Security of Infocommunication Systems and Internet of Things

2025 Vol 3, No 2

https://doi.org/10.31861/sisiot2025.2.02017

Received 11 November 2025; revised 21 December 2025; accepted 29 December 2025; published 30 December 2025

Modeling a Fog Computing Network Architecture for Secure IoT Data Processing

Yaroslav Malyuta, Maryna Derkach* and Taras Lobur

Departmet of Cybersecurity, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

*Corresponding author (E-mail: m_derkach@tntu.edu.ua)

ABSTRACT This article presents a fog computing network architecture designed for secure processing of Internet of Things data. The proposed architecture consists of four layers: the cloud layer – a central server for analytics and long-term data storage; the proxy layer – responsible for caching, routing, and load balancing; four fog nodes that provide real-time data processing; and the device layer – representing Internet of Things endpoints. This structure enables flexible load distribution and enhances the system's resilience to component failures. To verify the effectiveness of the developed architecture, simulations were performed in the iFogSim environment. Scenarios were created with different numbers of smart cameras (from 16 to 48). The modelling results showed that, with 16 cameras, the data processing latency of the proposed architecture was 286 ms, while in the traditional cloud-based architecture was 811 ms. These results demonstrate an overall 64.7% reduction in data processing latency in the developed architecture. The fog computing network architecture also achieved a 17-fold reduction in network resource utilization under minimum load (16 cameras) and a 4.3-fold reduction under maximum load (48 cameras). This translates to up to 90% savings in bandwidth and a significant decrease in the risk of network congestion. The proposed architecture ensures a high level of protection of users' personal data through the local processing of video streams. Sensitive information is processed on fog nodes without being transmitted to external networks, which minimizes the risk of personal data leakage. The modeled fog computing network architecture provides a solid foundation for further development of fog computing technologies in the Internet of Things domain.

KEYWORDS fog computing, IoT, security, network, architecture.

I. INTRODUCTION

The scalability issues in IoT systems create complex technical and architectural challenges that require innovative approaches to solve them [1]. Modern Internet of Things (IoT) ecosystems are characterized by an extraordinary diversity of devices, ranging from simple temperature and humidity sensors to complex industrial robots and autonomous vehicles [2-4]. Each type of device has unique characteristics in terms of power consumption, computing capabilities, the types of data it generates, and the frequency of data transmission. This heterogeneity poses significant difficulties for the development of unified data processing systems [5]. Horizontal scalability becomes critically important when a system must simultaneously serve millions or even billions of devices. Traditional centralized architectures quickly reach their performance limits due to constraints in network bandwidth, computing resources, and data storage capacity [6]. At the same time, vertical scalability is also limited by the physical characteristics of the hardware and economic factors. The traditional model of centralized cloud-based data processing, which has long been the standard for enterprise applications, proves inadequate for modern IoT systems due to several fundamental limitations and drawbacks [7]. The economic costs associated with transferring data to cloud can render centralized architectures economically impractical for large-scale IoT projects, especially for applications that generate large volumes of data or require continuous information transfer, particularly over mobile or satellite networks. Furthermore, centralized storage of large amounts of personal data creates attractive targets for cyberattacks and may conflict with local data protection regulations [8]. A promising solution to these challenges lies in the rapidly developing tools and platforms for implementing fog computing, which provide developers with a wide range of options for building distributed IoT systems [9].

The proposed model consists of four layers, each with specific functions and technical characteristics optimized for IoT data processing tasks (Fig. 1).

II. FOG COMPUTING NETWORK ARCHITECTURE MODEL

The fog computing network architecture is a complex multi-layer model that enables efficient data processing at different levels of proximity to the data sources [10].

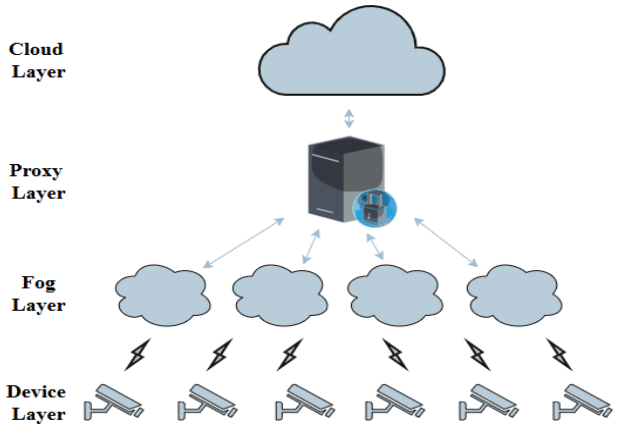

FIG. 1. Fog Computing network architecture model.

