ALFA BK UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGIES
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
International Scientific Conference

Alfa BK Univerzitet

UDK:711.45:004.78
DOI: 10.46793/ALFATECHproc25.113M
Original scientific paper

Testing IoT devices and systems in smart cities: challenges and solutions

Nikola MILOVIĆ, Dejan VIDUKA

Abstract: Smart cities rely on complex IoT systems to enhance urban services, yet testing these large-scale, heterogeneous, and security-critical deployments poses unique challenges. This paper identifies key issues—scalability, interoperability, security, and resource constraints—and reviews state-of-the-art solutions, including simulation frameworks, standardization efforts, automated testing, and AI-driven approaches, providing actionable insights for robust, reliable IoT testing in smart cities..

Keywords: Interoperability, IoT testing, Scalability, Security, Smart cities

1 INTRODUCTION

Smart cities represent a paradigm shift in urban management, integrating information and communication technologies to enhance efficiency, sustainability, and quality of life for citizens. Across domains such as transportation, energy management, healthcare, and public safety, these initiatives leverage datadriven servicespowered by IoT devices and complex infrastructuresto improve urban living. IoT systems are key enablers of these environments, consisting of interconnected devices, sensors, actuators, and platforms that continuously publish and collect data, acting upon it in various ways. These systems are expected to grow exponentially in the near future, with forecasts predicting more than 75 billion IoT devices will be connected by 2025, and as many as 500 billion by 2030 [1] (Fig. 1).

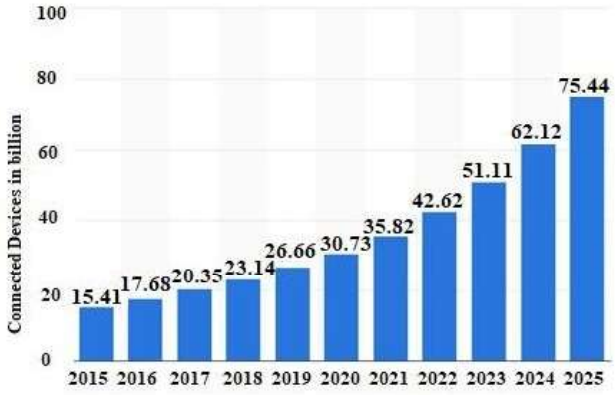

Figure 1 Internet of Things (IoT) connected devices from 2015 to 2025 (in billions)[1]

Compared to other IoT scenarios, smart cities present a unique set of challenges for testing. Cities operate at larger scales, often connecting thousands to millions of devices in a highly distributed environment. These devices must function under fluctuating network conditions and strict resource constraints, while also supporting diverse use cases, including public transport coordination, energy distribution, and emergency serviceseach with specific performance and security requirements. Moreover, the impact of any IoT failure in a city environment can be substantial, potentially affecting essential services and infrastructure, as well as raising privacy and safety concerns. Consequently, ensuring robust testing frameworks that can address real-time responsiveness, multi-vendor interoperability, and continuous data flows becomes imperative in urban IoT deployments.

Unlike traditional software systems, IoT systems span multiple-layersfrom physical sensing devices and communication networks to data processing platforms and application services. This multi-layered architecture enables real-time interaction with the physical world but also introduces significant complexity. The continuous generation of vast, heterogeneous data streams and the need for rapid response highlight the critical importance of rigorous testing to ensure reliability, security, and interoperability of current and future systems [2,3]. However, testing IoT systems under realworld city conditions poses unique challenges, as will be examined in this paper. Traditional software testing methods may not suffice due to the heterogeneous devices, limited resources, and highly distributed nature of IoT deployments. Moreover, vulnerabilities in IoT systems can lead to widespread disruptions, making security and privacy assurance indispensable [4,5].

2 BACKGROUND AND CONTEXT

The foundation of a smart city lies in a layered ecosystem of technologies that include sensing components, communication networks, data platforms, and application services. At the lowest level are sensors and actuatorsembedded within streetlights, public transportation systems, water management facilities, and buildingscollectively known as the “device” or “thing” layer. These devices capture real-time information from the environment, some of the data they collect are temperature, air quality, traffic flow, energy consumption and many others. This data then travels through communication networks, which may rely on a variety of

protocols such as Wi-Fi, 5G, LoRaWAN, MQTT, or CoAP, each chosen for its suitability to specific range, bandwidth, and energy constraints [6,7], for a simplified view of such a system refer to Fig. 2. Such vast amount of data coupled with the abundance of different usecases, pose a tough challenge for engineers to solve.

