DEPLOYING CLOUD, FOG AND EDGE TECHNOLOGIES IN A SMART CITY INFRASTRUCTURE: A COMPREHENSIVE ANALYSIS OF FUNCTIONAL ROLES AND SECURITY ASPECTS

A. Klychev, I. Tagangylyjov

Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan

Abstract. The article provides a detailed analysis of the implementation of cloud, fog and edge computing technologies within the framework of the smart city infrastructure. Cloud computing offers extensive storage and computational scalability; edge computing minimizes latency by processing data at or near the data source; and fog computing serves as an intermediate layer that enables localized, context-aware processing with enhanced reliability. The theoretical foundations of these technologies, their functional features, as well as the relationship with data processing systems that provide operational management of smart city services are considered. Particular attention is paid to assessing security threats associated with distributed architecture, and recommendations are being developed to improve the resilience of information systems.

Keywords: smart city; cloud computing; fog computing; edge computing; technology; security; data; processing; cyber; system.

Introduction

The development of the smart city concept requires the integration of modern information technologies for effective management of infrastructure, transport systems, utilities and urban security. Cloud, fog and edge computing are key components of this digital ecosystem, helping to reduce data latency, optimize resource utilization and improve decision-making. However, in parallel with the implementation of these technologies, the need to address information security issues increases, which becomes an important aspect in the context of cyber threats in the modern digital world.

Main Part

Theoretical bases of cloud, fog and edge technologies. Cloud technologies provide centralized storage, processing and analysis of large volumes of data, which allows for scalable computing processes. Benefits include the ability to flexibly allocate resources, centralized service management, and a high level of integration with analytical tools. Fog technologies act as an intermediary between cloud services and end devices. They allow data to be preprocessed directly near the source of its origin, which significantly reduces delays and increases the efficiency of distributed systems.

Edge computing is focused on performing analytical and computational tasks directly at the edge of the network. This ensures minimal system response time, reduces the load on central cloud platforms and allows you to quickly respond to changes in real time.

In the context of a smart city, these technologies are used to implement monitoring systems, traffic flow management, environmental control and security. Cloud computing provides analytics base and supports strategic decisions, while fog and edge technologies are responsible the real-time processing needed to implement mission-critical services such as emergency response systems and intelligent traffic management. The Table shows the application areas of these technologies in smart cities, their flexibility, using areas, security, and potential risks.

Table 1. Comparison technologies in smart cities

Feature	Cloud Computing	Fog Computing	Edge Computing
Processing Location	Centralized date centers (local or remote data centers)	Local nodes near data sources (another words between edge and cloud)	Directly on devices/ sensors (or near IoT devices)
Latency	High (due to long data transfer)	Low (closer to devices, but not real-time)	Very low (real-time decisions)
Bandwidth Usage	High (due to sending data to the cloud)	Moderate (less data sent to the cloud)	Low (Local processing)
Scalability	High (easily handles large data volumes)	Moderate (limited by local resources)	Low (limited by the edge device's resources)
Security	Dependent on the cloud provider's protocols	Enhanced (data can be processed locally)	High (minimal data transfer)
Security Risk	Centralized risk	Distributed risk	Device-level risk
Use case	City-wide analytics, big data processing	Real-time IoT applications (e.g., traffic)	Immediate local decisions (e.g., smart sensors)

The integration of distributed computing architectures is associated with a number of issues in the field of information security.

1. Centralized cloud computing threats. Centralized data storage and processing in the cloud attracts the attention of attackers, which can lead to denial of service attacks, data leaks and unauthorized access. Implementing strong encryption and authentication methods is critical.

2. Fog computing vulnerabilities. Fog nodes located at the edge of the network often have reduced security, making them vulnerable to man-in-the-middle attacks and other types of interference. Control over access to data and the implementation of local protection measures are necessary.

3. The risks of edge computing. Devices operating within edge computing may have limited resources to implement comprehensive security measures. This creates potential opportunities for exploiting vulnerabilities, which can negatively affect the overall security of the system.

An integrated computing architecture that combines cloud, edge, and fog computing can effectively balance the trade-offs between latency, processing power, and scalability.

1. Hybrid Models. Critical, time-sensitive applications can be handled at the edge or fog level, while computationally intensive tasks that are less sensitive to latency can be offloaded to the cloud.

2. Orchestration and Resource Allocation. Advanced orchestration frameworks (e.g., Kubernetes-based systems) are being developed to coordinate tasks across these layers, ensuring optimal resource utilization and quality of service.

3. Data Management and Analytics. The integration enables a multi-tiered approach where data is pre-processed at the edge, aggregated and analyzed in the fog, and stored or subjected to deep learning in the cloud.

Such a cohesive framework not only improves responsiveness and reduces network congestion but also enhances fault tolerance and system resilience in dynamic urban environments. Smart city networks must ensure robust security and privacy mechanisms across all computing layers. Challenges include.

1. Data Confidentiality and Integrity. Distributed processing increases the attack surface; thus, encryption, secure authentication, and anomaly detection must be integrated at both the fog and edge levels.

2. Access Control. Fine-grained access policies are needed to manage the diverse set of devices and users interacting with the network.

3. Trust Management. Ensuring the integrity and reliability of data processed at distributed nodes, especially when sensitive information (e.g., healthcare data or public safety alerts) is involved.

The development of standardized frameworks and protocols is crucial to address these security concerns while maintaining system performance. To improve the sustainability of smart city infrastructure, it is recommended.

1. Implementation of multi-level security systems, including complex mechanisms for encryption, authentication and access control.

2. Organization of continuous monitoring of network traffic and prompt response to cyber incidents.

3. Developing security standards for Internet of Things (IoT) devices taking into account the specifics of working in edge computing conditions.

4. Conducting regular audits and testing aimed at identifying and eliminating vulnerabilities in the distributed architecture.

Conclusion

The integration of cloud, edge, and fog computing is central to the development of smart city networks that require low latency, high scalability, and robust security. At the same time, the distributed nature of these systems creates significant security challenges that require the development of comprehensive protective measures. While cloud computing provides the necessary computational power and storage, edge and fog computing address the challenges of latency and localized data processing. Future research should focus on optimizing the interaction of computing platforms, improving security mechanisms, advanced orchestration techniques, unified security frameworks, and dynamic resource allocation strategies to further improve the performance and reliability of smart city infrastructures. Addressing these challenges will enable smarter, more resilient urban environments that can effectively meet the needs of growing populations and evolving technological demands.

References

1. Stojmenovic, I., & Wen, S. The fog computing paradigm: Scenarios and security issues. In 2014 Federated Conference on Computer Science and Information Systems (2014), 1–8.

2. Chiang, M., & Zhang, T. Fog computing for IoT: Security and privacy challenges. In R. Buyya & A.V. Dastjerdi (Eds.), Internet of Things: Principles and Paradigms (Morgan Kaufmann, 2016), 169–186.

3. Yi, S., Hao, Z., Qin, Z., & Li, Q. Fog computing: Platform and applications. In 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb) (2015), 73–78.

Information about the authors

Klychev A., senior lecturer, Oguz Han Engineering and Technology University of Turkmenistan, annamyrat.gylyjov@etut.edu.tm.

Tagangylyjov I., lecturer, Oguz Han Engineering and Technology University of Turkmenistan, i.tagangylyjow@gmail.com, i.tagangylyjov@etut.edu.tm.