DISTRIBUTED ARBITER
A Lightweight, and Enhanced Access Control Mechanism for Cloud Computing

by

Khalid Ali ALMARHABI [*]

Department of Computer Science, College of Engineering and Computing in Al-Qunfudah,
Umm Al-Qura University, Makkah, Saudi Arabia

Original scientific paper
https://doi.org/10.2298/TSCI2406969A

Since its discovery, computer technology has played a key role in changing the lifestyles of people and continues to provide countless benefits. Nevertheless, computer technology systems that facilitate smooth integration, such as, cloud computing; are prone to cyber breaches, which has negatively affected its reputation and perception. Therefore, computer technology systems that are secure are needed to curb cyber threats and increase user trust. The primary issue in computer technology systems is that, unlike alternative methods, most cloud access control mechanisms are inadequate. Furthermore, transitioning to a trust-based mechanism is not only complicated and costly but a significantly decision intensive process. As such, this present study investigates how network risks and threats analysis, edge computing and Arbiter, a mandatory access control mechanism, can be integrated into cloud computing to prevent single points of failure. It also examines how these integrating components can decrease the costs and effort required to change an entire operating system to meet the requirements of a trusted system.

Key words: *access control, cloud computing, network risks, edge computing, single points of failure, trusted systems, distributed systems*

Introduction

Computing was once considered rare and costly, but advancements have made it more accessible, with significant improvements in storage capabilities and network infrastructure to handle increasing information needs [1]. Cloud computing is the latest development, providing scalable, cost-effective services that replace traditional expensive computing. It offers vast storage and computational power for handling large data transfers and streams [2, 3]. Cloud computing, essentially a virtual web-based service, adapts to user requirements. The essential role of cloud computing in data storage and transfer necessitates strong security measures. Despite advancements, issues like data integrity and confidentiality due to loose connections and user mistrust in cloud servers persist. Table 1 highlights the primary risks, threats, and challenges associated with cloud computing security. It categorizes the issues into three main aspects: unmanaged attack surfaces and data breaches under risks, insider threats and IoT-based cyberattacks under threats, and challenges like cloud compliance and shadow IT. This table underscores the multifaceted nature of cloud security and lays the foundation for developing comprehensive access control mechanisms and policies. Sensitive data requires restricted ac-

[*] Author's e-mail: kamarhabi@uqu.edu.sa

cess control mechanisms (RACM) to ensure privacy and confidentiality [4]. Organizations implement access control policies (ACP) to regulate cloud data access, protecting sensitive information from unauthorized users [5].

Anonymity in cloud platforms can lead to illegal activities, posing security risks. Registered users have launched cyber-attacks on cloud storage, highlighting the need for enhanced security measures [6]. These attacks can lead to single points of failure (SPOF), causing system collapse. Figure 1 illustrates how threats can create a SPOF, where damage to a key router disrupts all network connections until repaired [7, 8].

Table 1. Cloud security risks, threats and challenges

Cloud attack danger level	Attack name
Risks	• Unmanaged attack surface • Data breach
Threat	• Insider threats • Cyberattacks (malware, SQL injections, and IoT based attacks.)
Challenges	• Lack of cloud security and skills • Identity and access management • Shadow IT • Cloud compliance

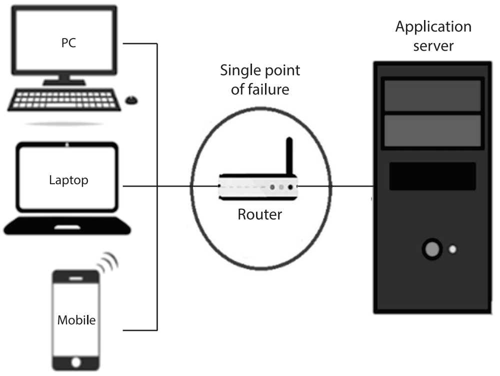

Figure 1. An illustration of an SPOF in a system

As hackers improve their cyber-attacks, the system of systems in corporate and residential networks is no longer isolated, making communication within companies dynamic. Networks and systems now connect across multiple access points, such as the Internet and telephone lines [9]. Al-Marhibi [10] notes that most systems are built on weak communication devices (ACM), making them vulnerable to eavesdropping attacks that collect private information. Hackers can use this information disrupt data flow, inject false data, or destroy information [11]. To counter these threats, organizations implement safeguards like key management, cryptography, antivirus solutions, and firewalls [9]. However, no single solution ensures total security. Discretionary access control mechanisms (DACM) allow information owners to request access but can’t distinguish between legitimate and malicious requests. Role-based access control mechanisms (RBAC) are fundamentally derived from discretionary access control mechanisms (DAC) [12-14]. Mandatory access control mechanisms (MACM) restrict access based on resource sensitivity and user rights, managed by a policy administrator [15]. Role-based access control mechanisms (RBACM) combine features of DACM and MACM [16, 17].

