts, including external API processing. Each stage has potential security problems that need specific protection measures. Data exposure risk increases at each processing stage, especially during external API communication.

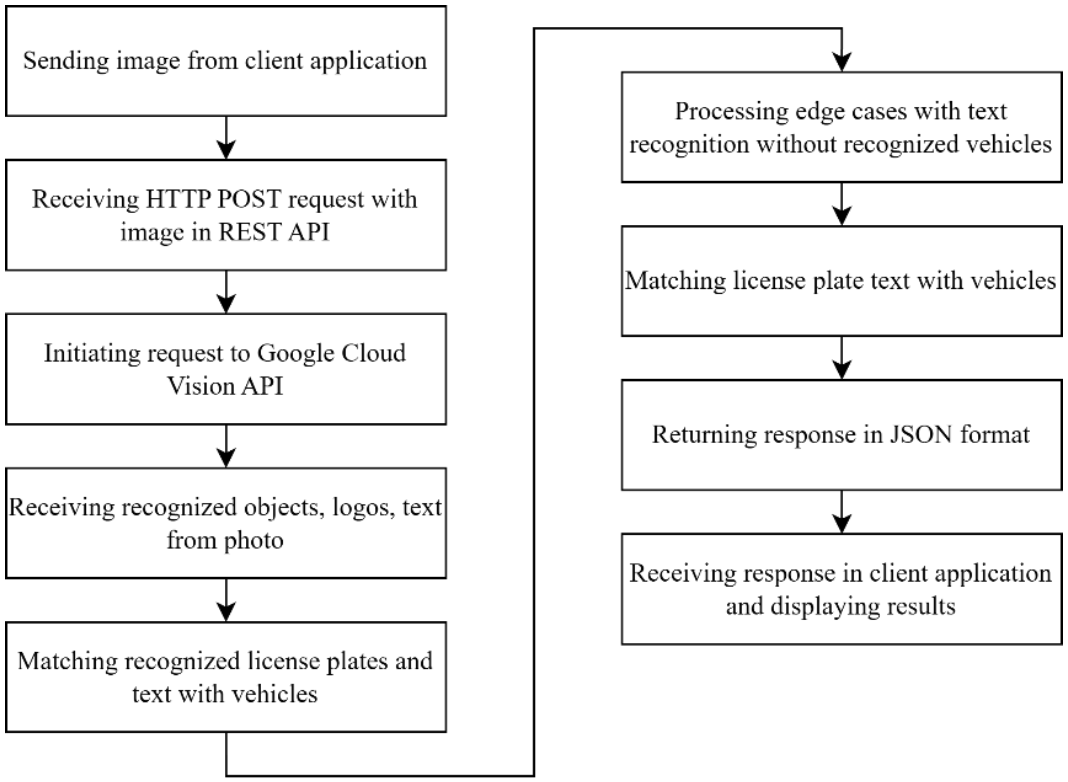

Fig. 3. Image processing workflow for automated license plate recognition system

Secure data transfer protocols and encryption standards are the main tools for protecting sensitive data during processing and transmission. We can determine data protection effectiveness through risk evaluation methods that consider exposure factors and processing complexity:

$$PrE = f\ (DER, PS, ES) \quad (5)$$

which is a formal signature description of relation between security context of system and its protection. Effective protection depends on minimizing data exposure risks (DER) across multiple processing stages (PS) while maintaining strong encryption standards (ES).

Network protection factors

Configuring a secure environment for accessing camera can greatly reduce RTSP vulnerability exposure. Virtual private networking and encrypted tunneling are perfect approaches for this task. Network segmentation (like DMZ) isolates camera traffic from other components, limiting potential attack spread.

We can calculate the network security factor for network-level protections:

$$NSF = 1 - (P(NI) \times P(PE)) \quad (6)$$

where P(NI) stands for probability of successful network interception and P(PE) indicates protocol-level abuse probability. Research shows that encrypted VPN tunnels and secured RTSP setups greatly reduce these vulnerability probabilities [29].

Data protection strategies

Data transfer protocols should encrypt license number (and other sensitive data) using algorithms like AES with appropriate key lengths. This measure includes cryptographically secure key generation, data integrity verification methods, and following proper key management practices.

Specifically, AES-256 encryption with responsibly managed keys provides strong data protection. Key rotation policies are needed to ensure security even if individual keys get compromised. We can evaluate data protection strength like this:

$$DPS = f(ES, KMQ) \quad (7)$$

where ES is strength of encryption algorithm and KMQ is a quality of key management. World-wide standards also recommend AES-256 encryption for sensitive data protection.

