DOI: https://doi.org/10.15276/ict.01.2024.16
UDC 004.9

A three-tier approach to Internet of Things software architecture design

Danylo K. Chumachenko[1)]
Postgraduate Student, Department of Software Engineering
ORCID: https://orcid.org/ 0009-0000-1477-534X; chumachdk@gmail.com
Vira V. Liubchenko[1)]
Dr. Sc., Professor, Department of Software Engineering
ORCID: https://orcid.org/ 0000-0002-4611-7832; lvv@op.edu.ua. Scopus Author ID: 56667638800
[1)] Odesa Polytechnic National University, 1, Shevchenko Av. Odesa, 65044, Ukraine

ABSTRACT

The Internet of Things (IoT) rapidly evolves, presenting challenges and opportunities. This study emphasises the critical role of software in advancing IoT technologies, focusing on machine learning (ML), fog computing, and process optimisation for security and resiliency. ML is pivotal in IoT for predicting equipment failures, evaluating process efficiency, and enabling informed decision-making through real-time data analysis. By integrating ML models directly into IoT devices (edge computing), latency is reduced, and data transmission needs are minimised. Fog computing and cloud computing address latency issues by moving computational resources closer to IoT devices, enhancing scalability and optimising network resource usage. Security remains a paramount concern due to the increasing number of connected devices and their vulnerabilities. IoT software must balance efficiency, security, and performance, employing deep learning for anomaly detection, blockchain for data transparency, and optimised encryption protocols. The trend towards distributed architectures like Edge Computing enhances system resilience by reducing latency and increasing fault tolerance. The proposed IoT system architecture is a three-tier structure consisting of Edge, Fog, and Cloud levels. At the Edge level, initial data processing occurs directly on IoT devices, reducing latency and network load. The Fog level processes data within the local network, utilising more powerful computational resources for complex tasks and ensuring security through advanced machine learning and encryption. The Cloud level serves as a central repository for long-term storage and global data analysis, leveraging containerisation and orchestration technologies for scalability and reliability. This multi-layered architecture ensures efficient data processing, high security, and adaptability, making it suitable for real-time applications. The study highlights the importance of software in optimising data processing across these levels, ensuring the IoT system's resilience, scalability, and long-term sustainability.

Keywords: Internet of Things; machine learning; fog computing; edge computing; three-tier architecture; scalability; sustainability; resiliency; data processing; software design

The study aims to highlight the essential role of software in implementing advances in the Internet of Things (IoT) and propose a three-tier IoT architecture (Edge, Fog and Cloud levels) to enhance system performance, reliability, and scalability.

Understanding trends is crucial for anticipating future IoT challenges and opportunities. This paper particularly highlights the essential role of software in implementing these advances. Critical areas in software development for IoT include machine learning (ML), fog computing, and process optimisation for security and resiliency.

In IoT, ML analyses data from various sensors to predict equipment failures, evaluate process efficiency, and enable informed decision-making. For instance, ML can detect patterns that signal future problems, allowing for proactive maintenance [1]. Real-time data analysis is vital, as IoT software uses ML models to respond quickly to environmental changes. Machine learning can be integrated directly into IoT devices (edge computing), reducing latency and minimising data transmission needs. Centralised approaches are also used, sending data to central servers to train more complex models. These techniques create intelligent, autonomous systems that adapt in real-time, enhance service quality, and optimise resources.

Traditional IoT involves physical devices collecting and exchanging data over the Internet, generating vast amounts requiring real-time processing. Fog computing and cloud edge computing address latency issues by moving computational resources closer to IoT devices [2]. Fog computing reduces latency by distributing data processing across devices and local servers, while cloud edge computing processes data at the network's edge. These approaches offer reduced latency, improved

scalability, and optimised network resource usage, leading to complex, distributed software architectures where data processing occurs at multiple network levels.

Security is increasingly crucial in IoT due to the growing number of connected devices and their vulnerabilities. Each IoT device is a potential cyberattack entry point, making security a critical aspect of modern software development. IoT software must address authentication, data encryption, and unauthorised access under the constraints of limited computational resources. Developers balance efficiency, security, and performance while employing deep learning for anomaly detection, blockchain for data transparency, and optimised encryption protocols [3]. “Security by design” and continuous monitoring are essential to ensure IoT devices' reliable operation.

The trend towards distributed architectures like edge computing enhances system resilience by reducing latency and increasing fault tolerance. IoT software must incorporate monitoring and recovery mechanisms to detect and recover from failures, ensuring reliable operation in dynamic environments. Integrating these features requires thorough testing, validation, and optimisation of energy consumption, particularly in resource-constrained IoT environments.