Despite reliable options like security-enhanced linux (SELinux), many organizations use less secure systems due to the high cost and complexity of transitioning from DACM [18, 19]. For instance, SELinux has a default policy with around 1500000 rules [20]. Administrators are often more familiar with commercial DACM like WINDOWS®. Edge computing processes time-sensitive data and ensures network reliability by replicating data across low latency connections, distributed nodes, and dynamic load balancing. This reduces SPOF and enhances security [21, 22]. Strengthening the collaboration between edge computing and cloud communication devices improves resource use and reduces cyber threats.

This study explores building a collaborative ecosystem between edge computing and cloud communication devices to prevent SPOF. It examines the risks and challenges in accessing cloud data and communication devices, focusing on the limitations of DACM [17].

Related work

Studies on this topic fall into three categories: reducing system costs with SPOF, using distributed systems to prevent SPOF, and creating trusted systems to prevent cloud risks. Huang *et al.* [23] emphasized identifying and managing SPOF during system design. Shneiderman [24] suggested evaluating system components to spot SPOF, while Cadavid *et al.* [25] noted that single systems are costly and vulnerable. Chandra *et al.* [26] highlighted the importance of trusted systems in security policies, stating that computing systems should respect privacy and safety. Lv *et al*. [27] argued that resilient systems build trust and must manage information transfer smoothly, avoiding SPOF. Studies suggest that trust in systems can be enhanced by incorporating data authentication and protecting user privacy. Almarhabi [10] developed a cost-effective cloud service model enhancing data protections, while Hachem *et al*. [11] found MACM can address persistent threats but lack flexibility. Alfarni *et al.* [28] stated cloud computing can centralize operations and perform specific tasks, but risks and threats remain distributed.

Almarhabi [10] proposed Arbiter, a lightweight, secure approach based on a MACM, which reduces overhaul costs. Singh *et al.* [3] suggested applying strict ACP to enhance security. The literature review highlighted the need for solutions addressing five requirements: distributed, secure, trusted, financially feasible, and easy to implement. Previous studies on edge computing to solve cloud security issues include Mao *et al.* [29] summarizing security threats and countermeasures for 6G networks, Huang *et al.* [30] exploring image data classification with edge and cloud collaboration, and Savaglio *et al.* [31] implementing K-means clustering for IoT. This study aims to develop a system that is distributed, secure, trusted, financially feasible, and easy to implement, preventing SPOF and enhancing RACM within DACM. It examines risks, proposes solutions for untrusted systems, and develops efficient, adaptable protection for cloud computing data.

Proposed framework

A new framework is needed to enhance trust, ensure data integrity, and minimize cyber-attacks in cloud computing. This framework should leverage edge computing to distribute data and address the weaknesses of ACM, making the system secure, updated, inexpensive, and lightweight. The proposed technique integrates edge computing and communication devices in a distributed system to manage cyber threats and safeguard data. Computing devices face issues like lack of privacy, ineffective fine-grained access control, and SPOF, requiring scalable systems. Fault-tolerant edge computing systems, which use algorithms and redundancies to maintain performance despite failures, are ideal. These systems ensure reliability and availability by identifying and recovering from failures immediately. Effective failure detection and recovery policies are essential, with the detection phase often taking longer than recovery due to recent advancements in recovery techniques.

A fault-tolerant distributed system detects and recovers from failures, commonly using end-to-end timeouts, though these can be inaccurate. Short timeouts risk false positives, while long timeouts cause unnecessary delays. However, such systems are designed to handle unexpected issues. The proposed framework uses a hierarchical approach to access control in cloud systems based on edge gateways, as shown in fig. 2. The first layer includes edge managers (EM) overseeing end-user devices and sub-device clusters. The second layer consists of aggregated edge manager (AEM) nodes facilitating communication between different clusters and managing MACM policies. The final layer, the cloud consortium manager (CCM), comprises nodes that represent cloud storage and verify transactions requested by external sources.