Performance factors

Protection enhancements usually affect performance — you need careful balance between defense and functionality. Performance factors must be checked in multiple areas:

Processing latency goes up because of encryption overhead. Protection setups generally introduce additional processing delays that must be considered in design.

License number recognition accuracy must stay at prominent levels despite protective measures. Computer vision should not experience performance variations when protection protocols are applied — the only one concern is decrypting image data.

Resource usage increases because of more processing needs for protective functions. It must be accounted for protection overhead in CPU and memory consumption.

Experimental setup observations

Our secure cyber-physical parking prototype shows several key capabilities. License number recognition maintains acceptable accuracy with active protection protocols. Results suggest that protective measures can successfully be integrated while preserving functional performance within acceptable ranges.

Testing shows that concurrent protective measure operation is achievable with proper design. System monitoring applies complete logging and capabilities that provide status information and threat detection.

The system achieves reliable productivity with protective measures enabled. Availability stays high during protection-enhanced operation.

Experience provides insights into practical factors for balancing protection needs with performance and functionality. The prototype shows that complete protection setup can be implemented in smart parking infrastructures when professionally designed and applied.

CONCLUSIONS AND FUTURE RESEARCH PROSPECTS

This research provides complete analysis of cybersecurity factors in cyber-physical smart parking systems with automated license plate recognition capabilities. Our study shows that smart parking setups face various security challenges requiring multifaceted security approaches.

The proposed security-conscious framework addresses vulnerabilities across network, application, and data protection layers while maintaining system functionality. Our setup proves that security measures can integrate into smart parking systems with careful attention to performance factors.

The practical contribution includes a security-conscious system architecture that addresses common vulnerabilities in smart parking setups. Research experience provides insights into balancing security needs with operational functionality. Vulnerability assessment methods provide systematic approaches for security improvement in similar systems.

Possible prospects for further research include direct applications like Ukrainian IT companies implementing the security framework in smart parking solution, educational

institutions integrating methodology into cybersecurity curricula, as well as local authorities benefit from established security requirements for smart parkings.

Key areas requiring further investigation include advanced threat modeling for computer vision systems, distributed security architectures for smart city infrastructure. Additionally, we should consider developing cybersecurity frameworks specifically adapted for Ukrainian post-war infrastructure reconstruction as it is critical research direction already.

The established methodology is not limited only to parking systems, but it can be extended to other cyber-physical infrastructure components, supporting comprehensive cybersecurity strategy development for smart city initiatives and digital transformation projects.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Radiuk, P., Pavlova, O., El Bouhissi, H., Avsiievych, V., & Kovalenko, V. (2022). Convolutional neural network for parking slots detection. *CEUR Workshop Proceedings*, *3156*, 284–293. https://hdl.handle.net/11300/26607
2. Durlik, I., Miller, T., Kostecka, E., Zwierzewicz, Z., & Łobodzińska, A. (2024). Cybersecurity in autonomous vehicles—Are we ready for the challenge? *Electronics*, *13*(13), 2654. https://doi.org/10.3390/electronics13132654
3. Higgins, M., Jha, D. N., Blundell, D., & Wallom, D. (2025). Security by design issues in autonomous vehicles. *arXiv preprint*. https://doi.org/10.48550/arXiv.2501.04104
4. Guirrou, H., Youssef, T., Mohamed, Z. E., & Amal, T. (2024). Cybersecurity in autonomous vehicles: A comprehensive review study of cyber-attacks and AI-based solutions. *International Journal of Engineering Trends and Technology*, *72*(1), 101–116. https://doi.org/10.14445/22315381/IJETT-V72I1P111
5. Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, *103*, 102150. https://doi.org/10.1016/j.cose.2020.102150
6. Ghazali, A. A., & Fadzil, L. M. (2025). Intelligent illuminated parking system from cybersecurity perspectives: A review. *International Journal of Electrical and Electronic Engineering (IJEEE)*, *12*(1). https://doi.org/10.14445/23488379/IJEEE-V12I1P119
7. Smart Parking Ltd. (2024, March 29). Innovative parking transformation. Retrieved from https://www.smartparking.com/nz
8. ZKTeco. (2024, April 20). ZKTecoParking. Retrieved from https://www.zkteco.com/en/VideoParkingGuidanceSystem/ZKTecoParking
9. OpenALPR. (2024, April 20). Automatic license plate recognition. Retrieved from https://www.openalpr.com/
10. OpenALPR. (2024, April 20). OpenALPR library. Retrieved from https://github.com/openalpr/openalpr
11. CVE-2025-30112: Bypass device pairing of 70mai Dashcam 1S. (2025, March 24). Retrieved from https://github.com/geo-chen/70mai/blob/main/README.md#finding-1---cve-2025-30112-bypass-device-pairing-of-70mai-dashcam-1s
12. CVE-2025-5113: Remote code execution on Diviotec IP Camera. (2025, June 3). Retrieved from https://www.onekey.com/resource/security-advisory-remote-code-execution-on-diviotec-ip-camera-cve-2025-5113
13. Kovalenko, V. V. (2022). *Cyber-physical smart parking system based on computer vision technology* (Master's thesis). Khmelnytskyi National University.
14. Avsiievych, V., & Kuzmin, A. (2022). Research of smart parking system vulnerabilities and ways to eliminate them. *Aktualni problemy komputernykh nauk (APKN-2022)*, 11–14. Khmelnytskyi National University.
15. Google Cloud. (2023, December 2). Vision AI. Retrieved from https://cloud.google.com/vision
16. Avsiievych, V., & Kawonga, R. (2023). Security of smart parking cyber-physical system. *Information Technology & Engineering – 2023*, 59–61. Mykolayiv, Ukraine.
17. Pavlova, O. O., Avsiievych, V. R., & Kuzmin, A. A. (2023). Research of factors influencing mobile application security on the example of the client part of a cyber-physical smart parking system. In *Stan, dosyahnennya ta perspektyvy informatsijnykh system i tekhnolohij: materialy XXIII Vseukrayinskoyi*

