ISSN: 3093-9305 VOLUME - 2

JOURNAL OF GLOBAL SCIENTIFIC INNOVATIONS

worldjournal.uz

CYBERSECURITY RISKS IN SMART STREET LIGHTING SYSTEMS: FROM IoT EFFICIENCY TO CRITICAL INFRASTRUCTURE PROTECTION

Nuriddinov Sardorbek

First-year student, Cyber University State University

Abstract. Smart street lighting integrates energy-efficient illumination with networked sensing, cloud services, remote control, and automated decision-making. While this improves operational efficiency, it also transforms conventional lighting assets into cyber-physical components of urban infrastructure. This study evaluates cybersecurity risks in a low-cost smart street lighting architecture based on an ESP32-class controller, motion and ambient-light sensors, Wi-Fi connectivity, a Firebase-style cloud backend, and a web dashboard. The assessment combines architecture decomposition, asset and trust-boundary identification, STRIDE threat modeling, and threat-to-control mapping. Six principal threat categories are identified: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The analysis shows that hardcoded credentials, insecure provisioning, misconfigured cloud rules, sensor spoofing, firmware compromise, unauthorized remote control, botnet recruitment, and lateral movement can cause consequences ranging from energy waste and loss of system availability to disruption of public safety.

Keywords: smart street lighting, IoT security, ESP32, Firebase, smart city cybersecurity, sensor spoofing, STRIDE, Zero Trust, secure-by-design, critical infrastructure.

AQLLI KO‘CHA YORITISH TIZIMLARIDA KIBERXAVFSIZLIK XATARLARI: IoT SAMARADORLIGIDAN MUHIM INFRATUZILMANI HIMOYA QILISHGACHA

Annotatsiya. Aqlli ko‘cha yoritish tizimlari energiya tejamkor yoritishni tarmoqqa ulangan sensorlar, bulutli xizmatlar, masofadan boshqaruv va avtomatlashtirilgan qaror qabul qilish imkoniyatlari bilan birlashtiradi. Bunday integratsiya operatsion samaradorlikni oshiradi, biroq an’anaviy yoritish vositalarini shahar infratuzilmasining kiberfizik tarkibiy qismiga aylantiradi. Ushbu tadqiqot ESP32 turidagi kontroller, harakat va tashqi yorug‘lik sensorlari, Wi-Fi ulanishi, Firebase turidagi bulutli platforma hamda veb-boshqaruv paneliga asoslangan kam xarajatli aqlli ko‘cha yoritish arxitekturasidagi kiberxavfsizlik xatarlarini baholaydi.

Baholash arxitekturani tarkibiy qismlarga ajratish, himoya qilinadigan aktivlar va ishonch chegaralarini aniqlash, STRIDE asosida tahdidlarni modellashtirish hamda tahdidlarni himoya choralariga muvofiqlashtirish usullarini birlashtiradi. Kiberxavfsizlik tahdidlarining oltita asosiy toifasi aniqlandi: identifikatsiyani soxtalashtirish, ma'lumotlar yoki tizimga noqonuniy o'zgartirish kiritish, harakatni inkor etish, axborotni oshkor qilish, xizmat ko'rsatishni rad etish va vakolat darajasini oshirish. Tahlil dasturiy kodga qattiq biriktirilgan autentifikatsiya ma'lumotlari, xavfsiz bo'lmagan dastlabki sozlash, bulutli xizmat qoidalarining noto'g'ri konfiguratsiyasi, sensorlarni soxtalashtirish, mikrodasturiy ta'minotning buzilishi, ruxsatsiz masofaviy boshqaruv, botnet tarmoqlariga jalb etish va tarmoq bo'ylab lateral harakatlanish energiya isrofidan va tizim mavjudligining yo'qolishidan tortib jamoat xavfsizligining buzilishigacha bo'lgan oqibatlarni keltirib chiqarishi mumkinligini ko'rsatadi.

Kalit so'zlar: aqlli ko'cha yoritish, IoT xavfsizligi, ESP32, Firebase, aqlli shahar kiberxavfsizligi, sensorlarni soxtalashtirish, STRIDE, Zero Trust, secure-by-design, muhim infratuzilma.