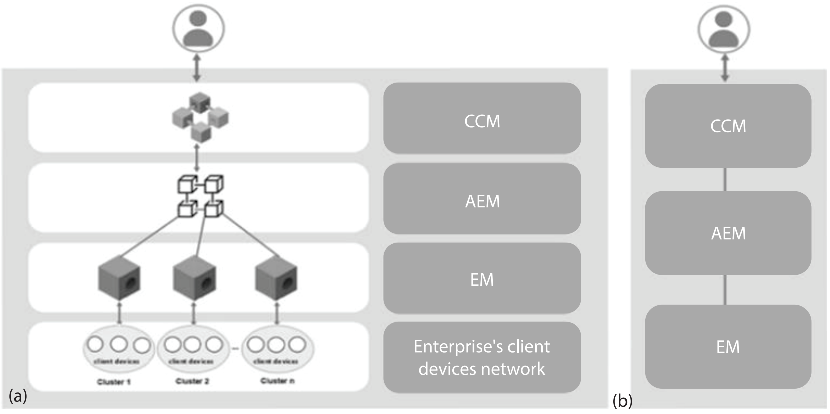

Figure 2. The proposed framework; (a) the layered hierarchical BC framework and (b) the high level software framework

Analyzing cloud risks, threats and challenges

Before beginning to design the system under study, we developed a set of guiding principles that enable network users, whether owned by a person or a company, to follow some procedures that enable him to identify the risks, threats, and challenges present in his network, to work on building an initial infrastructure for the system under study to help it reduce the rate of cyber threats occurred, and these measures were:

- Analysing the user's network security environment to help predict the user's immediate and future risks and reduce the risk of unmanaged attack surface.
- Educate the network users, keep only what the data you need then encrypt and backup it, maintain up-to-date security software and protect portable devices by complex password to minimize data breaches attack.
- Set a security policy for the network, secure the infrastructure, use threat modelling, set up strong authentication measures, eliminate idle accounts and investigate anomalous behaviour in order to minimize insider threats attack.

Use a strong and unique password to change the default router settings and discon nect IoT devices when they are not in use to minimize the IoT cyber-attacks.

Aggregate edge manager layer

In this layer we rely on building the best model of the network user's specific requirements and use cases, which applies the best scenarios that are sensitive to latency and scalability of the emerging edge devices with cloud to obtain the best cost effec-tiveness. In order for this model to be suitable for various networks of individuals and organizations, we concluded that training edge devices takes place through a group or types of training determined according to the needs of the organization, these types are:

- Train edge devices in the cloud and implementing them on the edge.
- Train edge devices in the datacenter and using various cloud management techniques and tools at the edge.
- Train edge devices at the edge and use cloud computing to centralize devices for better learning.

Arbiter device

The proposed framework introduces a novel distributed arbiter (DA) device as the AEM to preserve the existing cloud computing environment with minimal modifications. Table 2 presents arbiter (DA) device features constructed to fit the needs of the presented framework.

Table 2. Arbiter (DA) device features

Feature	Used element
Primary function	Using SELinux to enhance access control in the cloud by addressing the five aforementioned requirements, distributed, secure, trusted, financially feasible, and easy to implement
Incorporated models	Flask model, to enhance access control.
Running environment	Raspberry Pi (RPi) 2 single-board computer as it is affordable, contains essential features, and is commonly used in research settings

The SELinux, is an open-source reliable and trusted microkernel that meets the security standards of the trusted computer system evaluation criteria (TCSEC, orange book). In the cloud environment, the DA acts as a distributed gateway, connecting to servers and ensuring that the ACP' of an organisation are enforced effectively as shown in fig. 3.

As such, all access requests will pass through the DA, which uses the previous stated procedures in section (A), the trained model for the edge device and MACM to make permission decisions based on the organisation's policy administration settings. Therefore, by routing all access requests through the DA, the framework is a robust solution that enhances security and helps organisations maintain control over their cloud resources.

The security gateway application of the DA uses components of web service technologies that, when combined, bless it with distributed and platform-independent software capabilities. It is advantageous to use such technologies in a cloud environment as they are reusable, interoperable, scalable, adaptable, and maintainable.

