American Journal of Information Science and Technology
2024, Vol. 8, No. 2, pp. 45–55
https://doi.org/10.11648/j.ajist.20240802.13

Research Article

The Need for Adaptive Access Control System at the Network Edge

Muhammad Bello Aliyu*, Hassan Suru, Danlami Gabi, Muhammad Garba, Musa Argungu

Department of Computer Science, Kebbi State University of Science and Technology, Aliero, Nigeria

Abstract

The emergence of edge computing, characterized by its distributed nature and real-time processing, necessitates a paradigm shift in access control mechanisms. Traditional, static methods struggle to adapt to the dynamic and heterogeneous environment of edge computing. This research addresses this gap by proposing an Adaptive Risk-Based Access Control (ARBAC) model specifically designed for edge environments. The objective of this research is to develop a robust access control system that dynamically responds to the changing security landscape of edge computing. The proposed ARBAC model integrates real-time data on user context, resource sensitivity, action severity, and risk history to dynamically assess the security risk associated with each access request. This approach ensures a balance between robust security and user experience by tailoring access controls based on the specific context. The research builds upon the growing recognition of the limitations of traditional access control methods in edge environments. Existing literature highlights the need for adaptive and risk-based access control models to address the dynamic nature of edge computing. This research contributes to this evolving field by proposing an ARBAC model that leverages real-time information for contextually relevant access decisions. The proposed ARBAC model offers several advantages. By dynamically adjusting access controls based on risk levels, the model enhances security and ensures compliance with regulatory requirements. Additionally, it improves network performance by reducing load and facilitating faster access to resources. Furthermore, the model's scalability makes it suitable for managing access in large-scale edge deployments. In conclusion, this research proposes an ARBAC model that aligns with the dynamic nature of edge computing environments. By leveraging real-time data and contextual information, the model offers a robust and adaptable approach to access control, promoting security, compliance, performance, and scalability in edge computing. This research paves the way for further exploration and implementation of ARBAC systems, empowering organizations to effectively manage access control in the evolving landscape of edge computing and IoT.

Keywords

Adaptive Access Control, Adaptive Security, Access Control, Edge Computing, Risk-Based Access

1. Introduction

In recent times, cloud computing has played a vital role to meeting Information Technology requirements. Cloud computing defines a model that permits global, accessible, on-demand reach to a common collection of computing re-

*Corresponding author: mbacaspet@gmail.com (Muhammad Bello Aliyu)

Received: 17 April 2024; **Accepted:** 31 May 2024; **Published:** 14 June 2024

sources such as storage, servers, networks, computations, services and applications; that can be swiftly created and deployed with little to no communication between service provider and cloud data center. The utilization of cloud computing approach has increased the communication frequency between devices, such as smartphones, computers, wearables and so on [1]. In spite of the benefits inherent in cloud computing, a few large-scale data centers have been established by public cloud providers globally. These large-scale data centers are equipped to assist a very large user base with sufficient computing resources. However, the centralized nature of these resources indicates a large gap between the device of the user and their clouds, resulting in the increase of latency and jitter on the network [2]. Thus, cloud services lack direct access to local related information of users, such as detailed location, network statuses, and mobility behaviour. As well as, various real-time prerequisites such as context awareness, mobility support, reduced latency and reduced jitter [3]. These limitations have given rise to many emerging paradigms such as mobile (cloud and edge) computing and fog computing. The mutual denominator is that, Edge Computing allows applications to run on network nodes (edge). It is noteworthy that every knowledge model, whether implicit or explicit, is dedicated to some conceptualization; and ontology explicitly specifies the conceptualization. Therefore, an ontology is the assembly of various entities and their relationship [4].

Thus, from an ontological perspective, recognizing edge computing characteristics, features, behaviours, and other related important aspects, are vital for an adequate understanding of its conceptualizations. Considering cloud computing taxonomy as a pathway, an edge computing model can be built systematically by unifying its features into groups and subgroups. Edge Computing defines a distributed system of computing and storage at the network edge closer to the sourcing devices, hence allowing real-time computing tasks. Compared to cloud computing paradigm, edge computing allows data collection, analysis and usage on the device of the user or close to it in a distributed way. Although, decentralized system has been widespread before the centralized system, it has become more significant with the erratic increase in the data volume, traffic, analysis, and storage, with bandwidth and security as limiting factors. Thus, edge computing can be considered as a decentralized cloud computing paradigm and as such a complement to the current cloud computing methodologies [5]. In edge computing, infrastructure providers own and deploy edge data centers, which are implementing a multi-tenant virtualization infrastructure, wherein any customer can utilize the data centers' services. Furthermore, although edge data centers are autonomous and cooperative, they are still connected to the traditional cloud. Hence, an ordered multi-layered architecture unified by a network structure is possible. Also, considering existing underlying or core infrastructure, various support mechanisms can be provided, such as registration and authorization services. And trust domains, such as edge infrastructure, can cooperate to produce an open network where vast number of customers can be served [3].