РИСКИ КИБЕРБЕЗОПАСНОСТИ В СИСТЕМАХ УМНОГО УЛИЧНОГО ОСВЕЩЕНИЯ: ОТ ЭФФЕКТИВНОСТИ IoT ДО ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Аннотация. Умные системы уличного освещения объединяют энергоэффективное освещение с сетевыми датчиками, облачными сервисами, дистанционным управлением и автоматизированным принятием решений. Такая интеграция повышает операционную эффективность, но одновременно превращает традиционные объекты освещения в киберфизические компоненты городской инфраструктуры. В исследовании оцениваются риски кибербезопасности в архитектуре недорогой системы умного уличного освещения на базе контроллера класса ESP32, датчиков движения и внешней освещённости, Wi-Fi-соединения, облачной платформы типа Firebase и веб-панели управления. Оценка объединяет декомпозицию архитектуры, идентификацию защищаемых активов и границ доверия, моделирование угроз по методологии STRIDE и сопоставление угроз с мерами защиты. Выделены шесть основных категорий угроз: подмена идентичности, несанкционированное изменение данных или системы, отказ от совершённых действий, раскрытие информации, отказ в обслуживании и повышение привилегий. Анализ показывает, что жёстко заданные учётные данные, небезопасная первоначальная настройка, неправильная конфигурация облачных правил, подмена показаний датчиков, компрометация встроенного

программного обеспечения, несанкционированное дистанционное управление, вовлечение устройств в ботнеты и латеральное перемещение по сети могут привести к последствиям от неэффективного расходования энергии и потери доступности системы до нарушения общественной безопасности.

Ключевые слова: умное уличное освещение, безопасность IoT, ESP32, Firebase, кибербезопасность умного города, подмена показаний датчиков, STRIDE, Zero Trust, secure-by-design, критическая инфраструктура.

INTRODUCTION

Street lighting is a basic municipal service whose failure has immediate physical consequences. Reduced illumination may impair road visibility, pedestrian safety, camera performance, and emergency response. The digitalization of this service through Internet of Things (IoT) technologies therefore creates a dual effect: sensors, adaptive dimming, telemetry, and remote maintenance can reduce energy consumption and operational costs, while the same connectivity expands the attack surface of a system deployed in public space.

A contemporary smart lighting node may contain a microcontroller, motion and ambient-light sensors, a wireless interface, cloud-connected telemetry, remote command functions, and local automation. Once these elements are connected, the lighting system is no longer merely electrical equipment. Software decisions can directly alter the physical environment, and a successful cyberattack may produce unsafe darkness, uncontrolled illumination, false telemetry, loss of administrative control, or a pathway into other smart-city networks. IoT security, smart-city cybersecurity, and connected-lighting guidance consistently emphasizes secure identity, protected credentials, lifecycle management, segmentation, and resilience [1–4, 9–17].

Existing sources address these risks across several technical domains. ESP32 security guidance focuses on secure boot, flash encryption, signing keys, and debug-interface protection [3, 4]; Firebase documentation emphasizes server-enforced security rules and the risks created by overly permissive database access [5–7]; sensor-security research demonstrates that ultrasonic and other physical inputs can be manipulated [8]; and smart-city studies identify systemic risks arising from interconnected infrastructure [9–15]. However, these domains are rarely assessed together within a single smart street lighting architecture. This creates a need for an integrated analysis linking device, sensor, network, cloud, dashboard, and operational vulnerabilities to corresponding security controls.

The study therefore addresses the following research question: how can a low-cost IoT-based smart street lighting system preserve energy efficiency while maintaining acceptable levels of cybersecurity and public safety? To answer this question, the system attack surface is modeled as a unified architecture, STRIDE is applied across its trust boundaries, and identified threats are mapped to practical secure-by-design controls suitable for prototypes, pilot deployments, and subsequent experimental validation.

METHODOLOGY

This research uses a technical review and security-design methodology. The analytical object is a reference smart street lighting architecture consisting of seven interconnected layers: device, sensor, actuation, network, cloud, application/dashboard, and operations. The reference node uses an ESP32-class controller, motion and ambient-light sensors, a dimmable LED unit, Wi-Fi connectivity, a Firebase-style real-time backend, and local fail-safe logic. The study does not claim to report the results of a completed penetration test or city-scale field experiment.

