Analysis of identification and access management models in the context of fog computing

Anton Zahynei[1,†], Yurii Shcheblanin[2,†], Oleg Kurchenko[2,†], Iryna Melnyk[3,*,†] and Serhii Smirnov[4,†]

[1] State University of Information and Communication Technologies, 7 Solomyanska str., 03110 Kyiv, Ukraine
[2] Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., 01033 Kyiv, Ukraine
[3] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine
[4] Central Ukrainian National Technical University, 8 University ave., 25006 Kropyvnytskyi, Ukraine

Abstract

The paper analyzes the methods of obtaining access to resources in the case of fog computing. An analysis of the advantages and disadvantages of the Single Sign-On model, Federated Identity Management model, Role-Based Access Control model, Attribute-Based Access Control model, and Zero Trust Model was carried out. A comparison of models of obtaining access in the context of fog computing is carried out.

Keywords

fog computing, IAM, FIM, SSO, RBAC, ZTM, ABAC

1. Introduction

Fog computing is becoming more and more popular due to the large number of Internet of Things (IoT) applications and the increasing amount of information that needs to be processed and stored, resulting in increased information processing speed and resource requirements where it is processed and stored. It is fog computing that provides data processing closer to the sources of their generation, which allows to reduce delays and increase the productivity of such a process. However, given the spatial distribution of technical means on which fog computing is implemented, problems arise related to the management of identification and authentication of users and processes in such systems. Therefore, the study of the effectiveness of certain types of authentication models is extremely relevant.

2. Fog computing

With the development of the Internet of Things, computing, and network technologies, a new approach to the implementation of distributed information systems appears—fuzzy computing. Fog computing is an offshoot of the concept of cloud computing, which does not consist of transferring data to specialized processing centers, but in implementing the data processing process closer to the sources of their generation, or in the sources themselves. This approach allows you to distribute the load between various devices, reducing data transmission delays, and optimizing the use of resources, thus increasing the performance of information processing in distributed information systems [1].

Fog computing can be viewed as a hierarchical structure where data is processed at different levels as shown in Fig. 1.

The cloud layer (Cloud) consists of centralized data centers that provide appropriate services and ensure a high level of computational power, data storage, and management of large volumes of data.

The fog layer (Fog) involves intermediate devices between centralized databases and the edge layer, meaning these are devices located at the periphery of the controlled area. Typically, these include intermediate routers or certain low-power data processing centers [2].

The edge layer (Edge) consists of devices that generate data and facilitate its transmission and exchange, often including IoT devices, sensors, smartphones, routers, etc. [3, 4].

From the point of view of the efficiency of application and protection of information, fog computing has several advantages [5].

1. Distribution of sources of data generation and processing. The distribution of fog computing makes it possible to reduce dependence on centralized cloud resources, which at the same time reduces dependence both on the information systems themselves and on external connections to cloud computing, which increases the level of availability of the information to be processed and the survivability of the system as a whole.

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

* Corresponding author.
† These authors contributed equally.

antonio.com237@gmail.com (A. Zahynei); sheblanin@ukr.net (Y. Shcheblanin); kurol@ukr.net (O. Kurchenko); iy.melnyk@kubg.edu.ua (I. Melnyk); smirnov.ser.81@gmail.com (S. Smirnov)

0000-0002-0303-8501 (A. Zahynei); 0000-0002-3231-6750 (Y. Shcheblanin); 0000-0002-3507-2392 (O. Kurchenko); 0000-0001-6041-6145 (I. Melnyk); 0000-0002-7649-7442 (S. Smirnov)