A. Cloud Layer. The Cloud Layer represents the highest level of hierarchy, incorporating a high-performance central server. This layer is designed to perform resource-intensive computing tasks, long-term data storage, machine learning, and big data analytics. The cloud server parameters include 44,800 MIPS of computing power, equivalent to a powerful server-grade processor; 40 GB of RAM for processing large volumes of data; and asymmetric bandwidth of 100/10,000 Mbps, which reflects the typical configuration of data center Internet connections.

B. Proxy Layer. The Proxy Layer functions as an intermediate aggregation node between the cloud and local fog nodes. Its main functions include traffic routing, data caching, load balancing, and fault tolerance. The proxy server performs aggregation and routing functions while maintaining a balance between performance and energy efficiency:

– Computing power: 2,800 MIPS, sufficient for routing, caching, and data preprocessing.

– RAM: 4 GB for traffic buffering and temporary storage.

– Bandwidth: symmetric 10,000/10,000 Mbps for efficient data transit.

– Power consumption: 107.339/83.43 W, optimized for continuous operation.

– Hierarchical level: 1.

C. Fog Layer. The Fog Layer represents distributed computing nodes located near IoT data sources. These nodes perform the bulk of real-time data processing, ensuring low latency and reducing network load. The system models four fog nodes configured as routers with computing capabilities. Fog nodes are a key component of the architecture, providing localized processing of IoT data:

– Computing power: 2,800 MIPS for executing threat detection algorithms and processing video streams.

– RAM: 4 GB for buffering and intermediate calculations.

– Bandwidth: 1,000/10,000 Mbps with uplink throttling to optimize traffic.

– Power consumption: 107.339/83.43 W for energy-efficient operation.

– Hierarchical Level: 2.

D. Device Layer. The Device Layer includes IoT devices – in this case, smart cameras are used. Smart cameras function as edge computing devices with limited resources:

– Computing power: 500 MIPS for video capture and basic processing.

– RAM: 1 GB for buffering video streams.

– Bandwidth: 10,000/10,000 Mbps for high-quality video transmission.

– Power consumption: 87.53/82.44 W, corresponding to typical IP cameras.

– Hierarchical level: 3 (lowest level).

The network architecture is organized according to tree topology with controlled delays at each level. This approach enables realistic modeling of real network behavior and assessment of how network characteristics affect overall system performance. A latency of 100 ms reflects the typical characteristics of connections to remote cloud data centers over the Internet. This delay includes signal propagation time, processing in network equipment, and potential packet loss.

III. MODELLING RESULTS

To evaluate the fog computing network architecture, the iFogSim simulation platform was selected. iFogSim is a specialized extension of the well-known CloudSim platform, designed for modelling fog and edge computing environments.

As part of the study, two scenarios with different computing module placement strategies were developed, allowing for a comparison of the efficiency of the fog computing approach with traditional cloud-based solutions. For this purpose, a comprehensive smart home security simulation system was created to demonstrate typical IoT applications within a fog computing environment. The system includes video surveillance, threat analysis, and real-time notification generation. IoT traffic generation was simulated using a deterministic distribution. A transmission interval of 5 seconds was chosen to reflect the typical update frequency of video surveillance systems, balancing monitoring quality and network resource utilization. The multi-layer architecture provides natural isolation between different network segments. IoT devices do not have direct access to cloud resources, which reduces the attack surface and potential vectors of compromise [11, 12]. Fog nodes function as demilitarized zones, filtering and processing data before transmitting it to higher levels. This enables early detection of anomalous behavior and potential cyberattacks. The computing module distribution strategy aims to minimize the transmission of sensitive data. The video capture module is located directly on the cameras, ensuring local pre-processing without sending raw video data over the network. Critical threat detection and notification modules are deployed on fog nodes, enabling rapid response without dependency on cloud services. The system is modeled as a directed graph of interconnected processing modules. Each module is characterized by a computational complexity of 10 MIPS, allowing for flexible load distribution across different layers of the architecture.