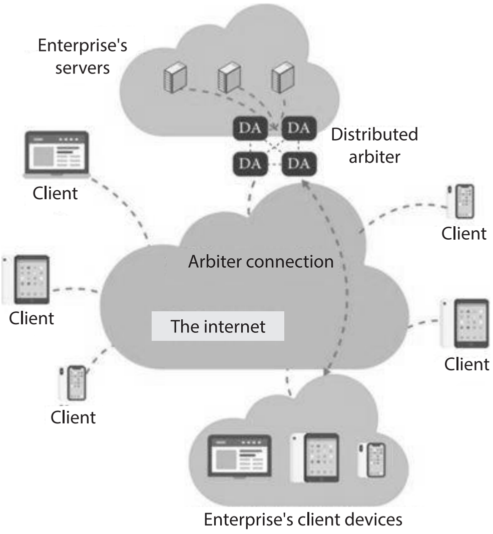

Figure 3. The position of the DA in the cloud environment

Therefore, using such technologies to co-ordinate with other machines will decrease the cost and amount of resources required. There are two main components of web service technologies in the DA. A policy administrator, as explained in our previous work [9], and a distributed gateway-based security shown in fig. 4.

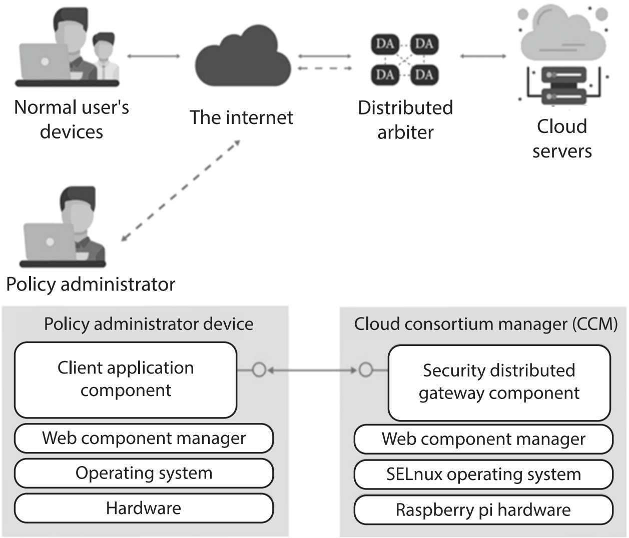

Figure 4. The proposed framework of the DA

Policy administrator and normal user's device

This main component is designated for the individual responsible for defining the policy, be they the chief security officer (CSO), policy administrator, or the company's CEO, as this individual plays a crucial role in establishing the security priorities for initial data and users.

Distributed gateway-based security

As the core of the proposed DA framework, this component is responsible for overseeing all the subcomponents; such as enforcing access control, the encryption policy, verifying signatures, authentication, auditing, and controls with which to manage these subcomponents. The role of the DA is to make access decisions according to the previous stated procedures in section (A), the trained model for the edge device and MACM by denying all access unless permission is, first, granted by the policy administrator.

Proposed use case

Advanced computing has become more urgent with the advent of 5G technology in communications networks, which in turn reduces access time, increases network speeds and data transfer capacity, and increases efficiency. The 5G technology in telecommunications networks enables data transfer at speeds of more than 20 GB per second and the ability to keep more than a million devices connected to the network in every square kilometer.

The proposed framework will enable communications service providers (CSP) to use edge computing to route user data traffic to edge nodes in a secure, more speed and cost-efficient manner. The proposed framework will also help in build a strong edge computing infrastructure in 5G networks, because the stages of data analysis and training are carried out based on the user's usage policies, which were previously mentioned in the section (B). This increases the confidence and stability of the network and secures data transmission in it. All that remains is the necessary need to increase the security of the edge nodes by managing and monitoring them, which in turn provides another level of data security.

Evaluation and discussion

To examine the efficacy of the proposed framework, a qualitative security analysis was conducted to assess how well it addressed fundamental security objectives, namely, confidentiality, integrity, and availability, as well as mitigated primary security threats. Its performance overhead was evaluated as well.