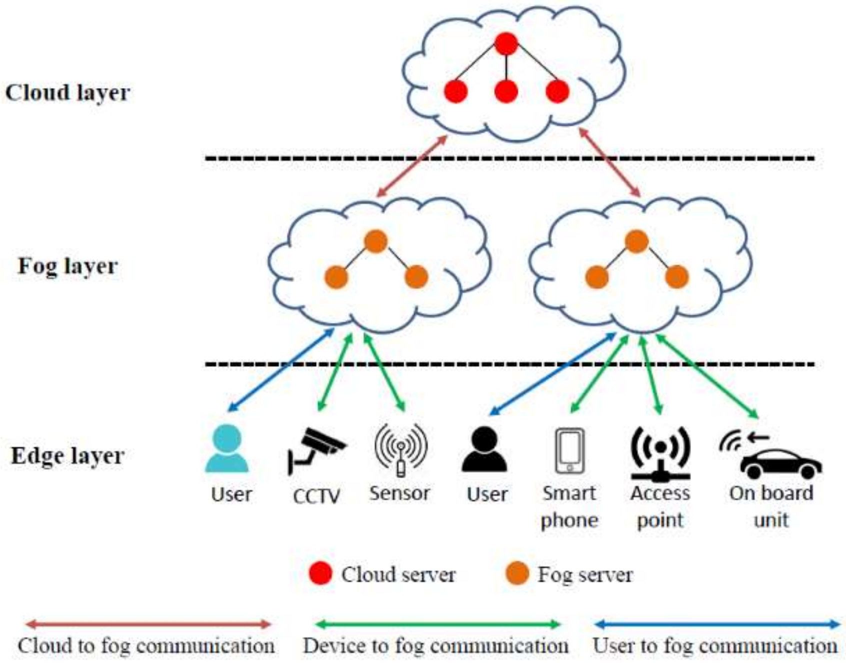

Figure 1: The concept of fog computing

2. Proximity to the data source. Proximity to the data source primarily ensures a reduction in delay time, correspondingly increasing the speed of data processing, and also allows controlling the perimeter where the fog nodes are located, thereby ensuring the protection of devices and the confidentiality of information, because it does not leave the controlled area.
3. Scalability and heterogeneity. Fog computing makes it easy to add a variety of new nodes and devices, thereby increasing the performance of distributed information systems. Nodes and devices can be IoT devices, network elements, servers, and even mobile devices, etc. [6–10].

3. Security issues in fog computing

However, when operating information systems built using fog computing, information security specialists face numerous security challenges, especially when it comes to ensuring the identity and access management process. The distributed nature of fog computing and the use of a large number of diverse devices create risks related to unauthorized access and data compromise.

Fog computing, using numerous nodes, which by their characteristics are located on the border of the controlled zone, creates difficulties in the centralized management of identification and access. It is the lack of a single point of control that makes it difficult to implement uniform access policies. In addition, the dynamic nature of the fog environment (connecting and disconnecting devices and their migration) makes the identification and access management procedure more complex, and therefore the detection of new devices and their reliability verification are key tasks [3].

Many fog nodes and devices operating in the fog environment use only one-factor authentication (PIN code, password, etc.), which makes the entire information system vulnerable to attacks such as brute force and social engineering [11]. At the same time, the use of multi-factor authentication can significantly complicate the processes of identity and access management and create an additional load on fog computing nodes, which will lead to a decrease in device performance. From this, it can be concluded that in information systems that are built using fog computing, especially those that are deployed on critical infrastructure facilities, where unauthorized access can lead to catastrophic consequences, creating a reliable identity and access management system is an important task [5].

4. Description of authentication models and IAM

Identity and Access Management (IAM) [12] models can be used to solve this task. These models make it possible to implement processes of identification and access management of users and devices in different domains, using a single identification (Single Sign-On) or other management methods, reducing the need for duplicating accounts and saving passwords in different elements of the system.

The main types of IAM models include Single Sign-On (SSO), Federated Identity Management (FIM), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Context-Based Access Control (CBAC), Zero Trust Model (ZTM) [13].

Let’s consider the basic principles of the functioning of IAM models.

4.1. Single sign-on model

The Single Sign-On (SSO) model is based on one-time authentication within a session, after which the user gains access to many systems and applications without the need to re-enter credentials [14]. The principle of implementation of the SSO model is shown in Fig. 2. This model significantly increases convenience for users, because there is no need to generate and store credentials for each system in integrity.

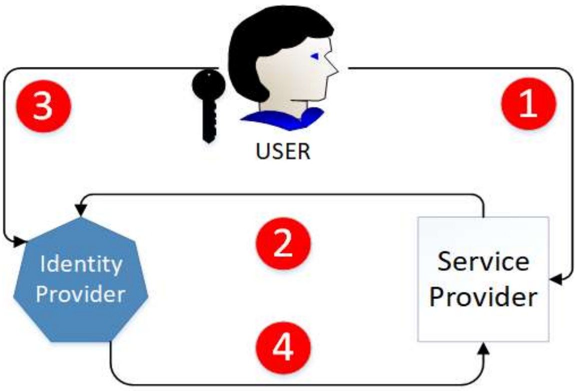

Figure 2: SSO model

According to Fig. 1, in the first stage user accesses the service provider, then the service provider identifies the user and sends the request to get authentication info for this user to the identity provider. In the third stage user logs into the identity provider and after all identity provider gives a response with user authentication info.