The research procedure consisted of four stages. First, the reference architecture and its principal trust boundaries were defined: the physical environment-to-sensor interface, sensor-to-microcontroller logic, firmware-to-cloud communication, cloud-to-dashboard interaction, operator-to-command function, and firmware-update source-to-device pathway. Second, protected assets and relevant attacker profiles were identified, including nearby attackers, remote internet attackers, credential thieves, botnet operators, insiders, and misconfigured operators. Third, threats were classified using STRIDE: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Fourth, each threat was mapped to controls derived from IoT security guidance, ESP32 security documentation, Firebase security practices, smart-city cybersecurity guidance, Zero Trust principles, and connected-lighting research [1–19].

RESULTS

Cybersecurity risk extends across the smart lighting lifecycle, affecting device firmware, sensors, provisioning, network communication, cloud services, operator access, and physical operation. Weakness at any trust boundary can undermine controls implemented elsewhere in the system.

Table 1. Cybersecurity evidence domains and their relevance to smart street lighting

Research area	Key finding	Relevance to smart lighting
IoT security guidance	IoT systems require device identity, secure updates, protected credentials, and lifecycle management [1, 2].	Directly applicable to ESP32-based lighting nodes.
ESP32 security	Secure boot, flash encryption, signing keys, and disabled debug interfaces reduce firmware and secret-extraction risks [3, 4].	Critical because lighting nodes may be physically reachable.
Firebase security	Realtime Database access depends on server-enforced rules; weak rules may expose data or allow writes [5–7].	Relevant to telemetry and command paths.
Sensor spoofing	Ultrasonic and other physical sensors can be manipulated by signal injection or environmental interference [8].	False readings may alter lighting behavior.
Smart city cybersecurity	Interconnected city systems expand attack surfaces and may affect public safety [9, 10, 14, 15].	Supports treatment of lighting as urban infrastructure.
Connected lighting risk	Network-connected lighting requires threat profiles and dedicated security controls [11–13].	Provides domain-specific evidence.
Zero Trust and resilience	Cyber-physical systems benefit from least privilege, continuous verification, segmentation, and damage limitation [16, 17].	Supports the secure-by-design architecture.

Research area	Key finding	Relevance to smart lighting
IoT botnets	Weak IoT devices can be recruited into botnets for DDoS or lateral movement [18, 19].	A lighting fleet can become an attacker resource.

The evidence summarized in Table 1 points to a common requirement: smart lighting must be secured as an end-to-end lifecycle system. Device hardening cannot compensate for permissive cloud rules, while strong cloud authentication cannot prevent manipulated physical sensor inputs. Risk therefore accumulates across interconnected trust boundaries.

Table 2. STRIDE analysis of the reference smart street lighting system

STRIDE category	Smart lighting example	Potential impact	Recommended controls
Spoofing	Fake device submits telemetry; attacker uses a stolen operator account.	False status reports; unauthorized commands.	Unique device identity; MFA; certificate-based authentication.
Tampering	Firmware or cloud command paths are modified; sensor readings are manipulated.	Unsafe lighting behavior or device takeover.	Secure boot; signed OTA; database validation; plausibility checks.
Repudiation	Operator denies sending a high-risk command.	Weak post-incident accountability.	Audit logs; signed commands; time-stamped records.
Information disclosure	Open cloud rules expose locations, schedules, or credentials.	Privacy loss; reconnaissance; targeted attacks.	Deny-by-default rules; least privilege; encrypted communication.
Denial of service	Devices are flooded, cloud paths abused, or lights forced offline.	Loss of lighting control and public-safety risk.	Rate limits; fail-safe local mode; segmentation; monitoring.
Elevation of privilege	Maintenance account obtains administrator-level control.	City-wide command abuse.	RBAC; approval workflow; separation of duties.

The STRIDE assessment shows that the most consequential threats are those that translate digital compromise into physical effects. Tampering, denial of service, and elevation of privilege can directly alter illumination at scale. Spoofing and information disclosure can provide the access or intelligence needed for subsequent attacks, while repudiation weakens accountability for remote commands affecting public infrastructure.