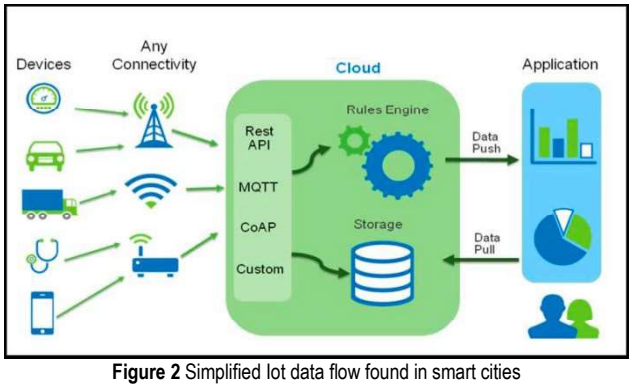

Figure 2 Simplified Iot data flow found in smart cities

Above the communication layer reside data management platformscloud or edge-based environments responsible for storing, filtering, and processing sensor data. These platforms transform raw data into meaningful insights, applying analytical reasoning, machine learning algorithms, and custom domain specific logic, that help us make sense of what is happening in our cities. On top of these platforms, application services present userfacing functionalities, dashboards, and controls to city operators and citizens. While some reference models propose numerous layers, many IoT systems share four essential ones: a device layer, a network layer, a platform (cloud/edge) layer, and an application layer [6], see Fig. 3. Together, these interconnected layers must work seamlessly, enabling physical devices to interact with the real world and deliver responsive, datadriven services that us citizens can use to improve our quality of life, or for decision-makers to be able to more easily come to conclusions and make the best possible datadriven decisions.

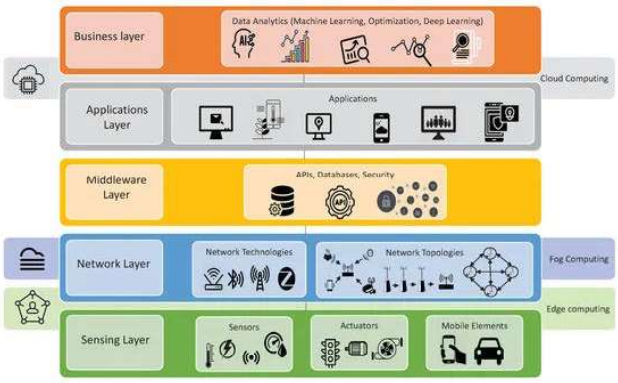

Figure 3 IoT layered architecture [25]

From a software engineering perspective, ensuring quality in such layered, heterogeneous environments demands robust testing. Traditional testing principlessuch as unit, integration, system, and acceptance testingstill apply, but their implementation differs. IoT devices may run on constrained hardware with limited computational resources. Communication links may be intermittent, data formats may be diverse, and system configurations may evolve dynamically. Conventional testing tools and approaches often assume stable, resourcerich environments, making them insufficient for IoT and smart cities. Instead, new testing frameworks must consider the unpredictable nature of networks, the variability in device capabilities, and the integration of various communication protocols. Furthermore, security and privacy testing must be prioritized, as IoT devices often reside in public spaces where breaches can have serious societal impacts. Consequently, the testing of IoT systems requires adaptation, innovation, and the development of specialized techniques and tools that can operate effectively within these complex, distributed environments.

3 CHALLENGES IN TESTING IOT DEVICES AND SYSTEMS IN SMART CITIES

Smart cities often rely on extensive, citywide IoT deployments that integrate tens of thousands of heterogeneous devicesfrom air quality sensors and smart meters to traffic lights and surveillance cameras. Ensuring that each device interacts seamlessly with the rest of the system poses significant challenges, especially when scaling test efforts to match real-world complexity. Cities like Santander, located in Spain, have experimented with large-scale IoT testbeds, deploying thousands of sensors and services to support applications such as intelligent transportation and environmental monitoring [8]. At this scale, selecting representative devices for testing and ensuring coverage of diverse communication protocols is non-trivial [9,10]. Additionally, some devices operate under strict power constraints and cannot rely on stable energy or network availability, complicating testing strategies that assume continuous connectivity [11].