naukovo-tekhnichnoyi konferentsiyi molodykh vchenykh, aspirantiv ta studentiv (pp. 98–99). ONTU Publishing House.

18. Hikvision Ukraine. (2024, April 20). Hikvision cameras with PoE support and outdoor installation. Retrieved from https://hikvision.co.ua/ua/kamery-videonablyudeniya/ip-kamery/?ocf=F76S3V430F60S3V373
19. Laravel. (2024, February 19). The PHP framework for web artisans. Retrieved from https://laravel.com/
20. Laravel. (2024, February 19). Laravel framework GitHub. Retrieved from https://github.com/laravel/framework
21. TutorialsPoint. (2024, February 19). Laravel – overview. Retrieved from https://www.tutorialspoint.com/laravel/laravel_overview.htm
22. Netguru. (2024, April 20). What is React Native. Retrieved from https://www.netguru.com/glossary/react-native
23. Facebook. (2024, April 20). React Native. Retrieved from https://github.com/facebook/react-native/blob/main/packages/react-native/scripts/cocoapods/helpers.rb
24. Google Cloud. (2024, April 20). Vision API. Retrieved from https://cloud.google.com/vision?demo
25. Internet Engineering Task Force. (2024, December 15). RFC 7519: JSON Web Token (JWT). https://tools.ietf.org/html/rfc7519
26. Elfaki, A. O., Messoudi, W., Bushnag, A., Abuzneid, S., & Alhmiedat, T. (2023). A smart real-time parking control and monitoring system. *Sensors*, *23*(24), 9741. https://doi.org/10.3390/s23249741
27. Alpana, A., Nikhil, K., Kunal, M., Shritej, N., & Shreenath, P. (2024). Parking the future: A review of IoT based parking systems. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(11), 2513–2517. https://doi.org/10.56726/IRJMETS63971
28. Mohamed, E., Heba, A., Mahmoud, S. E., Anca, D. J., & Marianne, A. A. (2023). Intrusion detection for electric vehicle charging systems (EVCS). *Algorithms*, *16*(2), 75. https://doi.org/10.3390/a16020075
29. National Institute of Standards and Technology (NIST). (2024, December 15). *Cybersecurity framework: NIST special publication 800-53 Rev. 5*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
30. ISO/IEC. (2024, December 15). *ISO/IEC 27005:2018 – Information security risk management*. Retrieved from https://www.iso.org/standard/75281.html
31. OWASP. (2024, December 15). *Internet of Things (IoT) Top 10*. Retrieved from https://owasp.org/www-project-internet-of-things/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Авсієвич Володимир Русланович
Студент магістратури факультету інформаційних технологій
Хмельницький національний університет, Хмельницький
ORCID ID: 0009-0004-2040-8756
avsiievychvr@gmail.com