Table 3. Threat-to-control matrix for smart street lighting

Threat	Example	Potential impact	Recommended controls
Firmware extraction	Attacker reads ESP32 flash.	Credential leakage; device cloning.	Flash encryption; secure storage; unique credentials.
Malicious firmware	Unsigned update is installed.	Full device takeover.	Secure boot; signed OTA; rollback protection.
Cloud misconfiguration	Firebase rules allow public writes.	Unauthorized lighting commands.	Deny-by-default rules; authentication; validation.
Provisioning hijack	Attacker configures a rogue Wi-Fi network.	Traffic interception; loss of device control.	One-time pairing; encrypted provisioning; timeout.
Sensor spoofing	Fake motion or light values.	Unsafe darkness or energy waste.	Sensor fusion; plausibility checks; shielding.
Dashboard compromise	Stolen operator password.	Remote-control abuse.	MFA; RBAC; audit logs; approval workflow.
Botnet recruitment	Lighting nodes used for DDoS.	Operational and reputational harm.	Patching; egress filtering; monitoring; isolation.
Lateral movement	Lighting network used as a pivot.	Compromise of other city systems.	Segmentation; least privilege; Zero Trust access.
Cloud outage	Devices lose access to remote commands.	Reduced operational control.	Autonomous offline safe mode.

The threat-to-control mapping confirms that no single safeguard can eliminate the attack surface. Effective protection depends on layered controls: unique credentials and flash encryption reduce the consequences of physical extraction; signed updates and secure boot protect firmware integrity; cloud validation and deny-by-default rules restrict unauthorized writes; and segmentation, Zero Trust access, and offline safe mode limit the spread and physical impact of compromise.

Figure 1. Secure Smart Lighting Architecture

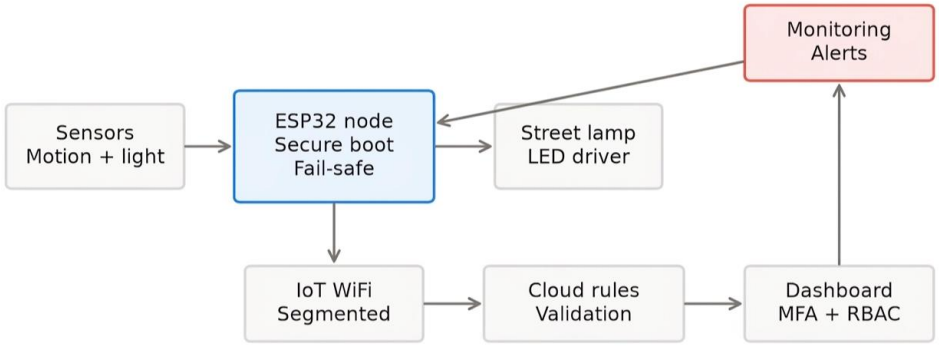

Figure 1 illustrates the secure data and control flow from the sensors to the ESP32 node, through the segmented IoT network and cloud validation layer, to the dashboard protected by MFA and RBAC. Monitoring and alerting are integrated into the architecture, while local fail-safe behavior preserves safe operation without relying exclusively on cloud availability.

Figure 2. Attack Surface Map

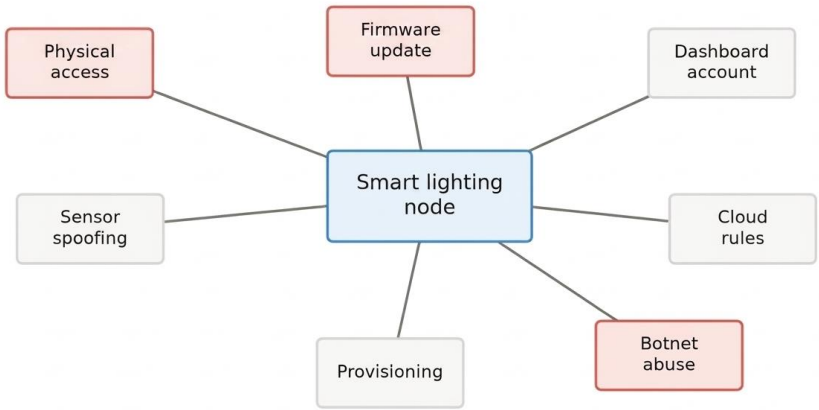

Figure 2 identifies the principal attack entry points around the smart lighting node: physical access, firmware updates, dashboard accounts, cloud rules, provisioning, botnet abuse, and sensor spoofing. The attack surface therefore spans both cyber and physical interfaces.