The first scenario demonstrates the full implementation of fog computing principles, with data processing maximally shifted toward the data sources. The second scenario models the traditional centralized approach, in which data processing is performed in the cloud for comparative analysis. The scenarios are selected using a Boolean parameter that enables dynamic switching between architectural approaches without altering the underlying network topology. This ensures a fair and consistent comparison between the two models.

One of the most critical performance indicators is data processing latency. Therefore, key performance metrics were measured for both the proposed fog-based architecture and the traditional cloud-based approach.

In Table 1, the modelling results demonstrate a significant difference in IoT data processing latency between fog and cloud approaches. When using the

proposed fog-based architecture, latency increased from 286.44 ms for 16 cameras to 823.76 ms for 48 cameras. This growth is associated with the increased load on local fog nodes and the need to process a larger number of video streams at the edge level. However, even under maximum load, the latency of the fog solution remained within acceptable limits for real-time applications. In contrast, the cloud-oriented approach demonstrated an initial latency of 811.57 ms for 16 cameras, which gradually increased to 997.99 ms for 48 cameras. It is important to note that even the minimum latency of the cloud solution exceeded the maximum performance of the fog architecture, confirming the efficiency and advantage of local data processing.

TABLE 1. Data processing latency analysis.

Number of cameras	Fog Latency (ms)	Cloud Latency (ms)
16	286.44	811.57
20	505.82	865.7
24	580.13	901.78
28	697.32	927.56
32	746.66	946.89
40	792.14	973.947
44	814.62	983.785
48	823.76	997.99

The difference in latency between the fog and cloud approaches is particularly evident in the comparative analysis (Fig. 2). Fog computing provided a 64.7% latency reduction with 16 cameras and 17.4% reduction with 48 cameras compared to the cloud solution. This trend can be explained by the fact that fog nodes gradually reach the limits of their computing capabilities as the load increases, whereas cloud infrastructure possesses greater scalability and resource capacity.

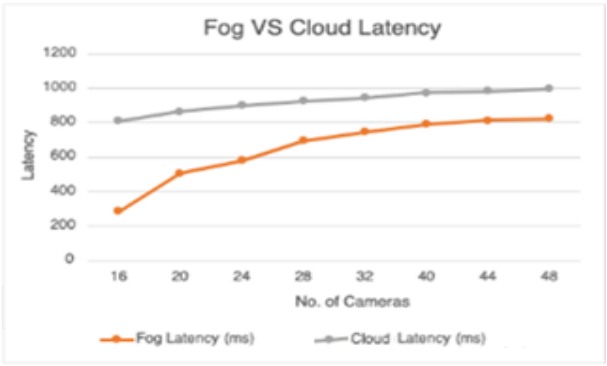

FIG. 2. Latency comparison.

The analysis of network resource utilization revealed fundamental differences between fog and cloud architectures in the context of data transmission. These differences are critically important for IoT applications, where limited network bandwidth often becomes a system bottleneck (Table 2). The fog-computing architecture demonstrated significantly lower load on the backbone networks. Fog network utilization increased from 24.9 MB for 16 cameras to 112.1 MB for 48 cameras. This growth was nonlinear, with a sharper increase observed when scaling from 40 to 48 cameras, indicating that the critical load threshold of fog nodes had been reached. The cloud-oriented approach was characterized by considerably higher consumption of network resources – from 429.8 MB for 16 cameras to 479.6 MB for 48 cameras.

TABLE 2. Network resources consumption analysis.

Number of cameras	Fog Network Usage (kB)	Cloud Network Usage (kB)
16	24912.2	429832.6
20	31136.2	436056.6
24	37360.2	442280.6
28	43584.2	454728.6
32	49808.2	467176.6
40	62256.5	467176.6
44	87168.7	473400.6
48	112080.9	479624.6

Even with a minimal number of devices, the cloud solution consumed 17.3 times more network traffic compared to the fog architecture. At maximum load, this difference decreased to 4.3 times but remained a critical factor for system scalability (Fig. 3).

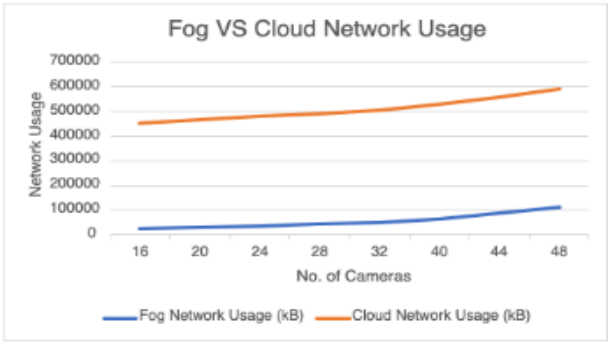

FIG. 3. Network resources consumption comparison.