In addition, using the SSO model provides centralized management of identity and access to multiple resources of the organization. A number of these advantages create a rather high risk that in case of compromise of one account, an attacker will be able to gain access to all connected systems, and therefore the reliability of the security system, which should provide stable protection against attacks on authentication data, is a direct dependency of the effectiveness of this model as a whole. Most often, this model is used in corporate networks, and cloud services, in particular, on SaaS platforms, where users, after logging in once, get appropriate access to several interconnected applications.

4.2. Federated identity management model

The Federated Identity Management (FIM) model envisages the implementation of a single user identification system that will allow access to resources of many different organizations or domains using a single account based on trust relationships between organizations that ensure effective interaction between them so that users do not need to create different accounts for each system [15]. This model effectively centralizes the inter-organizational level of access management, therefore increasing the level of security through unified identification. This requires high-level coordination and complex management of access policies and security, so it can be a major challenge to configure and maintain such a model. FIM finds its main application among enterprises, government structures, or organizations that often interact with each other and therefore need to share resources or data using a single identity and access management mechanism.

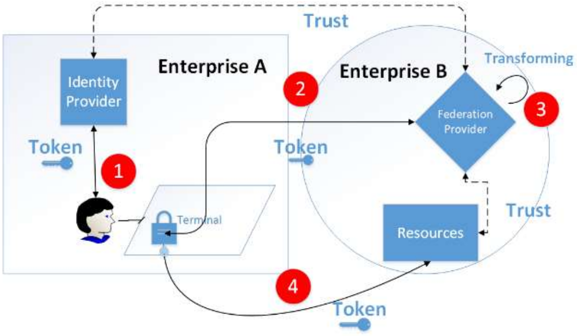

Figure 3: FIM model

The figure shows how clients authenticate through their identity provider (step 1). After the client is successfully authenticated, the identity provider issues a token. The client terminal forwards this token to Enterprise B's federation provider, which trusts the tokens issued by the identity provider to issue a token that is valid for Enterprise B's federation provider (step 2). If necessary, before returning the new token to the client terminal, the federation provider converts the assertions in the token to those recognized by certain resources (step 3). Enterprise B's resources trust the tokens issued by Enterprise B's federation provider and use the assertions in the token to apply authorization rules (step 4).

4.3. Role-based access control model

The Role-Based Access Control (RBAC) model is based on the concept that access to resources in an organization is determined by roles that are assigned to users according to their job duties, and these roles grant certain access rights to systems or data, which allows to simplify the process access management by standardizing rights for entire groups of users instead of setting individual rights for each employee [16]. While this approach allows for efficient management of large groups of users and reduces the risk of errors when setting up access, it has limited flexibility as roles must be manually updated for each new role or change in responsibilities, which can be challenging in large-scale systems with frequent changes in structure companies This model is most often used in corporate management systems such as ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management), where users' access to information resources is strictly controlled depending on their role in the organization.

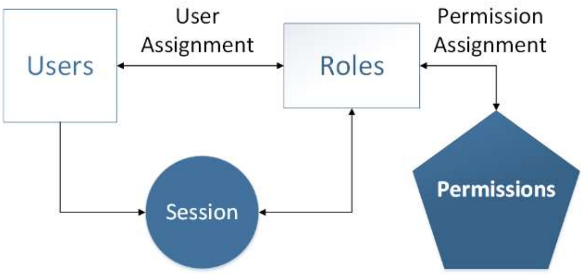

Figure 4: RBAC model

4.4. Attribute-based access control model

The Attribute-Based Access Control (ABAC) model is more complex and flexible than RBAC because it allows access to be granted based not only on roles, but also on other attributes of the user, objects, or environment, such as the user's location, time of day, type of requested data or even the state of the device being accessed from, allowing fine-tuning of access rights based on multiple conditions and context [17]. The main advantage of this approach is that it allows dynamic and precise access control, especially in complex and changing environments, but its implementation requires complex settings and significant resources to support a large number of rules and attributes, which can be a challenge for organizations with limited technical opportunities ABAC is an ideal model for use in government systems or organizations with high-security requirements, where multiple factors must be considered when making access decisions.