Security analysis

The CIA triad – confidentiality, integrity, and availability – was used to evaluate the security of the proposed framework. Confidentiality ensures that information is accessible only to authorized individuals, integrity ensures information remains accurate and unaltered, and availability ensures information is accessible to trusted users. The framework's ability to prevent CIA-related threats was assessed.

Access control policy testing

Various attacks were simulated during the transfer, processing, and storage stages to test the ACP's efficacy. Ten attacks targeted the ACP: five during processing and five during storage. These attacks modified the ACP, changing the hash value detected by the policy administrator, as shown in fig. 5.

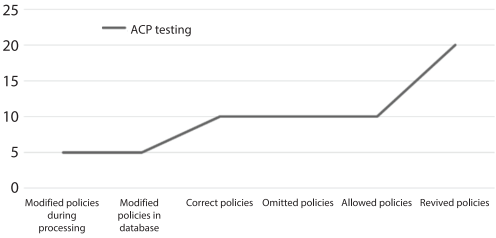

Figure 5. The number of policies uploaded, received, saved, and rejected

Threats to integrity

Protecting data integrity is crucial to prevent unauthorized modifications. Traditional centralized approaches are vulnerable to exploitation. This study created a distributed system to enhance database integrity and resilience against tampering. Verification and validation were conducted using white and black box testing methods, with no faults or failures observed. The framework successfully satisfied the CIA objectives and mitigated primary security threats while maintaining acceptable performance overhead.

Conclusions

Despite the rise in cyberattacks, cloud computing remains crucial for business growth, evolving into an edge computing model that accesses a dynamic pool of resources like applications, networks, databases, and servers. Introduced in 2006, it has transformed computing but requires changes like defining usage policies and integrating ACM to enhance security and effectiveness. The lack of restrictive policies in cloud computing makes it vulnerable to misuse, negatively affecting demand due to perceived vulnerability and cost. Engineers must install RACM to secure databases and deny unauthorized access, increasing the demand for cloud computing. This study examined various ACM and found existing mechanisms insufficient, while trust-based mechanisms are complex and expensive. Integrating network threat analysis, edge computing, and MACM can reduce cyber-attack risks, address SPOF, enhance security, and lower costs.

Future work should evaluate integrating Arbiter into cloud computing environments to improve system security and resilience. Developing strategies for integrating Arbiter can help organizations transition more secure systems. Addressing current ACM shortcomings and adopting trust-based approaches like edge computing will enhance security and confidence in cloud computing, benefiting individuals, organizations, and society. In conclusion, further research on implementing Arbiter and practical approaches to secure systems will increase the adoption of reliable cloud computing solutions.

References

[1] Davison, C. B., *et al*., Factors for Cloud Computing Technology Adoption: An Exploration of Scaling Strategies, *Journal of Technology Research*, *9* (2020), pp. 1-11

[2] Chang, C., *et al*., Internet of Things (IoT) and New Computing Paradigms, *Fog and Edge Computing: Principles and Paradigms*, *6* (2019), Jan., pp. 1-23

[3] Singh, S. P., *et al*., Fog Computing: From Architecture to Edge Computing and Big Data Processing, *The Journal of Supercomputing*, *75* (2019), Nov., pp. 2070-2105

[4] Xu, Q., *et al*., Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption, *IEEE Access*, *6* (2018), June, pp. 34051-34074

[5] Jessintha, J. P., Anbuselvi, R., Behaviour Analysis Model with Level Based Access Restriction Algorithm for Cloud Security Development, *International Journal of Advanced Research in Computer Science*, *9* (2018), 1

[6] Chang, V., *et al*., Cloud Computing Adoption Framework: A security Framework for Business Clouds, *Future Generation Computer Systems*, *57* (2016), Apr., pp. 24-41

[7] Trope, R. L., Ressler, E. K., Mettle Fatigue: VW's Single-Point-of-Failure Ethics, *IEEE Security and Privacy*, *14* (2016), 1, pp. 12-30

[8] Saeed, R., *et al*., An Automated System to Predict Popular Cybersecurity News Using Document Embeddings, *CMES-Computer Modelling in Engineering and Scienc*es, *127* (2021), 2

[9] Kabir, S., Papadopoulos, Y., Computational intelligence for safety assurance of cooperative systems of systems. Computer, *53* (2020), 12, pp. 24-34