Currently, the core paradigms for processing data in the IoT are cloud computing, fog computing, and edge computing. They differ in their architecture, capabilities, and typical use cases.

Cloud computing is characterised by centralised processing and storage in large data centres. This model offers virtually unlimited computational power and storage, which can be scaled up or down as needed. However, cloud computing often faces latency and bandwidth constraints, especially in applications requiring real-time processing, such as health monitoring or emergency services. Transmitting data to and from the cloud can introduce delays and increase network traffic, making cloud computing less ideal for time-sensitive IoT applications [4].

Fog computing extends cloud capabilities closer to the data source by creating a layer of intermediary nodes between the cloud and IoT devices. These nodes can perform processing, storage, and networking functions locally. This hierarchical structure reduces latency and bandwidth usage by processing data closer to where it is generated. The fog nodes act as local data processors, filtering and analysing data before sending only the necessary information to the cloud for long-term storage or further processing.

Edge computing pushes the boundary even further by performing data processing at the very edge of the network, directly on the IoT devices or nearby infrastructure, such as gateways or routers. This approach minimises latency to the greatest extent by processing data almost instantaneously. Edge computing is essential for applications that require immediate data processing and low-latency communication, such as autonomous vehicles, augmented reality, and industrial automation. It reduces the dependency on central data centres, ensuring that operations can continue even with intermittent or unreliable internet connections [5].

In general, each computing option has its advantages and disadvantages. Oversized systems will undoubtedly require cloud computing more often than small IoT systems. However, with proper separation, each type of computing will complement the other, creating the necessary level of functional interaction to accomplish the tasks at hand.

The architecture of the proposed IoT system (Fig. 1) is a three-tier structure consisting of the Edge level, Fog level, and Cloud level. IoT devices perform initial data processing at the Edge level using embedded machine learning models [6]. These devices minimise latency and reduce the volume of data that needs to be transmitted to higher levels. After initial processing, the data is encrypted and sent to microservices for further processing, preparation, and forwarding. Modular components are employed to allow flexible adaptation of software interfaces to the system's evolving requirements.

At the Fog level, data from IoT devices is processed further. More powerful machine learning algorithms and authentication mechanisms are utilised here, ensuring higher security and more accurate data analysis. Microservices at this level are designed according to software abstraction principles, enabling efficient management of localised tasks and interaction with cloud services for forwarding results to the Cloud level.

The Cloud level serves as a centralised data repository and manages complex machine learning models, providing long-term storage and global data analysis. Centralised authentication management and security assurance for the entire infrastructure are also handled at this level, ensuring the system's resilience and scalability [7]. Containerisation and orchestration technologies are used to guarantee the flexibility and reliability of the software components at this level. This architecture ensures the efficient distribution of computational and analytical tasks, enhancing the overall performance and reliability of the IoT system. In contrast, software solutions ensure its adaptability and long-term sustainability.

The Security module in the IoT architecture is about keeping the system safe by handling unusual data and managing the data we store across different (Edge, Fog and Cloud) levels. It's constantly watching and analysing the data, looking for anything unusual that might hint at security issues. Part of the system also makes sure that the data we store is not only secure but also easy to access whenever it's needed. If the system picks up on anything strange or unusual with the data, it acts immediately. This might mean isolating or flagging the suspicious data so someone can take a closer look.

Let's detail each component of the proposed architecture, enhancing system resilience and scalability.

At the Edge level (Fig. 2a), IoT devices initially process data directly on their computational resources, reducing latency and easing network load. More powerful devices perform additional operations optimised by efficient software.