In addition to the continuous advancements in wireless sensor networks, ubiquitous computing, and communication, the number of interconnected devices is growing. Edge computing is a key player in several of these sectors, facilitating internet-based communication between disparate physical devices that are each uniquely identifiable [6]. Consequently, edge computing makes available solutions by mining and processing the basic data and information at the source with very little to no data center capacity. And afterwards, forwards to the central cloud data center; thus, increases organizational profit at different levels such as cost saving, reduced cloud connection time, instant data queries analysis as well as most precise and fastest user response [7]. In light of this, infrastructures for registration and permission are essential for registering and examining the credentials of different entities in order to approve their requests to do specific tasks. In the absence of an authorization infrastructure, anyone can misuse the resources of the infrastructure, assume the role of an administrator and manage its services, and allow attackers to access all resources. Because edge concepts have advantages, it is imperative that an authorization infrastructure be implemented in each trust domain. This enables trust domain owners to disseminate and put their security guidelines into action [3]. Such infrastructures can, in theory, process any entity's credentials based on an established trust relationship. In addition, taking into account a variety of contextual data, such the location, who owns the resources, and the details of the authentication procedures. Access control management system became essential as a result.

However, traditional access control techniques are limited by inflexible and invariable access control policies which are inappropriate to dynamic and heterogeneous settings, which presents a continual change in available users and resources as well as increasing administrative complexity [8]. However, the advent of new access control prerequisites resulting from existing security needs and the need of very dynamic environments, has brought about the advancement of access control models based on risk management [9]. A major benefit of risk-based access control models is the incomparable handling of access requests, when access must be granted to execute an important action, even without prior authorization, enabling flexibility in accessing resources. In order to respond to access requests and provide a dynamic response, this research uses an adaptive risk-based access control system that takes into account real-time data and information. In principle, each access request must be dynamically analyzed, with regards to predefined policies and contextual information and may exceptionally grant access request if the risk is tolerable.

1.1. Objective of the Study

This research seeks to elucidate the need for adaptive Ac-

cess Control system at the Network edge. The objectives are to: provide an understanding of access control policies; carry out a literature review of existing access control strategies and identify inherent limitations. Based on these limitations, we propose an access control system, discuss on findings and conclude.

1.2. Significance of the Study

Traditionally, access requests have often been granted based on static and rigid policies, which do not consider real-time risk factors. By not considering these risk factors, trusting has been implicit, such that access is granted based on having the correct credentials. However, it is not ideal to grant access at the time of connection as the risk level may change. Adopting adaptive access is important for ensuring the right users are granted connection to sensitive data and information. This research aims to show that the application of an Adaptive Access Control System offers a better and improved fine-grained access control to edge services while increasing network efficiency, flexibility and reliability.

1.3. Contribution to Knowledge

There are various ways in which creating an adaptive access control system at the network edge through an adaptive risk-based methodology might advance knowledge:

Improving security: One of the main benefits is that it can help improve the security of an organization's network by controlling and monitoring access to resources. By using an Adaptive Access Control System to dynamically adjust access controls based on the contextual features associated with a particular request, providing an additional layer of security.

Enhancing compliance: An adaptive approach offers a means of controlling access to sensitive data and resources, which can assist firms in meeting regulatory compliance obligations.

Enhancing Performance: An Adaptive Access Control System at the network edge, can reduce the load on the internal network, which may result in better performance, and faster access to resources.

Enhancing Scalability: An Adaptive Access Control System at the network edge can also improve scalability, making it easier for organizations to manage access controls for large numbers of users and resources.

Adaptive Security: This research can also contribute to the field of adaptive security by providing an understanding of how security measures can be adjusted in real-time based on the level of risk.