Interoperability is another key concern. Today's IoT market includes devices from numerous vendors, each with unique interfaces, data formats, and proprietary standards. Without universal protocols, testers must grapple with integrating components that may not readily communicate, leading to fragmented testing scenarios and difficulties in ensuring end-to-end functionality. The absence of widely adopted standards hinders automated testing and complicates the creation of unified test frameworks [12].

Data heterogeneity further compounds these issues. IoT devices continuously stream large volumes of data in varied formats, making it challenging to achieve consistent, high-quality data for testing. In addition, there may be a lack of standardized APIs, limiting the ability to efficiently gather and analyze this data. Such complexities can skew test results, introduce delays, and reduce trust in the overall system's reliability [10].

Security and privacy remain among the most pressing concerns. As IoT networks expand, so too do the potential

attack surfaces (Fig. 4). Testing for vulnerabilities in open, interconnected urban environments is far more complex than in isolated, well-defined systems. Even minor security gaps can allow malicious actors to disrupt services or compromise sensitive information. The distributed nature of IoT systems and their reliance on various networks makes replicating potential attack scenarios during testing difficult, necessitating specialized security test methodologies [13].

Real-time constraints heighten these challenges. Many smart city applicationsfrom traffic signal optimization to emergency response systemsrequire near-instantaneous data processing and reaction. Testing must ensure not only logical correctness but also strict timing requirements and fault tolerance under unpredictable conditions [14]. Meanwhile, the resource limitations of many IoT devicessuch as limited processing power, memory, and battery capacityrestrict the complexity and duration of tests that can be run directly on the devices themselves.

Finally, the tight coupling between hardware and software in IoT systems complicates both test design and execution. A bug at the hardware level can have cascading effects on software components, and vice versa. These multilayered dependencies make isolating faults more difficult and require broader test coverage across the entire IoT stack. Moreover, environmental conditions and non-repeatable scenariossuch as variable wireless signal quality or fluctuating weather conditionscan affect device behavior and test outcomes, making it hard to reproduce and diagnose issues [15].

Overall, testing IoT devices and systems in smart cities involves not only addressing technical hurdlessuch as scale, interoperability, data variety, security, real-time constraints, and resource limitationsbut also dealing with the inherent unpredictability and complexity of real-world conditions. Developing effective test strategies and tools that can handle these multidimensional challenges is crucial for ensuring that the promises of smart cities are fully realized.

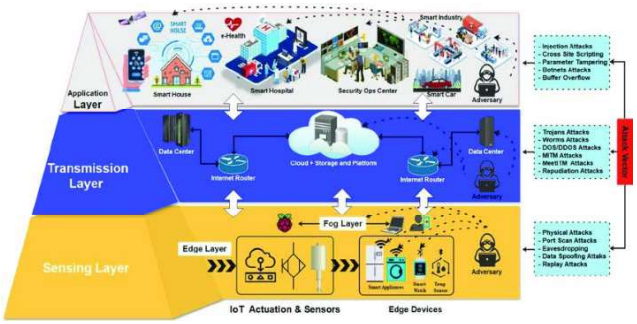

Figure 4 IoT layered architecture [25]

4 STATE-OF-THE-ART SOLUTIONS AND TESTING METHODOLOGIES

Addressing the complex challenges of testing IoT systems in smart cities has prompted the development of various methods and tools. These solutions often combine simulation, automation, interoperability standards, intelligencedriven testing, and robust security validation to ensure that devices and services function reliably in large, heterogeneous urban environments.

Simulation and Emulation Tools:

Simulating city environments and modeling sensor networks at scale allows testers to evaluate IoT deployments before committing to costly real-world experiments. Digital twins and hybrid simulation-based testing frameworks replicate real-world scenarios, enabling the validation of device behavior, communication protocols, and data processing pipelines under controlled, yet realistic conditions [15]. For instance, testbeds incorporating fog and cloud layers replicate distributed architectures found in many smart city applications, allowing developers to fine-tune device configurations and optimize network resource usage before mass deployment [16] (Fig. 5).