Павлова Ольга Олександрівна
Доктор філософії, доцент,
завідувач кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет, Хмельницький
ORCID ID: 0000-0001-7019-0354
olya1607pavlova@gmail.com

Михальчук Ігор Володимирович
Викладач кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет, Хмельницький
ORCID ID: 0009-0002-5162-5986
mykhalchukiv@khmnu.edu.ua

СИСТЕМА БЕЗПЕКИ ДЛЯ КІБЕР-ФІЗИЧНИХ РОЗУМНИХ СИСТЕМ ПАРКУВАННЯ З АВТОМАТИЧНИМ РОЗПІЗНАВАННЯМ НОМЕРНИХ ЗНАКІВ

Анотація. Розумні системи паркування з автоматичним розпізнаванням номерних знаків (ALPR) стають все більш популярними в містах, але вони мають серйозні проблеми з кібербезпекою. У цьому дослідженні проаналізовано загрози безпеці в інфраструктурі розумного паркування та запропоновано шляхи їх зменшення за допомогою оцінки вразливостей та вдосконалення дизайну безпеки. Ми проаналізували різні атаки, такі як вразливості протоколів та ризики перехоплення даних у кіберфізичних системах паркування. Ми вивчаємо вразливості зв'язку з камерами RTSP, проблеми безпеки REST API та ризики інтеграції хмарних сервісів у системах розпізнавання номерних знаків з використанням технологій комп'ютерного зору. Наш підхід включає тестування вразливостей, моделювання загроз за допомогою фреймворку STRIDE, тестування на проникнення та аналіз безпеки. Ми вивчили проблеми протоколу камер RTSP, HTTP/HTTPS-з'єднань, налаштування REST API Laravel та інтеграції API Google Cloud Vision. Результати показують, що розумні системи паркування можуть мати ризики перехоплення даних, несанкціонованого доступу, проблеми з безпекою API та загрози цілісності системи, які потребують багаторівневих підходів до безпеки. Ми розробили прототип кібер-фізичної системи паркування з покращеними заходами безпеки у всіх компонентах. Прототип має хорошу точність розпізнавання номерних знаків при застосуванні методів безпеки без значного зниження продуктивності. Важливими факторами безпеки є захищені протоколи зв'язку, зашифрована передача даних, системи автентифікації, валідації вхідних даних, обмеження швидкості та системи реєстрації. Це дослідження допомагає зрозуміти аспекти кібербезпеки в системах паркування на основі Інтернету речей і пропонує методи безпечного налаштування автоматичного розпізнавання транспортних засобів у розумних містах. Ця робота дійсно актуальна для українських проектів розумних міст, оскільки демонструє методологію, яку застосовують IT-компанії для захисту критично важливої інфраструктури.

Ключові слова: кібербезпека; кіберфізичні системи; розумне паркування; автоматичне розпізнавання номерних знаків; комп'ютерний зір; безпека Інтернету речей; моделювання загроз; оцінка вразливості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Radiuk, P., Pavlova, O., El Bouhissi, H., Avsiievych, V., & Kovalenko, V. (2022). Convolutional neural network for parking slots detection. *CEUR Workshop Proceedings*, *3156*, 284–293. https://hdl.handle.net/11300/26607