2. Literature Review

2.1. Edge Computing

Cloud computing have been trending owing to its assemblage of computing resources (server, network, storage) shared to serve numerous users, using a multi-tenant model. The cloud computing paradigm offers an assortment of deployment and service models, ranging from private to public clouds, and from Infrastructure as a Service (IaaS) to Platform as a Service models (PaaS) among other services. Its economical and efficient services have made it wildly accepted in various fields. Thus, producing a global increase of cloud and edge computing. Despite the inherent benefits of cloud computing, the centralize nature of resources infers a large gap between consumer devices and their clouds, thus, increasing the network latency and jitter [2]. As well as, cloud services lacking the ability to access local contextual information, such as detailed location, network statuses, mobility behaviour. For these reasons, in recent years, several emerging paradigms have emerged, such as edge computing. A new paradigm in computing called "edge computing" promises to speed up service requests and bring cloud computing services closer to customers. Numerous additional technological applications have improved as a result of edge computing. Thus, enabling the provision of a large variety of services and information in large quantities [10].

The goal of edge computing is to offer a network edge computing platform with cloud computing capabilities. Reduced latency, more bandwidth, access to radio network data, and location awareness are benefits of placing cloud services at the network edge. This enables the implementation of new services and the improvement of current infrastructure. Third-party service providers are also free to choose how their services are positioned. Additional application areas include gateways for the Internet of Things, smart video acceleration, linked autos, and augmented reality, among others [3]. In order to establish an edge computing environment, virtualization servers must be positioned at multiple network edge locations. LTE/5G base stations (eNodeB), 3G Radio Network Controllers (RNC), and multi-Radio Access Technology cell aggregation sites are a few examples of deployment locations. Services connected to edge computing as well as other relevant services should be hosted on this virtualization infrastructure [11].

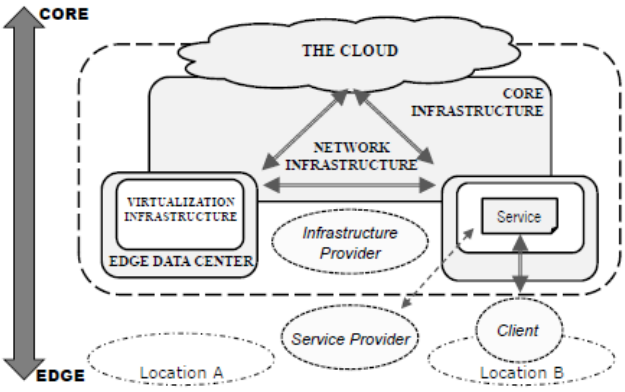

Figure 1. *Functional structure of edge paradigms [3].*

2.2. Benefit of Edge Computing

There are several noticeable benefits of implementing Edge Computing, which can be categorized as follows:

Communication: Edge Computing networks can tremendously improve network communication performance, thus, reduces latency, bandwidth usage, power consumption, and packet data complexity [12]. This enables the fulfilment of Quality of Service (QoS) requirements in real-time applications and services.

Computation: In edge computing networks, data processing and computation are done at the edge servers, reducing the enormous burden on the centralized cloud servers. This promises improved network efficiency considering utilization of resources and priority management. [13]

Storage: Since end devices typically lack storage capabilities, edge computing servers can offer storage services, by transferring all generated and collected data to the storage servers. Hence, assisting with handling load balancing and failure recovery issues, resulting in a substantial improvement of Quality of Service (QoS) [14].

2.3. Challenges of Edge Computing

Even with the numerous benefits of edge computing, there still many key challenges such as:

Security and Privacy: Since sensitive information will be exchanged and, in some cases, put in storage in the edge computing servers; privacy and security are critical limitations in such decentralized network. This makes edge computing networks more susceptible to cyber-attacks and threats. By and large, attacks are faced during the three essential edge computing resources (communication, computation, and storage) [3].

Network Heterogeneity: Edge Computing networks are heterogeneous, bringing together various topologies, servers and platforms. Hence, guaranteeing continuous functions for devices, characterizes a major limitation in a complex and sophisticated environment.

Resource Management: Governing, handling, and enhancing the three key resources of Edge Computing networks, which are communication, computation, and storage, is a crucial issue that requires appropriate investigation. This issue is as a result of the heterogeneousness of service providers, edge applications, devices and so on.

Smart System Support: The integration of smart devices will provide an unparalleled opportunity for data collection and exchange, provision and optimization of resources, and management. However, there are limitations in enabling multiple edge computing servers to store, process and exchange data from these multi-platform devices across a large topographical area, in a way consistent with optimum and well-timed management decisions [14].

2.4. Access Control Mechanism

It is important to remember that access control is used to restrict actions taken by authorized users and stops any actions that might lead to a security breach. The security objectives of availability, integrity, and confidentiality should be met. Authorization policies are imposed via access control techniques, which restrict users from accessing things they shouldn't be able to, hence imposing consent [15].

Access control is currently used for resource management at several levels in many different domains, allowing only authorized users to access resources in an authorized manner. An access control model encompasses five essential elements [16]:

Subjects: This characterizes several units that represent users or agents, requesting access to resources.