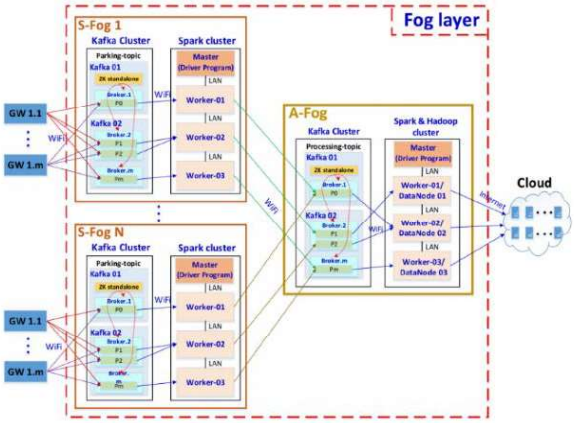

Figure 5 Two-tier fog layer architecture [16]

Automated Testing Frameworks:

Continuous integration and continuous deployment (CI/CD) pipelines are increasingly used to streamline IoT system testing, integrating automated test suites that run at every code commit or hardware update. By combining unit, integration, and system-level tests, developers and testers can quickly identify regressions and validate changes without manual intervention [17]. Automated testing frameworks also enable scalable testing of large device fleets, helping teams maintain quality in fast-paced, iterative development cycles.

Interoperability Testing Solutions:

Ensuring that devices from different vendors and platforms communicate seamlessly is vital. Standardized protocols, such as oneM2M (Fig. 6), promote interoperability and enable test frameworks to verify compliance and compatibility across diverse devices [18]. Platforms like F-Interop have emerged to support online interoperability and performance tests for IoT protocols, allowing stakeholders to confirm that devices and services adhere to agreed-upon specifications before deployment [19]. These initiatives also help prevent vendor lock-in and ensure that smart city solutions remain flexible and future-proof.

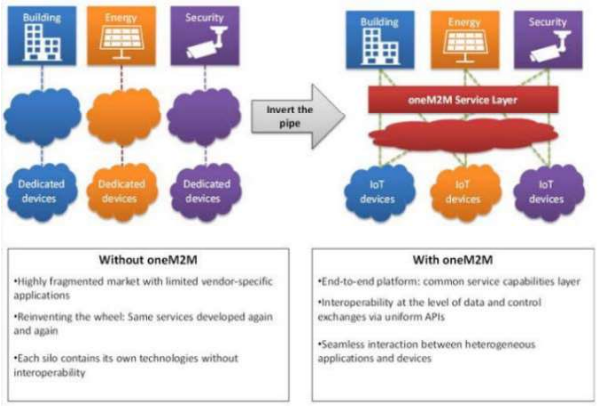

Figure 6 Comparison between oneM2M and non-oneM2M solutions [27]

AI/ML-driven Testing Approaches:

As the volume and complexity of IoT data grow, artificial intelligence (AI) and machine learning (ML) techniques are increasingly employed to detect anomalies, predict failures, and guide adaptive test strategies. For example, ML-based analysis can identify unusual patterns in sensor data and trigger targeted testing scenarios focused on potential faults [20]. Adaptive testing frameworks dynamically adjust test cases, resource allocation, and timing based on insights gleaned from data-driven models, helping to ensure coverage of rare yet critical scenarios.

Security Testing and Penetration Frameworks:

Robust security validation is crucial in interconnected city environments, where a single compromised device can lead to widespread disruption. Specialized testing frameworks employ penetration testing, fuzzing, and runtime verification to identify vulnerabilities in communication protocols, authentication mechanisms, and device firmware [21]. By subjecting IoT solutions to stress tests and adversarial conditions, these tools help ensure that systems can withstand real-world threats, safeguarding both infrastructure and citizens' privacy.

5 CASE STUDIES

Real-world pilot projects and testbeds have played a critical role in understanding the complexities of testing IoT systems for smart cities. For example, the SmartSantander project, conducted in the city of Santander, Spain, deployed thousands of IoT devicesranging from environmental sensors to traffic and parking sensorsacross an urban landscape to enable data-driven decision-making [8]. Within this large-scale environment, testers needed to address multiple challenges simultaneously, including hardware variations, network congestion, and the seamless integration of new applications as the city's needs evolved. Lessons learned from this initiative underscored the importance of continuous monitoring, adaptive testing strategies, and open data standards that streamline interoperability among disparate devices and platforms.