2. Durlik, I., Miller, T., Kostecka, E., Zwierzewicz, Z., & Łobodzińska, A. (2024). Cybersecurity in autonomous vehicles—Are we ready for the challenge? *Electronics*, *13*(13), 2654. https://doi.org/10.3390/electronics13132654
3. Higgins, M., Jha, D. N., Blundell, D., & Wallom, D. (2025). Security by design issues in autonomous vehicles. *arXiv preprint*. https://doi.org/10.48550/arXiv.2501.04104
4. Guirrou, H., Youssef, T., Mohamed, Z. E., & Amal, T. (2024). Cybersecurity in autonomous vehicles: A comprehensive review study of cyber-attacks and AI-based solutions. *International Journal of Engineering Trends and Technology*, *72*(1), 101–116. https://doi.org/10.14445/22315381/IJETT-V72I1P111
5. Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, *103*, 102150. https://doi.org/10.1016/j.cose.2020.102150
6. Ghazali, A. A., & Fadzil, L. M. (2025). Intelligent illuminated parking system from cybersecurity perspectives: A review. *International Journal of Electrical and Electronic Engineering (IJEEE)*, *12*(1). https://doi.org/10.14445/23488379/IJEEE-V12I1P119
7. Smart Parking Ltd. (2024, March 29). Innovative parking transformation. Retrieved from https://www.smartparking.com/nz
8. ZKTeco. (2024, April 20). ZKTecoParking. Retrieved from https://www.zkteco.com/en/VideoParkingGuidanceSystem/ZKTecoParking
9. OpenALPR. (2024, April 20). Automatic license plate recognition. Retrieved from https://www.openalpr.com/
10. OpenALPR. (2024, April 20). OpenALPR library. Retrieved from https://github.com/openalpr/openalpr
11. CVE-2025-30112: Bypass device pairing of 70mai Dashcam 1S. (2025, March 24). Retrieved from https://github.com/geo-chen/70mai/blob/main/README.md#finding-1---cve-2025-30112-bypass-device-pairing-of-70mai-dashcam-1s
12. CVE-2025-5113: Remote code execution on Diviotec IP Camera. (2025, June 3). Retrieved from https://www.onekey.com/resource/security-advisory-remote-code-execution-on-diviotec-ip-camera-cve-2025-5113
13. Kovalenko, V. V. (2022). *Cyber-physical smart parking system based on computer vision technology* (Master's thesis). Khmelnytskyi National University.
14. Avsiievych, V., & Kuzmin, A. (2022). Research of smart parking system vulnerabilities and ways to eliminate them. *Aktualni problemy komputernykh nauk (APKN-2022)*, 11–14. Khmelnytskyi National University.
15. Google Cloud. (2023, December 2). Vision AI. Retrieved from https://cloud.google.com/vision
16. Avsiievych, V., & Kawonga, R. (2023). Security of smart parking cyber-physical system. *Information Technology & Engineering – 2023*, 59–61. Mykolayiv, Ukraine.
17. Pavlova, O. O., Avsiievych, V. R., & Kuzmin, A. A. (2023). Research of factors influencing mobile application security on the example of the client part of a cyber-physical smart parking system. In *Stan, dosyahnennya ta perspektyvy informatsijnykh system i tekhnolohij: materialy XXIII Vseukrayinskoyi naukovo-tekhnichnoyi konferentsiyi molodykh vchenykh, aspirantiv ta studentiv* (pp. 98–99). ONTU Publishing House.
18. Hikvision Ukraine. (2024, April 20). Hikvision cameras with PoE support and outdoor installation. Retrieved from https://hikvision.co.ua/ua/kamery-videonablyudeniya/ip-kamery/?ocf=F76S3V430F60S3V373
19. Laravel. (2024, February 19). The PHP framework for web artisans. Retrieved from https://laravel.com/
20. Laravel. (2024, February 19). Laravel framework GitHub. Retrieved from https://github.com/laravel/framework
21. TutorialsPoint. (2024, February 19). Laravel – overview. Retrieved from https://www.tutorialspoint.com/laravel/laravel_overview.htm
22. Netguru. (2024, April 20). What is React Native. Retrieved from https://www.netguru.com/glossary/react-native
23. Facebook. (2024, April 20). React Native. Retrieved from https://github.com/facebook/react-native/blob/main/packages/react-native/scripts/cocoapods/helpers.rb
24. Google Cloud. (2024, April 20). Vision API. Retrieved from https://cloud.google.com/vision?demo
25. Internet Engineering Task Force. (2024, December 15). RFC 7519: JSON Web Token (JWT). https://tools.ietf.org/html/rfc7519
26. Elfaki, A. O., Messoudi, W., Bushnag, A., Abuzneid, S., & Alhmiedat, T. (2023). A smart real-time parking control and monitoring system. *Sensors*, *23*(24), 9741. https://doi.org/10.3390/s23249741

27. Alpana, A., Nikhil, K., Kunal, M., Shritej, N., & Shreenath, P. (2024). Parking the future: A review of IoT based parking systems. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(11), 2513–2517. https://doi.org/10.56726/IRJMETS63971
28. Mohamed, E., Heba, A., Mahmoud, S. E., Anca, D. J., & Marianne, A. A. (2023). Intrusion detection for electric vehicle charging systems (EVCS). *Algorithms*, *16*(2), 75. https://doi.org/10.3390/a16020075
29. National Institute of Standards and Technology (NIST). (2024, December 15). *Cybersecurity framework: NIST special publication 800-53 Rev. 5*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
30. ISO/IEC. (2024, December 15). *ISO/IEC 27005:2018 – Information security risk management*. Retrieved from https://www.iso.org/standard/75281.html
31. OWASP. (2024, December 15). *Internet of Things (IoT) Top 10*. Retrieved from https://owasp.org/www-project-internet-of-things/