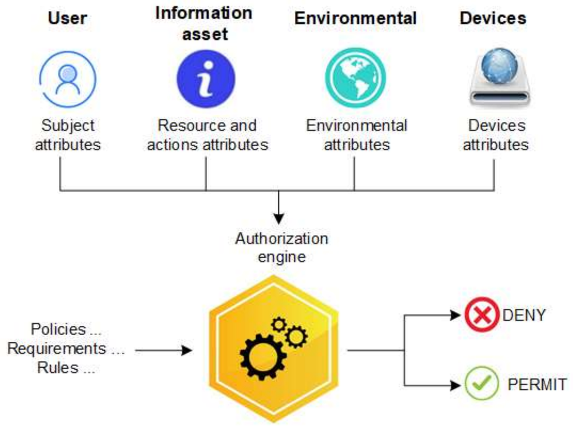

Figure 5: ABAC model

4.5. Zero trust model

The Zero Trust Model (ZTM) is fundamentally different from traditional approaches to security, as it is built on the principle that no user or device can be trusted by default, even if it is inside the corporate network, and every access request must be thoroughly vetted and authorized regardless of the user's location or the status of his device, which allows you to effectively protect systems from unauthorized access and internal threats [18–26]. This approach provides the maximum level of security, as all actions are verified in real-time, however, the implementation of the Zero Trust Model is technically complex and requires integration with many existing systems, which can increase the cost of its implementation and reduce productivity due to constant checks [27]. The main applications of this model are organizations with high-security requirements, such as financial institutions or government agencies, as well as companies operating in cloud or hybrid environments where multiple access points need to be protected.

Each of the considered models of identity and access management has its advantages and disadvantages, which determine the feasibility of their use on different occasions. The SSO and FIM models provide convenience and centralized management but require robust security. RBAC is easier to implement, but less flexible than ABAC or CBAC, which provide more opportunities to manage access in a changing environment, but require significant resources to implement. Finally, the Zero Trust Model provides the highest level of security but is complex to configure and integrate, making it relevant for highly secure environments.

In the case of using these models in a fog environment to manage the identity and access of devices, certain difficulties arise regarding their application, and as a result, security risks that cannot be accepted are increased, namely:

- Single Sign-On provides a single sign-on to access various fog nodes, which provides convenience for users, but if this single account is compromised, an attacker can gain access to many fog nodes and resources, which increases security risks.
- Federated Identity Management is appropriate to use in the case of a shared cloud environment between different organizations or domains, which provides flexibility and scalability of such an environment. However, this creates difficulties in terms of coordination between organizations, as well as in maintaining agreed access policies.
- Role-Based Access Control defines access to fog nodes based on user roles, which provides ease of configuration and access control, as well as flexibility for typical roles, but this flexibility is limited because it can only be applied to well-defined users, to manage new, a constant upgrade of the entire identity and access management system is required to meet the dynamic nature of fog computing.
- Attribute-Based Access Control is a flexible approach that can be effectively applied to build an identity and access control system in fog computing because it uses attributes of the user, environment, and resources to determine access to fog nodes, which can ensure the reliability of access control and adaptation to dynamic changes in the environment. However, the effective use of this method is possible only in the case of applying complex policies for the management of identification and access processes, which require constant control.
- Zero Trust Model ensures the maximum level of security by checking every access request regardless of other factors and circumstances. Suitable for distributed and heterogeneous fog environments with a high level of threat probability and the need to perform full access verification. At the same time, the complexity of implementing and administering such a system forces one to compare the risks and feasibility of using ZTM.

5. Conclusions

Fog computing is a distributed architecture where data processing and storage take place closer to end devices, unlike traditional cloud computing. Identity and Access Management (IAM) in such an environment faces unique challenges due to the dynamism, distribution, and limited resources of fog nodes. Choosing the right IAM models is important to ensure the security and efficiency of fog systems.

One of the more effective IAM models in the framework of fog computing is Attribute-Based Access Control. The ABAC model allows the use of user, device, and context attributes (such as location, time, or device specifications) to control access to resources. In fog computing, this is important to ensure accurate access control, taking into account a variety of conditions and dynamic contexts. The use of attributes such as device state, geolocation, and fog node load level provides flexible access control that adapts to environmental conditions. This is especially relevant for IoT networks, where end devices are dynamic and change their status.

In fog computing, there is often a need to integrate different systems and services that may be managed by organizations or companies. The FIM model allows different systems to trust a user's identification data without having to store this data in each system separately.