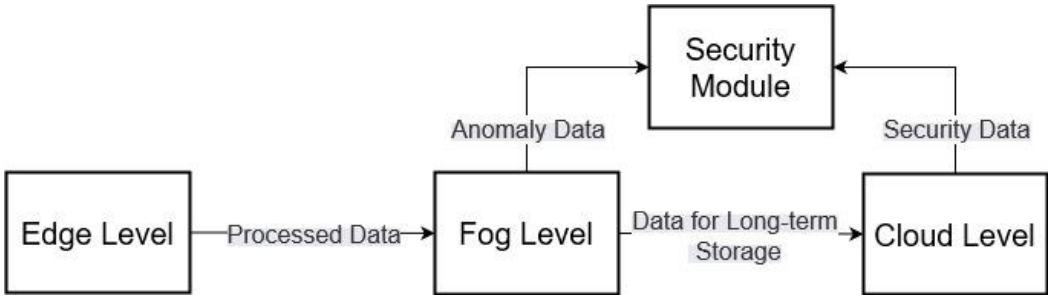
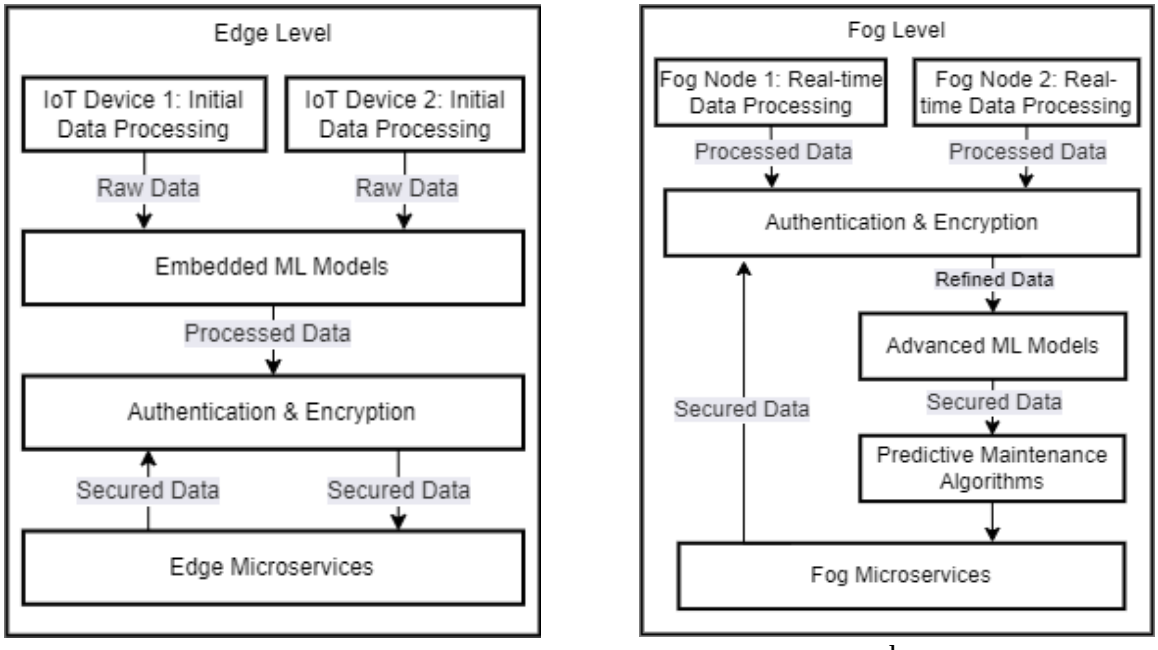


Fig. 1. **The high-level schema of a proposed architecture**



a b

Fig. 2. **The schema of Edge (a) and Fog (b) levels of the proposed architecture**

Devices at the Edge level generate and process raw data using embedded machine learning models [8], minimising latency and reducing the volume of data needing higher-level processing. Optimised algorithms enable high performance with minimal resources.

Processed data undergoes authentication and encryption, ensuring security before being passed to microservices for further processing. These microservices integrate with various devices and protocols, ensuring system versatility and scalability [9]. This software reduces cloud dependency and latency by processing data closer to its source, supporting a resilient and scalable IoT architecture.

At the Fog level (Fig. 2b), in-depth data processing occurs within the local network to which IoT devices are connected. This allows the use of more powerful computational resources than at the Edge level, enabling more complex tasks. Processed data undergoes authentication and encryption, ensuring security and confidentiality [5]. This software-integrated process protects data from unauthorised access and tampering. This practice is mandatory at all architecture levels, as each data modification requires repeated decryption and encryption.

After encryption, refined data is passed to advanced machine learning models, which perform complex analyses to improve data quality for predictive analysis. These components flexibly adapt to different data types and efficiently handle large volumes.

Predictive algorithms analyse data, forecast failures, and enable proactive management, reducing risks and downtime. If the vulnerability is detected, it's addressed at the Fog level. Finally, processed data is transmitted to microservices for distributed task management and cloud interaction, ensuring scalability and resilience.

At the Cloud level (Fig. 3) of the IoT architecture, centralised storage, management, and analysis of data collected from various system levels are conducted [7]. The primary element here is long-term storage, where data from multiple sources, including raw and processed data, is stored for extended periods. The software solutions responsible for managing this storage are designed to ensure high availability and reliability of the data, which is crucial for long-term retention.

This level involves various types of resource-intensive processing on server machines, whose capabilities allow for complex and computationally demanding operations. By leveraging containerisation and orchestration technologies, the system can efficiently distribute computational tasks across available resources, ensuring scalability and fault tolerance.