Figure 3. Risk Reduction Map

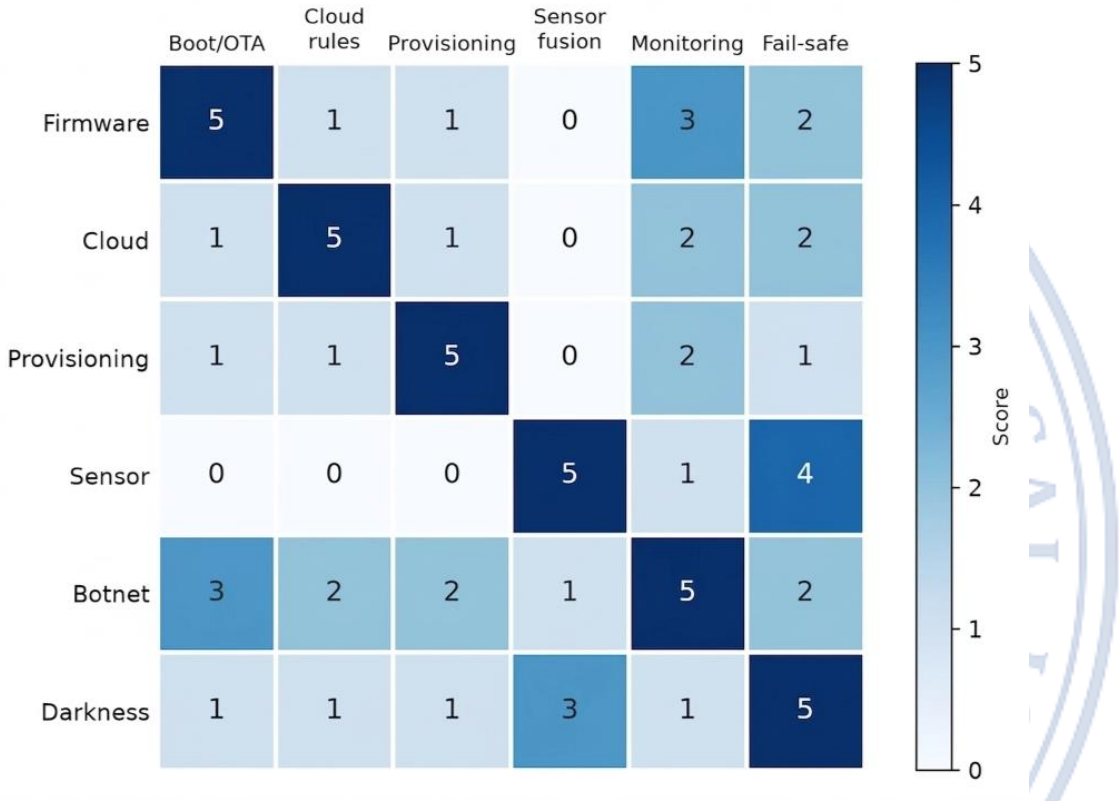

Figure 3 presents a comparative 0–5 risk-reduction matrix. Higher scores indicate stronger direct mitigation relationships between the proposed controls and the corresponding risks. Because the scores are derived from a design-based assessment rather than experimental measurement, they represent relative mitigation strength rather than empirical effect sizes.

Effective security depends on limiting implicit trust and preserving safe physical operation when individual components fail. The resulting secure-by-design baseline includes tamper resistance, sensor plausibility checking, secure boot, flash encryption, signed OTA updates, unique credentials, WPA2/WPA3, network segmentation, restricted outbound traffic, deny-by-default cloud rules, server-side command validation, MFA, RBAC, audit logging, approval of high-risk commands, asset inventory, patch management, incident response, backup, and fail-safe local illumination.

DISCUSSION

Smart street lighting should be treated as cyber-physical urban infrastructure because the protected interest extends beyond data confidentiality and device availability to the continuity and safety of a public physical service. Compromise of a single node may falsify telemetry or expose credentials, whereas compromise of a fleet may affect visibility, emergency response, surveillance effectiveness, energy use, and public confidence.

These findings align with IoT and smart-city guidance emphasizing device identity, secure updates, segmentation, least privilege, and lifecycle governance [1, 2, 9, 10, 14–17], as well as connected-lighting research that treats networked lighting as an infrastructure-security problem [11–13]. Within the reference architecture, these controls are interdependent: device hardening is insufficient without cloud access control, while cloud protection cannot compensate for manipulated sensor inputs or unsafe local behavior.