Objects: This defines the system resources, which includes data and/or information, that needs to be retrieved by the subjects.

Actions: This characterizes several categories of activities (read, write, execute) that subjects can carry out on a specific object.

Privileges: These are the approvals granted to subjects to enable the carrying out of a specific activity on a specific object.

Access policies: These are a collection of rules that stipulate the criteria needed to ascertain the access decision for each access request, whether granted or denied.

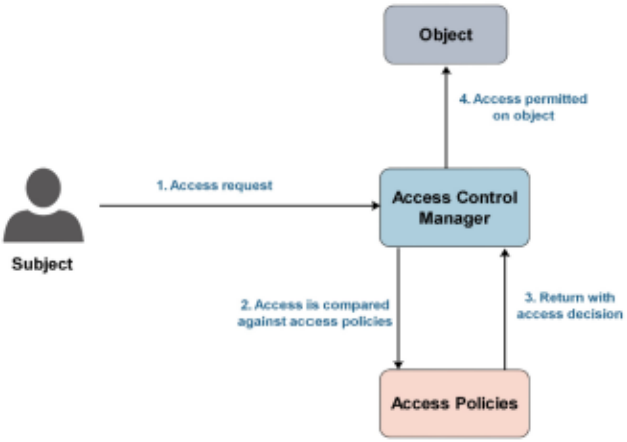

Figure 2. *An access control process flow [17].*

It begins when a subject requests access from the access control manager to a specific object. Then, the subject's credentials are compared against the access policies, by the access control manager, to resolve whether or not to grant or deny access respectively. If granted, the subject is allowed access by the access control manager to the object. While if denied, the subject is not allowed access by the access control manager to the object.

2.5. Traditional Access Control Mechanism

Static and prearranged policies are used by traditional access controls to control access decisions. Thus, these static rules make the same choice in various instances. While traditional access controls have been successfully implemented in many environments to address various issues, their primary purpose is to establish a connection between the resources that a request for access is made for and the information pertaining to an access control policy. The management of an access control implementation can range from dealing with an unforeseen circumstance to many malicious entities acquiring access to active accounts. Because of these limitations, using static, pre-planned policies to address unforeseen scenarios is not a viable option when using traditional access control techniques. More flexibility in resource access is needed for many dynamic and decentralized systems, and this tight approach does not provide the necessary robust security safeguards. Alternatively, in situations where contextual information are not collected during the access request, this static method works well [18]. There are numerous traditional access control techniques which includes [17]: Access Control List (ACL); Discretionary Access Control (DAC); Mandatory Access Control (MAC); Role-Based Access Control (RBAC).

2.5.1. Advantages

Easy to comprehend, assessment, and sustain.

Faster to be produced.

It applies an impartial method; thus, the result is more accurate.

No contextual data needed; thus, access decisions are faster.

2.5.2. Disadvantages

Flexibility is affected as it cannot adapt to changes in conditions.

It has an imperfect policy and lacks a plan for all possibilities; thus, problems may arise.

Poor scalability particularly with a bulky number of subjects and objects.

Difficult to bring up-to-date access rights for individual users.

2.6. Dynamic Access Control Mechanism

The core idea behind dynamic access control techniques is that access choices are made by taking contextual factors into account in addition to access policies that are gathered at the time of the access request [19]. As a result, it offers more flexibility and may be adjusted to different situations when choosing access. When offering a well-organized and flexible access control method, accepting dynamic access control should be a top focus. However, because current access control methods rely on strict access regulations, they are unable to offer recommendations for enhancing automation. The human analysis and lack of automation in current access control techniques make them prone to mistakes and other forms of cyberattacks. Furthermore, when addressing a threat that was unknown before, typical access restrictions have limitations when it comes to addressing risks and hazards in real time. This is based on the facts that decisions about access are based on a set of policies that are limited to solving issues that have already been identified and are unable to quickly determine various access control scenarios [20]. Dynamic access control techniques use real-time aspects including trust, setting, risk, history, and operational requirement to offer access decisions, in contrast to static regulations. Furthermore, dynamic access control can adjust to various situations when making decisions.

2.6.1. Advantages

Adjust to unexpected conditions that is not expected by the policies.

Flexibility improves while accessing system resources.

Real-time risk and threat resolution, especially when addressing an earlier danger.

2.6.2. Disadvantages

Increased complexity, particularly with several contextual characteristics.

Contextual features are adjusted based on the application area.

Effective contextual features are difficult to identify for the access control technique.

Prejudice in designating a level to the contextual feature.