[10] Al-Marhabi, K., Arbiter: A Lightweight, Secured and Enhanced Access Control Mechanism for Cloud Computing, *Proceedings*, IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-5

[11] Hachem, J. E., *et al*., Modelling, Analyzing and Predicting Security Cascading Attacks in Smart Buildings Systems-of-Systems, *Journal of Systems and Software*, *162* (2020), 110484

[12] Singh, M. P., *et al*., A Role-Based Administrative Model for Administration of Heterogeneous Access Control Policies and Its Security Analysis, *Information Systems Frontiers*, 2021, https://doi.org/10.1007/s10796-021-10167-z

[13] Benantar, M., *Access Control Systems: Security, Identity Management and Trust Models*, Springer Science and Business Media, Berlin, Germany, 2005

[14] Kuhn, D. R., Chandramouli, R., *Role-based Access Control* [Electronic Resource], Artech House, 2003

[15] Bates, A., *et al.*, Take Only what You Need: Leveraging Mandatory Access Control Policy to Reduce Provenance Storage Costs, *Proceedings*, 7th USENIX Workshop on the Theory and Practice of Provenance (TaPP 15), Edinburg, Scotland, UK, 2015

[16] Biswas, P., *et al.*, A Unified Administrative Model for Role-Based Access Control, In Information Security, *Proceedings*, 19th International Conference, ISC 2016, Honolulu, Hi., USA, 2016, pp. 218-230

[17] Xue, K., *et al*. Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage*, IEEE Transactions on Information Forensics and Security*, *13* (2018), 8, pp. 2062-2074

[18] Liu, T., Agrawal, P., A trusted integrity measurement architecture for securing enterprise network, *Proceedings*, IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China, 2011, pp. 726-731

[19] Wadhwa, A., Gupta, V. K., Proposed Framework with Comparative Analysis of Access Control and Authentication Based Security Models Employed over Cloud, International Journal of Applied Engineering Research, *12* (2017), 24, pp.15715-15722

[20] Marouf, S., Shehab, M., SEGrapher: Visualization-Based SELinux Policy Analysis, *Proceeding*s, 4th Symposium on Configuration Analytics and Automation (SAFECONFIG), Arlington, Va., USA, 2011, pp. 1-8

[21] Ren, S., Qiu, S., Cheng, K., An Edge Computing Algorithm Based on Multi-Level Star Sensor Cloud, *CMES-Computer Modelling in Engineering and Sciences*, *136* (2023), 2

[22] Ren, J., *et al.*, An Edge-Fog-Cloud Computing-Based Digital Twin Model for Prognostics Health Management of Process Manufacturing Systems, *CMES-Computer Modelling in Engineering and Sciences*, *135* (2023), 1, pp. 599-618

[23] Huang, J., *et al*., Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism, *IEEE Transactions on Industrial Informatics*, *15* (2019), 6, pp. 3680-3689

[24] Shneiderman, B., Human-Centered Artificial Intelligence: Reliable, Safe and Trustworthy, *International Journal of Human-Computer Interaction*, *36* (2020), 6, pp. 495-504

[25] Cadavid, H., *et al.*, Architecting Systems of Systems: A Tertiary Study, *Information and Software Technology*, *118* (2020), 106202

[26] Chandra, K., *et al*., How Designers Use Design Principles: Design Behaviors and Application Modes. *Journal of the Association for Information Systems*, *23* (2022), 5, pp. 1235-1270

[27] Lv, Z., *et al*., Trustworthiness in Industrial IoT Systems Based on Artificial Intelligence, *IEEE Transactions on Industrial Informatics*, *17* (2020), 2, pp. 1496-1504

[28] Algarni, S., *et al.*, Blockchain-Based Secured Access Control in an IoT System, *Applied Sciences*, *11* (2021), 4, 1772

[29] Mao, B., *et al*., Security and Privacy on 6G Network Edge: A Survey, *IEEE Communications Surveys and Tutorials*, *25* (2023), 2, pp. 1095-1127

[30] Huang, Y., Zhang, W., Research on the Methods of Data Mining based on the Edge Computing for the IoT, *Proceedings*, IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6

[31] Savaglio, C., *et al.*, Data Mining at the IoT Edge, *Proceedings*, 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019, pp. 1-6

Paper submitted: June 23, 2024
Paper revised: September 18, 2024
Paper accepted: October 30, 2024