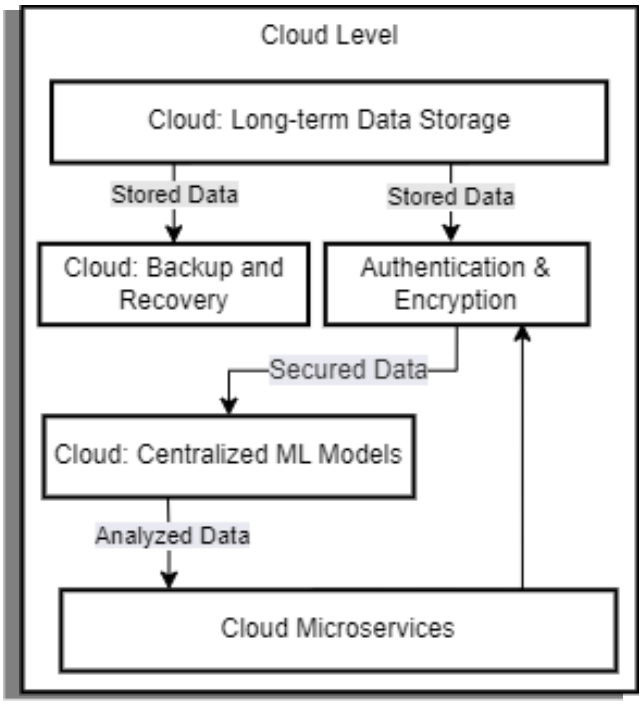


Fig. 3. **The schema of the Cloud level of the proposed architecture**

Data stored in the cloud undergoes stages of backup and recovery, as well as authentication and encryption. The backup and recovery processes are integrated into the software architecture to guarantee the reliability of data storage and protection against loss or damage. Software components provide the capability for automatic data recovery in case of failures, enhancing the system's resilience.

The secured and stored data is then transferred to centralised machine learning models, where it undergoes in-depth analysis and processing. These models, implemented using cloud computing power, can identify complex patterns and perform tasks that require significant computational resources. The software solutions managing these models employ scalable algorithms and distributed computing, enabling the efficient processing of large data volumes.

The analysed data is passed on to microservices at the cloud level for management tasks, further analysis, and integration with other system components. Microservices at the Cloud level play a key role in ensuring interaction and coordination between different parts of the system. They integrate data and analysis results from centralised machine learning models and enable various scenarios for data manipulation. This may include incorporating external services through APIs and interaction with mobile, web, or desktop applications, providing comprehensive support and scalability for the IoT system.

The proposed IoT architecture emphasises the importance of software in optimising data processing across the Edge, Fog, and Cloud levels. At the Edge level, devices perform initial data processing, reducing network load and minimising latency by handling data close to its source. The Fog level utilises more powerful computational resources for deeper analysis and enhanced security through advanced machine learning and encryption. At the Cloud level, data is centralised for storage and management, supporting complex computational tasks and long-term data retention. The use of containerisation and orchestration technologies ensures scalability and reliability. This multi-layered structure allows the IoT system to adapt to changes, efficiently process large volumes of data, and maintain high levels of security, making it well-suited for real-time applications.

REFERENCES

1. Molaei F., Rahimi E., Siavoshi H., Afrouz S. G., Tenorio V. "A comprehensive review on Internet of Things (IoT) and its implications in the mining industry". *American Journal of Engineering and Applied Sciences*. 2020; 13 (3): 499–515. DOI: https://doi.org/10.3844/ajeassp.2020.499.515.

2. Andriopoulou F., Dagiuklas T., Orphanoudakis T. "Integrating IoT and fog computing for healthcare service delivery". *Components and Services for IoT Platforms* / Ed. by G. Keramidas N. Voros, M. Hübner. *Springer, Cham*. 2017. p. 213–232. DOI: https://doi.org/10.1007/978-3-319-42304-3_11.

3. Kumar S. A., Vealey T., Srivastava H. "Security in Internet of Things: Challenges, solutions and future directions". *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*. Koloa, HI, USA. 2016. p. 5772–5781. DOI: https://doi.org/10.1109/HICSS.2016.714.

4. Escamilla-Ambrosio P. J., Rodríguez-Mota A., Aguirre-Anaya E., Acosta-Bermejo R., Salinas-Rosales M. "Distributing computing in the Internet of Things: Cloud, Fog and Edge computing overview". *Studies in Computational Intelligence*. 2017; 731: 87–115. DOI: https://doi.org/10.1007/978-3-319-64063-1_4.