Time complexity increases for treating contextual features with the policy.

Increased computing power is required.

2.7. Review of Related Literature/Works

The control of access requests is a pivotal component in ensuring the security of network access. Existing access control mechanisms, predominantly reliant on public keys, have shown complexity and vulnerabilities against attacks. [21] introduced novel access control methods based on hash trees. Their evaluation highlighted reduced computation, storage, and communication complexities compared to prevailing methods. These approaches demonstrated resilience against node capture, replay attacks, and request-based threats. However, security levels remained consistent with earlier mechanisms. a [22] dressed access control in cloud computing with categorical quantum cryptography. Their protocols, analyzed via graphical language, showcased unrestricted security and current implementation feasibility. Meanwhile, [23] responded to limitations in attribute-based access control (ABAC) with fuzzy-extended ABAC (FBAC). Experimental assessments revealed enhanced time efficiency and serviceability while maintaining security, albeit at a similar complexity level.

Advancements in virtualization technology have prompted

access control strategies. D. Lang et al. [24] introduced a Docker role access control mechanism, rectifying gaps in other strategies. Additionally, in Software Defined Network (SDN) settings, [25] presented an MD-UCON access control model, tailored for multi-domain SDN needs, while ensuring adaptability and finer granularity. With the surge in Internet of Things (IoT), [26] conducted an exhaustive study on Context-Aware Access Control (CAAC) mechanisms, addressing Internet of Things' shift to dynamic cloud environments. A. I. Abdi et al. [27] scrutinized blockchain-based access control for Internet of Things, leveraging decentralization and tamper-proof features to resolve security issues. Yet, concerns around privacy integration remained. Blockchain's influence extended to medical data sharing. [28] proposed a blockchain-based privacy-preserving scheme, bolstering privacy and access control for medical data sharing. Similarly, [29] decentralized access control through blockchain implementation, preventing tampering and single points of failure.

Incorporating multi-level security, [30] introduced the Matrix-Domain-Security-Label Access Control Model (MSAC), emphasizing coarse-grained scope classification for cross-domain and cross-organization MLS 'Need-to-know'. [31] addressed Internet of Things' scale with a blockchain-backed attribute-based access control mechanism, ensuring trusted access control while preserving privacy. Attribute-based access control found application in blockchain environments. [32] developed a revocable attribute-based access control system, enhancing security by enabling attribute revocation. In conclusion, access control mechanisms have evolved to address intricate security challenges, spanning cloud computing, Internet of Things, virtualization, and blockchain. These studies collectively strive to enhance security, privacy, and efficiency in an increasingly interconnected digital landscape.

2.8. Limitations of Reviewed/Related Literature

From the literatures reviewed, some of the proposed access control strategies employed in Edge computing services, for achieving fine-grained access control are able to meet their requirements but some still suffers from the following:

1) Lack of real time, automated monitoring
2) Security policy issues
3) Poor performance and accuracy
4) Computational complexity
5) Algorithmic bottleneck.

3. Methodology

The effective management of network security is paramount in safeguarding against both external and internal attacks. These attacks pose a significant threat to the functionality, availability, and integrity of Information Technology (IT) systems. To address these challenges, a comprehensive security strategy is essential, which necessitates a deep understanding of the security requirements and a careful assessment of the existing security landscape. The conceptual framework presented here draws from established security standards such as the National Institute of Standards and Technologies (NIST) Cybersecurity Framework [33], COBIT 5 [34], ISA 62443 [35], and ISO/IEC 27000 [36] to provide a holistic approach to adaptive access control system implementation. The National Institute of Standards and Technologies (NIST) Cybersecurity Framework serves as the foundational basis for this conceptual framework. It offers a taxonomy and methodology for characterizing both current and desired security strategies. It emphasizes communication among stakeholders to address cybersecurity threats, guides risk evaluations, and manages risks in the face of vulnerabilities, threats, and risk tolerance. In addition to the National Institute of Standards and Technologies (NIST) Cybersecurity Framework, this framework integrates principles from other renowned security standards such as COBIT 5, ISA 62443, and ISO/IEC 27000. These standards provide a comprehensive perspective on cybersecurity, and by referencing specific sections from each, a unified strategy for cybersecurity can be developed. The objective is to harness common principles from these standards to outline a robust approach to adaptive access control system design.