A comparative analysis of system behavior with an increasing number of IoT devices highlights key aspects of the scalability of fog computing architecture. The simulation results show that the fog solution exhibits a nonlinear relationship between performance and load, which is typical for distributed systems with limited local resources.

However, it is particularly important to note that even under maximum load, the fog architecture provided better performance than the cloud solution under minimum load. Fog nodes are responsible for critical threat detection and real-time analysis based on pre-processed video data received from IoT devices. This result confirms that fog computing is an effective approach for a wide range of practical IoT applications.

IV. PRIVACY AND SECURITY OF FOG COMPUTING NETWORK ARCHITECTURE

One of the most important advantages of fog computing from a privacy perspective is the ability to process personal data within the local network, without transmitting it externally [10].

In a smart home system, video recordings may contain intimate details of residents' lives, including their habits, daily routines, and personal interactions. The video capture module performs lightweight pre-processing directly on the cameras, such as frame filtering and extraction of basic metadata. This reduces the amount of raw video data transmitted over the network. Actual threat detection and decision-making are performed on fog nodes, which analyze the pre-processed data received from the cameras.

Fog computing also enables the implementation of differential privacy, by introducing controlled "noise" into

data before transmitting it to cloud services. In the context of a security system, this may include the generalization of timestamps, event locations, or object characteristics. The distributed processing architecture also provides increased resilience to DDoS attacks and other network threats. The failure of individual fog nodes does not result in total system downtime, unlike centralized cloud-based solutions.

Finally, the modular application design implemented in the system allows isolation of critical security components and the application of differentiated protection policies for various data types and operations.

V. CONCLUSION

As a result of the research, a fog computing network architecture was developed for the secure processing of IoT data. Modelling of the developed architecture using the example of a smart home system in the iFogSim environment demonstrated the optimal balance between performance, security and cost-effectiveness, which is a critical factor for modern IoT applications.

The modelling results show that the proposed fog-based solution exhibits a nonlinear relationship between performance and load, which is typical for distributed systems with limited local resources. The effectiveness of fog computing was particularly evident in the optimization of upstream traffic to cloud services. Local processing of video streams enables only aggregated and non-sensitive threat metadata (such as event type, timestamp, and location) to be transmitted to the cloud for long-term storage and statistical analysis, instead of full video feeds. Typical detected threats include unauthorized presence, abnormal motion patterns, and intrusion events.

The research findings confirm the feasibility and efficiency of fog computing architectures in addressing the challenges of modern IoT systems and provide a foundation for the development of next-generation distributed computing platforms.

REFERENCES

[1] V. Kharchenko, A. L. Kor, and A. Rucinski, *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*. Boca Raton, FL, USA: CRC Press, 2022.

[2] M. Derkach, D. Matiuk, I. Skarga-Bandurova, T. Biloborodova, and N. Zagorodna, “A robust brain-computer interface for reliable cognitive state classification and device control,” in *Proc. 14th Int. Conf. Dependable Systems, Services and Technologies (DESSERT)*, Oct. 2024, pp. 1–9.

[3] A. Palamar, M. Palamar, and H. Osukhivska, “Real-time health monitoring computer system based on Internet of Medical Things,” in *Proc. ITTAP*, Nov. 2023, pp. 106–115.

[4] I. S. Skarga-Bandurova and M. V. Derkach, “Investigation of the efficiency of using Kalman filter to predict the arrival time of local transport,” *Herald of KHNTU*, no. 4, p. 63, 2017.

[5] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: A review,” *Journal of Big Data*, vol. 6, art. no. 111, 2019.

[6] A. Palamar, M. P. Karpinski, M. Palamar, H. Osukhivska, and M. Mytnyk, “Remote air pollution monitoring system based on Internet of Things,” in *Proc. ITTAP*, Nov. 2022, pp. 194–204.

[7] R. M. Babakov *et al.*, *Internet of Things for Industry and Human Application*, vol. 3. 2019, pp. 1–917.

[8] T. Wang, G. Zhang, A. Liu, M. Bhuiyan, and Q. Jin, “A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4831–4843, 2019.