Another noteworthy example is the FIESTA-IoT initiative (Fig. 7), a European testbed federation that integrates multiple heterogeneous testbeds into a single, standardized platform [22]. By unifying different testing environments under a common set of semantic models, data formats, and APIs, FIESTA-IoT enabled researchers and developers to run cross-domain experiments quickly and cost-effectively. In practice, this meant that an IoT solution initially trialed in a smart home setting could be easily tested in a smart agriculture context, allowing engineers to identify issues related to scaling, data heterogeneity, and real-time constraints before deploying solutions in production.

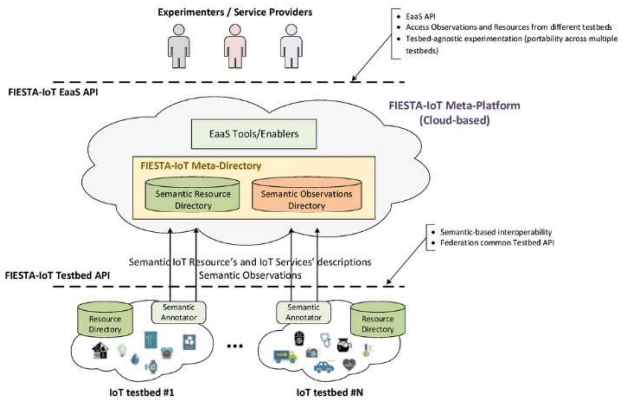

Figure 7 FIESTA-IoT testbed federation concept overview [23]

Lessons from these projects suggest a few best practices. First, establishing early standards for device communication and data modeling helps mitigate interoperability issues. Second, using federated testbeds and shared data models simplifies testing across multiple domains and scales, encouraging broader participation and knowledge exchange. Third, maintaining flexible, automated, and adaptive testing frameworks allows for the rapid iteration and improvement of IoT solutions, even as the city's technology infrastructure and environmental conditions change.

6 CONCLUSION

In the coming years, as smart cities become more interconnected and sophisticated, testing IoT systems will continue to demand innovative, multifaceted approaches. The diversity of devices and protocols, coupled with real-time demands and evolving security threats, requires more than traditional testing frameworks. Future research should explore

how blockchain technology can bolster data integrity and provide tamper-evident audits across large networks, especially when standardization lags or vendor heterogeneity is high. Similarly, AI and ML hold immense promise for dynamically adapting test strategies to detect anomalies, predict failures, and optimize resources in complex, distributed scenarios.

By building on the simulation, automation, and interoperability testing approaches outlined in this paper, researchers and practitioners can create resilient, self-improving test environments. Integrating these solutions with emerging blockchain-based tools and advanced AI/ML algorithms has the potential to enhance both security and efficiency across the entire lifecycle of urban IoT systemsfrom design and deployment through ongoing operation. In this way, smart cities can realize not only the benefits of large-scale, data-driven services but also maintain the trust and reliability that underpin safe and sustainable urban living.

7 REFERENCES

[1] Alam, T. (2018). A reliable communication framework and its use in internet of things (IoT). CSEIT1835111, 3(5), 450–456.

[2] Alhafidh, B., & Allen, W. (2016). Design and simulation of a smart home managed by an intelligent self-adaptive system. International Journal of Engineering Research and Applications, 6, 2248–2264.

[3] Fahmideh, M., Ahmad, A., Behnaz, A., Grundy, J., & Susilo, W. (2021). Software Engineering For Internet of Things: The Practitioners' Perspective. IEEE Transactions on Software Engineering, 48(8), 2857–2878.

[4] White, G., Nallur, V., & Clarke, S. (2017). Quality of Service Approaches in IoT: A Systematic Mapping. Journal of Systems and Software, 132, 186–203.

[5] Medhat, N., Moussa, S., Badr, N., & Tolba, M. F. (2019). Testing Techniques in IoT-Based Systems. In 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS) (pp. 394–401). IEEE.

[6] Kaur, H., & Kumar, R. (2021). A Survey on Internet of Things (IoT): Layer-specific, Domain-specific and Industry-defined Architectures. In Advances in Computational Intelligence and Communication Technology (pp. 265–275). Springer.