The primary focus of this conceptual framework is to counteract security threats and mitigate risks to Information Technology systems. Security threats are recognized as detrimental to the functionality, performance, availability, and integrity of Information Technology systems. The goal is to proactively reduce the impact of potential security threats to a level where Service Level Agreements (SLAs) can be upheld while adhering to risk management principles [37]. The framework emphasizes an adaptive security approach to effectively respond to evolving threats and vulnerabilities. Adaptive security is aimed at preventing attacks in a timely manner, thereby minimizing the potential impact and extent of threats. This approach aligns with the overarching goal of ensuring that Information Technology systems remain operational and resilient even in the face of emerging security challenges. The conceptual framework is guided by the principles of comprehensiveness, adaptability, and risk management. It acknowledges that a one-size-fits-all approach is inadequate in the realm of cybersecurity. Instead, it promotes a systematic evaluation of security needs, the implementation of adaptive strategies, effective communication among stakeholders, and the continuous improvement of security measures.

3.1. Proposed Architecture

This research adopts a comprehensive adaptive access control system architecture proposed by [9]. A comprehensive design of an adaptive risk-based access control model for Internet of Things technology that takes into account real-time data information request for Internet of Things devices and

gives dynamic feedback. The proposed model uses Internet of Things environment features to estimate the security risk associated with each access request using user context, resource sensitivity, action severity and risk history as inputs for security risk estimation algorithm that is responsible for access decision. Then the proposed model uses smart contracts to provide adaptive features in which the user behaviour is monitored to detect any abnormal actions from authorized users. The following design is presented:

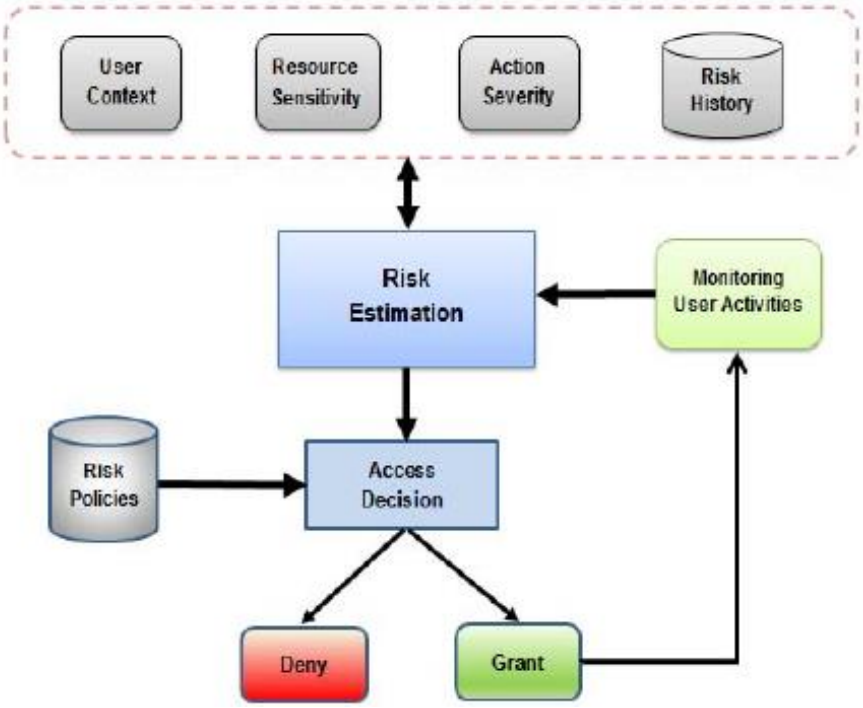

Figure 3. *The proposed Adaptive Risk-based Access Control Model [9].*

Dynamic access control methods utilize real-time environmental attributes to determine access decisions. Among these attributes, the security risk associated with access requests is a key factor, integrated into our proposed model for access decisions, illustrated in Figure 3. The model features four inputs: user/agent context, resource sensitivity, action severity, and risk history. These inputs, collectively referred to as risk factors, measures the security risk linked to each access request. The resultant risk value is then compared against risk policies to authorize or deny access. For adaptability, user behavior is continuously monitored to detect anomalous actions by authorized users. This model ensures a balanced security level while retaining scalability and adaptability for IoT systems.

User/agent context encompasses the environmental attributes tied to the user/agent during access requests, with location and time being common contexts.

Resource sensitivity measures data importance to the owner or service provider, assigning a sensitivity level based on potential damage from disclosure. Resource sensitivity is coupled with a risk metric proportional to data value.

Action severity measures the impact of actions on resources in terms of security requirements. Various operations carry different risks, such as 'view' versus 'delete'.

User risk history predicts risk by analyzing past behavioural patterns, identifying good and bad authorized users. The risk estimation module quantifies risk values based on input features, streamlining the risk estimation process.