The ABAC and FIM models appear to be more effective for providing IAM in fog computing, but it is the combination of FIM and ABAC that allows for simultaneous centralized authentication (via federation) and flexible access control based on contextual attributes.

Thus, in general, the most effective principle of identity and access management will be the combination of ABAC and FIM models. However, depending on the context of use, the combination options may differ, which is the subject of further research.

References

[1] M. Iorda, et al., Fog Computing Conceptual Model, Natl. Inst. Stand. Technol., NIST Special Publication 500–325 (2018). doi: 10.6028/NIST.SP.500-325.

[2] A. S. M. Kayes, et al., A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues, Sensors, 20(9) (2020) 2464. doi: 10.3390/s20092464.

[3] W. Shafik, S. A. Mostafavi, Fog Computing Architectures, Privacy and Security Solutions, Journal of Communications Technology, Electronics and Computer Science, 24 (2019).

[4] O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.

[5] A. Zahynei, et al., (2024). Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 432–439.

[6] V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.

[7] Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25. doi: 10.1109/UkrMiCo52950.2021.9716700.

[8] Y. Shcheblanin, et al., Research of Authentication Methods in Mobile Applications, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 266–271.

[9] O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.

[10] O. Mykhaylova, et al., Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 239–251.

[11] H. Noura, et al., Preserving Data Security in Distributed Fog Computing, Ad Hoc Networks, 94 (2019) 101937. doi: 10.1016/j.adhoc.2019.101937.

[12] C. Singh, J. Warraich, R. Thakkar, IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations, European J. Eng. Technol. Res. 8(4) (2023) 30–38.

[13] B. Cremonezi, et al., Identity Management for Internet of Things: Concepts, Challenges and Opportunities, Comput. Commun. 224 (2024) 72–94. doi: 10.1016/j.comcom.2024.05.014.

[14] S. Mookherji, et al., Fog-Based Single Sign-On Authentication Protocol for Electronic Healthcare Applications, IEEE Internet of Things Journal, 1 (2023). doi: 10.1109/jiot.2023.3242903.

[15] Y. Imine, A. Gallais, Y. Challal, An Efficient Federated Identity Management Protocol for Heterogeneous Fog Computing Architecture. 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (2022). doi: 10.23919/SoftCOM55329.2022.9911414.

[16] M. A. Aleisa, A. Abuhussein, F. T. Sheldon, Access Control in Fog Computing: Challenges and Research Agenda, IEEE Access, 8 (2020) 83986–83999. doi: 10.1109/access.2020.2992460.

[17] Q. Xu, et al., Secure Data Access Control for Fog Computing based on Multi-Authority Attribute-Based Signcryption with Computation Outsourcing and Attribute Revocation, Sensors, 18(5) (2018) 1609. doi: 10.3390/s18051609.

[18] M. Ahmed, K. Petrova, A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments. WISP 2020 Proceedings, 4 (2020).

[19] S. O. Ogundoyin, I.A. Kamil, Secure and privacy-Preserving D2D Communication in Fog Computing Services, Comput. Netw. 210 (2022) 108942. doi: 10.1016/j.comnet.2022.108942

[20] S. Balamurugan, et al., New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, Wiley & Sons, Limited, John (2022).

[21] R. Bensaid, Security and Privacy Issues in Fog Computing for the Internet of Things: An unpublished PhD thesis, Abu Bekr Belkaid University (2023).

[22] M. Whaiduzzaman, et al., HIBAF: A Data Security Scheme for Fog Computing, Journal of High Speed Networks, 27(4) (2021) 381–402. doi: 10.3233/jhs-210673.

[23] B. A. Mohammed, et al., FC-PA: Fog Computing-Based Pseudonym Authentication Scheme in 5G-Enabled Vehicular Networks, IEEE Access, 11 (2023) 18571–18581. doi: 10.1109/access.2023.3247222.

[24] A. Murugesan, et al., Analysis on Homomorphic Technique for Data Security in Fog Computing, Transactions on Emerging Telecommunications Technologies (2020). doi: 10.1002/ett.3990.

[25] R. El Sibai, et al., A Survey on Access Control Mechanisms for Cloud Computing, Transactions Emerging Telecommun. Technol. 31(2) (2019). doi: 10.1002/ett.3720.

[26] M. Al-khafajiy, et al., COMITMENT: A Fog Computing Trust Management Approach, Journal of Parallel and Distributed Computing, 137 (2020) 1–16. doi: 10.1016/j.jpdc.2019.10.006.

[27] P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 97–106.