A central trade-off concerns energy efficiency and safety. Adaptive dimming is beneficial only while the sensing and control chain can be trusted. When sensor readings are uncertain, cloud connectivity is unavailable, or remote commands are anomalous, a fail-safe illumination level is preferable to maximum energy savings. The operational objective should therefore be to minimize energy use subject to a defined safety constraint, rather than to minimize energy consumption regardless of cyber-physical uncertainty.

Cloud connectivity introduces a second trade-off. Firebase-style real-time backends simplify prototyping and dashboard integration, but remote convenience should not become a single point of operational dependence. Devices should retain sufficient local autonomy to maintain safe illumination during internet outages, cloud failures, or cyber incidents. Telemetry and command channels should also be separated so that permission to report status does not automatically confer permission to issue high-impact commands.

Security requirements also change between prototype and operational deployment. Shared credentials, persistent provisioning modes, exposed debug interfaces, and manual recovery may be acceptable in a controlled laboratory environment but are unsuitable for city-scale operation. Production systems require secure manufacturing and provisioning, device-specific identity, update governance, continuous monitoring, incident response, retirement procedures, and clear operator accountability. Scale therefore increases both technical risk and institutional responsibility.

The principal limitation is methodological. The study does not include penetration testing, controlled sensor-spoofing experiments, a city-scale deployment dataset, or measured before-and-after security performance. The proposed architecture should therefore be treated as a security baseline for implementation and testing rather than as experimentally validated evidence of effectiveness. Future work should compare secure and insecure cloud-rule configurations, test provisioning methods, simulate sensor spoofing, measure the performance and energy costs of security controls, and develop anomaly-detection datasets for smart-lighting telemetry.

CONCLUSION

Smart street lighting begins as an energy-efficiency application but becomes a cybersecurity and public-safety concern when lighting nodes are connected to sensors, networks, cloud databases, dashboards, and other urban systems. The assessment identifies risks across device firmware, physical interfaces, provisioning, sensors, cloud authorization, remote control, and network dependencies.

The STRIDE assessment and threat-to-control mapping show that security requires layered protection rather than a single defensive technology. Secure boot and signed firmware protect device integrity; unique identity and encrypted provisioning reduce credential and onboarding risks; deny-by-default cloud rules and server-side validation restrict unauthorized commands; MFA, RBAC, and audit logging protect operator functions; segmentation and Zero Trust principles limit lateral movement; and fail-safe local behavior preserves the essential physical service when connectivity or trust is lost.

Connected street lighting should therefore be designed and managed as resilient cyber-physical infrastructure. Energy efficiency remains an important objective, but it must be pursued within a security architecture that preserves safe illumination, accountability, recoverability, and public trust.

REFERENCES

[1] ENISA. “Guidelines for Securing the Internet of Things.”

[2] IEEE Standards Association. “Internet of Things (IoT) Security Best Practices Whitepaper.”

[3] Espressif Systems. “ESP-IDF Security Overview.”

[4] Espressif Systems. “Secure Boot v2 — ESP32.”

[5] Google Firebase Documentation. “Understand Firebase Realtime Database Security Rules.”

[6] Google Firebase Documentation. “Avoid insecure rules.”

[7] Acunetix. “Firebase database accessible without authentication.”

[8] “Spoofing Attack on Ultrasonic Distance Sensors Using a Continuous Signal.” PubMed Central.

[9] CISA. “Cybersecurity Best Practices for Smart Cities.”

[10] CERT-In. “Cyber Security Guidelines for Smart City Infrastructure.”

[11] Pacific Northwest National Laboratory. “A Cybersecurity Threat Profile for a Connected Lighting System.”

[12] U.S. Department of Energy. “Cyber Security for Lighting Systems.”

[13] Stormshield. “The Smart City and Cybersecurity: The Issue of Public Lighting.”

[14] NIST. “Cyber-Physical Systems/Internet of Things for Smart Cities.”

[15] NIST. “Smart City Framework.”

[16] NIST. “Implementing a Zero Trust Architecture Project.”

[17] NIST CSRC. “Zero Trust Architecture and Defense in Depth.”

[18] TechScience. “Design the IoT Botnet Defense Process for Cybersecurity in Smart City.”

[19] Rambus. “Smart Cities: Threats and Countermeasures.”

worldjournal.uz