Access decisions, granting or denying access, adhere to risk policies defined by resource owners. Risk policies guide the risk estimation module, created to identify access terms and conditions. The total risk value is contrasted with risk policies to finalize access decisions. The model advances flexibility by monitoring user behavior during access sessions. In traditional models, once access is granted, preventing abnormal data access becomes challenging. A monitoring module adapts risk values based on real-time user behavior. Implementing smart contracts introduces challenges, especially for the first-time application in this context. Smart contracts, running on blockchains, enforce functional demands and validate terms' fulfilment. Comparing monitored behavior with smart contracts prevents security breaches during access sessions. In conclusion, the proposed model leverages dynamic access control principles and incorporates security risk considerations to enhance access decisions. This approach ensures a comprehensive security strategy while accommodating Internet of Things system demands and user behaviours.

3.2. Process Flow of the Adaptive Risk-Based Access Control Model

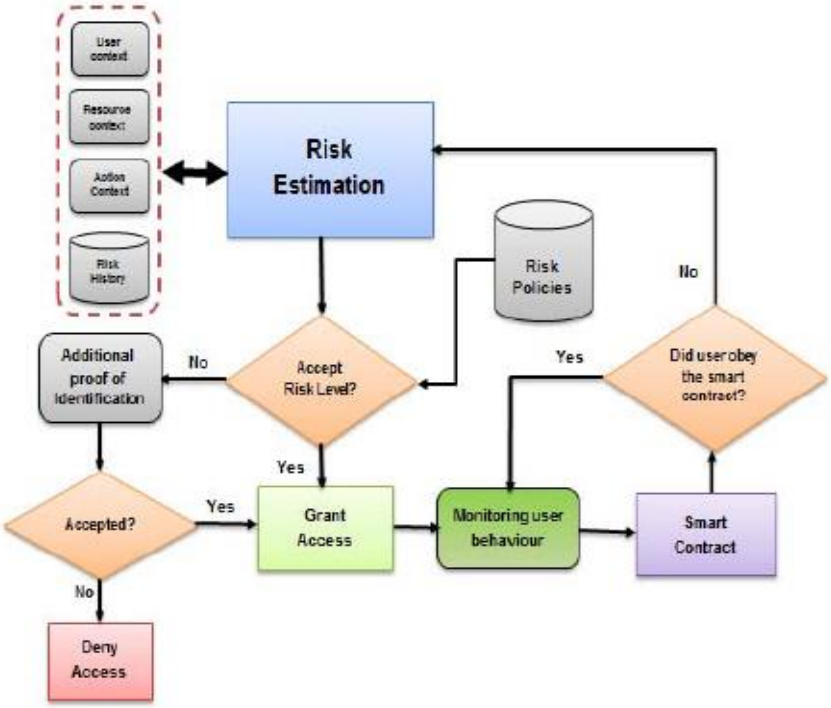

Figure 4. *The process flow of the Adaptive Risk-based Access Control Model [9].*

The adaptive risk-based access control model's process flow, depicted in Figure 4, outlines the sequence of actions. Initiated by the user's access request, the flow commences with the access control manager's reception of the request. Subsequently, the access control manager solicits system contexts encompassing the user/agent, resource, and action associated with the request. Additionally, the user's risk history is considered. Leveraging these contexts and the risk history, the risk estimation module computes an aggregate access risk value linked to the requesting user. This estimated risk value is then juxtaposed with predefined risk policies to ascertain the access decision. This juncture yields two potential outcomes:

Access Granted: In the event of access being granted, the monitoring module initiates user behavior tracking. The underlying smart contract utilizes this monitored data to gauge adherence to contract terms. If the user's behavior aligns with the contract, monitoring persists. However, any deviations prompt a return to the risk estimation module. This ensures proactive adjustments to user permissions or termination of the access session to thwart potential security breaches.

Access Denied: When access is denied, the system prompts the user for supplementary identification proof. This step prevents legitimate users from being blocked and curbs false positives. If the user supplies the requisite identification, access is sanctioned. Subsequently, the flow seamlessly resumes as in the case of the access-granted decision. If identification proof is not provided, the system maintains the access denial.

In summary, the process flow navigates through access request handling and risk assessment to determine access authorization or denial. This adaptive approach, grounded in the user's behavior and risk history, ensures robust security while accommodating authorized users and minimizing false positives.