5. Kim T, Yoo S-e, Kim Y. "Edge/Fog computing technologies for IoT infrastructure II". *Sensors*. 2023; 23 (8): 3953. DOI: https://doi.org/10.3390/s23083953.

6. Sarker I. H., Khan A. I., Abushark Y. B. et al. "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions". *Mobile Networks and Applications*. 2023; 28: 296–312. DOI: https://doi.org/10.1007/s11036-022-01937-3.

7. Mijuskovic A., Chiumento A., Bemthuis R., Aldea A., Havinga P. “Resource management techniques for Cloud/Fog and edge computing: An evaluation framework and classification”. *Sensors*. 2021; 21 (5): 1842. DOI: https://doi.org/10.3390/s21051832.

8. Ahmed S., Shuravi S., Afrin S., Rafa S., Hoque M., Gandomi, A. “The power of Internet of Things (IoT): Connecting the dots with cloud, edge and fog computing, distributed, parallel, and cluster computing”. 2023. DOI: https://doi.org/10.48550/arXiv.2309.03420.

9. Power A., Kotonya G. “A microservices architecture for reactive and proactive fault tolerance in IoT systems”. *IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. Chania, Greece. 2018. p. 588–599. DOI: https://doi.org/10.1109/WoWMoM.2018.8449789.

DOI: https://doi.org/10.15276/ict.01.2024.16
УДК 004.9

Трирівневий підхід до розробки архітектури програмного забезпечення для систем Інтернету речей

Чумаченко Данило Кирилович[1)]
Аспірант каф. Інженерії програмного забезпечення
ORCID: https://orcid.org/ 0009-0000-1477-534X; chumachdk@gmail.com
Любченко Віра Вікторівна[1)]
Д-р техніч. наук, професор каф. Інженерії програмного забезпечення
ORCID: https://orcid.org/ 0000-0002-4611-7832; lvv@op.edu.ua. Scopus Author ID: 56667638800
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Інтернет речей (IoT) стрімко розвивається, створюючи як виклики, так і можливості. Це дослідження підкреслює важливу роль програмного забезпечення у розвитку технологій Інтернету речей, зосереджуючись на машинному навчанні (ML), туманних обчисленнях та оптимізації процесів для забезпечення безпеки та відмовостійкості. Машинне навчання має ключове значення в IoT для прогнозування збоїв обладнання, оцінки ефективності процесів і прийняття обґрунтованих рішень за допомогою аналізу даних в режимі реального часу. Інтеграція моделей ML безпосередньо в пристрої IoT (периферійні обчислення) зменшує затримки та мінімізує потреби в передачі даних. Туманні обчислення і хмарні обчислення розв'язують проблеми затримок, переміщуючи обчислювальні ресурси ближче до пристроїв IoT, підвищуючи масштабованість і оптимізуючи використання мережевих ресурсів. Безпека залишається першочерговим завданням через збільшення кількості підключених пристроїв та їх вразливостей. Програмне забезпечення Інтернету речей має поєднувати ефективність, безпеку та продуктивність, використовуючи глибоке навчання для виявлення аномалій, блокчейн для прозорості даних та оптимізовані протоколи шифрування. Тенденція до розподілених архітектур, таких як периферійні обчислення, підвищує стійкість системи шляхом зменшення затримок і підвищення відмовостійкості. Запропонована архітектура системи IoT – це трирівнева структура, що складається з периферійного, туманного і хмарного рівнів. На периферійному рівні первинна обробка даних відбувається безпосередньо на пристроях IoT, що зменшує затримку та навантаження на мережу. Туманний рівень обробляє дані в локальній мережі, використовуючи більш потужні обчислювальні ресурси для складних завдань і забезпечуючи безпеку за допомогою передового машинного навчання і шифрування. Хмарний рівень слугує центральним репозиторієм для довгострокового зберігання та глобального аналізу даних, використовуючи технології контейнеризації та оркестрування для масштабованості та надійності. Така багаторівнева архітектура забезпечує ефективну обробку даних, високу безпеку та адаптивність, що робить її придатною для застосування у режимі реального часу. Дослідження підкреслює важливість програмного забезпечення для оптимізації обробки даних на всіх цих рівнях, забезпечуючи відмовостійкість, масштабованість і довгострокову стійкість системи IoT.

Ключові слова: Інтернет речей (IoT); машинне навчання; туманні обчислення; периферійні обчислення; трирівнева архітектура; масштабованість; відмовостійкість; обробка даних; проєктування програмного забезпечення.