[9] A. Stanko, W. Wieczorek, A. Mykytyshyn, O. Holotenko, and T. Lechachenko, “Realtime air quality management: Integrating IoT and fog computing for effective urban monitoring,” in *Proc. CITI*, 2nd ed., 2024.

[10] M. Muneeb, K.-M. Ko, and Y.-H. Park, “A fog computing architecture with multi-layer for computing-intensive IoT applications,” *Applied Sciences*, vol. 11, no. 24, art. no. 11585, 2021.

[11] O. Mishko, D. Matiuk, and M. Derkach, “Security of remote IoT system management by integrating firewall configuration into tunneled traffic,” *Scientific Journal of TNTU (Ternopil)*, vol. 115, no. 3, pp. 122–129, 2024.

[12] M. Waqdan, H. Louafi, and M. Mouhoub, “Security risk assessment in IoT environments: A taxonomy and survey,” *Computers & Security*, vol. 154, Jul. 2025.

Yaroslav Malyuta

In 2025, I graduated with a bachelor's degree in Cybersecurity. Currently, I am studying for a master's degree in Cybersecurity and Information Protection at Ivan Pulyuy Ternopil National Technical University. Field of scientific interests: Internet of Things, Safety and Reliability.

ORCID ID: 0009-0003-8913-6034

Maryna Derkach

In 2019, I defended my dissertation for the degree of Candidate of Technical Sciences in Information Technologies. Currently, I work as an Associate Professor at the Department of Cybersecurity at Ivan Pulyuy Ternopil National Technical University. Field of scientific interests: IoT, Intelligent Robotic Systems, Biomedical Engineering, Safety and Reliability.

ORCID ID: 0000-0001-8977-2776

Taras Lobur

In 2013, I graduated from Kharkiv National University of Radio Electronics with a degree in Information and Communication Systems Security (specialist diploma). Currently, I work as a senior lecturer at the Department of Cybersecurity at Ivan Pulyuy Ternopil National Technical University. Field of scientific interests: Computer Networks, Safety and Reliability, IoT.

ORCID ID: 0000-0001-8318-3815

Моделювання архітектури мережі туманних обчислень для безпечної обробки даних Інтернету речей

Ярослав Малюта, Марина Деркач*, Тарас Лобур

Кафедра кібербезпеки, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

*Автор-кореспондент (Електронна адреса: m_derkach@tntu.edu.ua)

АНОТАЦІЯ В статті представлена розроблена архітектура мережі туманних обчислень для безпечної обробки даних Інтернету речей. Запропонована архітектура містить 4 рівні: хмарний – центральний сервер для аналітики і довготривалого зберігання; проксі – для кешування, маршрутизації та балансування; 4 туманних вузли – для обробки даних в реальному часі; рівень пристроїв. Така структура дозволяє гнучко розподіляти навантаження та підвищує стійкість системи до відмов окремих компонентів, в разі недоступності туманного вузла, обробка може здійснюватися в хмарі, забезпечуючи безперервність роботи. Для перевірки ефективності розробленої архітектури було проведено моделювання у середовищі iFogSim. Було створено сценарії з різною кількістю розумних камер (від 16 до 48). Результати моделювання показали, що при 16 камерах затримка обробки даних на запропонованій архітектурі складає 286 мс, а затримка обробки даних на традиційній хмарній архітектурі - 811 мс. Це свідчить про загальне зниження затримки обробки даних на 64,7% на розробленій архітектурі. Архітектура мережі туманних обчислень дозволила зменшити споживання мережевих ресурсів у 17 разів при мінімальному навантаженні (16 камер) та в 4.3 рази при 48 камерах. Що, в свою чергу, економить до 90% пропускної здатності та зменшує ризик перевантаження мережі. Запропонована архітектура забезпечує високий рівень захисту персональних даних користувачів завдяки локальній обробці відеоданих. Чутлива інформація обробляється на туманних вузлах без передачі в зовнішні мережі, що мінімізує ризики витоку персональних даних. Промодельована архітектура мережі туманних обчислень створює міцну основу для подальшого розвитку технологій туманних обчислень в середовищі Інтернету речей, підкреслює переваги туманних обчислень над традиційними хмарними підходами.

КЛЮЧОВІ СЛОВА туманні обчислення, Інтернет речей, безпека, мережа, архітектура.