[7] Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors, 18(9), 2796.

[8] Sanchez, L., et al. (2014). SmartSantander: IoT Experimentation Over a Smart City Testbed. Computer Networks, 61, 217–238.

[9] Hu, L., Wong, W. E., Kuhn, D. R., Kacker, R. N., & Li, S. (2022). CT-IoT: A Combinatorial Testing-Based Path Selection Framework For Effective IoT Testing. Empirical Software Engineering, 27, 1–38.

[10] Murad, G., Badarneh, A., Qusef, A., & Almasalha, F. (2018). Software Testing Techniques in IoT. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 17–21). IEEE.

[11] Marinissen, E. J., et al. (2016). IoT: Source of Test Challenges. In 2016 21st IEEE European Test Symposium (ETS) (pp. 1–10). IEEE.

[12] Kaiser, A., & Hackel, S. (2019). Standards-Based IoT Testing With Open-Source Test Equipment. In 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 435–441). IEEE.

[13] Chandan, A. R., & Khairnar, V. D. (2018). Security Testing Methodology of IoT. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 1431–1435). IEEE.

[14] Walker, M. A., Schmidt, D. C., & Dubey, A. (2019). Testing At Scale of IoT Blockchain Applications. In Advances in Computers, 115 (pp. 155–179). Elsevier.

[15] Bosmans, S., Mercelis, S., Denil, J., & Hellinckx, P. (2019). Testing IoT Systems Using A Hybrid Simulation-Based Testing Approach. Computing, 101, 857–872.

[16] Nguyen, S., Salcic, Z., Zhang, X., & Bisht, A. (2020). A Low-Cost Two-Tier Fog Computing Testbed For Streaming IoT-Based Applications. IEEE Internet of Things Journal, 8(8), 6928–6939.

[17] Ramprasad, B., Mukherjee, J., & Litoiu, M. (2018). A Smart Testing Framework For IoT Applications. In 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion) (pp. 252–257). IEEE.

[18] Demirel, S. T., Demirel, M., Dogru, I., & Das, R. (2019). InterOpT: A new testing platform based on oneM2M standards for IoT Systems. In 2019 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE.

[19] Ziegler, S., Fdida, S., Viho, C., & Watteyne, T. (2017). F-Interop: Online Platform Of Interoperability And Performance Tests For The Internet Of Things. LNICST, 190, 49–55.

[20] Medhat, N., Moussa, S. M., Badr, N. L., & Tolba, M. F. (2020). A Framework For Continuous Regression And Integration Testing In IoT Systems Based On Deep Learning And Search-Based Techniques. IEEE Access, 8, 215716–215726.

[21] Liu, X., Cui, B., Fu, J., & Ma, J. (2020). HFuzz: Towards Automatic Fuzzing Testing Of NB-IoT Core Network Protocols Implementations. Future Generation Computer Systems, 108, 390–400.

[22] Serrano, M., et al. (2022). Cross-Domain Interoperability Using Federated Interoperable Semantic IoT/Cloud Testbeds and Applications: The FIESTA-IoT Approach. In Building the Future Internet through FIRE (pp. 287–321). River Publishers.

[23] Lanza, J., Sanchez, L., Gomez, D., Elsaleh, T., Steinke, R., & Cirillo, F. (2016). A Proof-of-Concept for Semantically Interoperable Federation of IoT Experimentation Facilities. Sensors, 16(1006), 1–20.

[24] Khalil, U., Uddin, M., Malik, O., & Hussain, S. (2022). A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions. IEEE Access, 10, 1–1.

[25] Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. (2021). IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. Smart Cities, 4, 429–475.

[26] oneM2M. (n.d.). Devices & Examples. oneM2M. Retrieved from https://www.onem2m.org/using-onem2m/devices-examples

Contact information:

Nikola MILOVIĆ, BCS
2001
Alfa BK university
Bulevar maršala Tolbuhina 8, 11070
nikolamilovic2001@gmail.com

Dejan VIDUKA, Full Professor, PhD
1980
Alfa BK university
Bulevar maršala Tolbuhina 8, 11070
dejan.viduka@alfa.edu.rs
https://orcid.org/0000-0001-9147-810