4. Discussion of Findings

The landscape of information technology has transformed with the rise of cloud computing, enabling global access to computing resources. While cloud computing has offered significant advantages, the centralized nature of large-scale data centers has introduced latency and inefficiencies. This has led to the emergence of edge computing, which places computing resources closer to the sourcing devices, allowing real-time processing and reducing latency. The concept of edge computing has further been integrated with IoT, resulting in an interconnected network of devices generating and processing data. Edge computing, which involves processing data closer to the data source, has gained significance due to its ability to address the limitations of cloud computing. Interconnected devices, driven by the Internet of Things (IoT), generate vast amounts of data that need to be

processed in real-time. Edge computing allows for data processing at the network edge, resulting in reduced cloud connection times, instant data analysis, and more precise user responses. By improving network efficiency, scalability, and flexibility, edge computing contributes to enhancing performance and user experience. This paradigm shift has created the need for adaptive access control systems that can respond to the dynamic and heterogeneous nature of edge environments.

The reviewed literature reflects a growing awareness of the limitations of traditional access control mechanisms. Traditional access control methods have often been rigid and static, failing to adapt to dynamic and heterogeneous settings. The advent of edge computing, with its dynamic and real-time nature, demands an access control system that is responsive to changing contexts. As a response to these limitations, adaptive access control models have gained traction such risk-based access control models. Unlike traditional methods, risk-based models consider real-time risk factors associated with each access request, allowing for dynamic adjustments in access control. This research contributes to this evolving field by proposing an adaptive access control system that considers real-time data and information to respond to access requests dynamically. Such an approach aligns with the principles of edge computing, where responsiveness and real-time decision-making are crucial.

This research proposes an adaptive risk-based access control model for edge computing environments. The model integrates real-time environmental attributes such as user context, resource sensitivity, action severity, and risk history to estimate the security risk associated with each access request. By considering these risk factors, the model provides a balanced security level while ensuring adaptability for IoT systems. Access decisions are guided by risk policies defined by resource owners, allowing for dynamic adjustments based on real-time risk assessments. Furthermore, the incorporation of smart contracts and continuous monitoring enhances security measures. The discussion reveals that the Adaptive risk-based access control offers several advantages such as:

It improves security by dynamically adjusting access controls based on contextual factors and risk levels.

It enhances compliance with regulatory requirements by providing more granular control over access to sensitive resources.

Additionally, it enhances performance by reducing load on the internal network and ensuring faster access to resources.

The adaptive approach is scalable, making it suitable for managing access controls for a large number of users and resources.

Furthermore, adaptive risk-based access control contributes to adaptive security, where security measures can be adjusted in real-time based on risk levels.

In summary, the reviewed research works collectively contribute to the development of advanced access control strategies in the context of edge computing. These strategies consider real-time risk factors, improving security, compliance, performance, and scalability. Adaptive Risk-based access control models emerge as a solution to the limitations of traditional static approaches. These models align well with the dynamic nature of edge computing environments, ensuring that access decisions are responsive and contextually relevant. The concept of adaptive risk-based access control is poised to reshape the way access to resources is managed in edge environments.

5. Conclusions

In conclusion, the rapid evolution of cloud computing, edge computing, and IoT has highlighted the necessity for adaptive access control systems. Traditional access control mechanisms fall short in addressing the dynamic and heterogeneous nature of edge environments. This research advocates for the adoption of an adaptive risk-based access control system that utilizes real-time data and information to make dynamic access decisions. The proposed model integrates user context, resource sensitivity, action severity, and risk history to estimate security risk and make access decisions that align with the principles of edge computing.

Building on the research findings, it is recommended that organizations and researchers further explore and implement adaptive risk-based access control systems. This recommendation is grounded in the need for cybersecurity measures that align with the dynamic nature of edge computing and IoT environments. Organizations should consider the proposed model's benefits, including improved security and performance, and evaluate its applicability to their specific contexts. Furthermore, future research should focus on refining the implementation of smart contracts and continuous monitoring to ensure seamless and effective integration.

To conclude, the integration of adaptive access control systems into edge computing environments represents a significant advancement in ensuring data security and access management. By leveraging real-time data and contextual information, these systems offer a dynamic and responsive approach to access control, aligning with the principles of edge computing's agility and efficiency.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] I. Sitton-Candanedo and J. M. Corchado, "An Edge Computing Tutorial," *Oriental Journal of Computer Science and Technology*, vol. 12, no. 2, pp. 34-38, 2019.

[2] M. Satyanarayanan, "A Brief History of Cloud Offload: A Personal Journey from Odyssey Through Cyber Foraging to Cloudlets," *Mobile Computing and Commmunication*, vol. 18, no. 4, pp. 19-23, 2015.

[3] R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, pp. 1-31, 2016.

[4] S. Sengupta, J. Garcia and X. Masip-Bruin, "A Literature Survey on Ontology of Different Computing Platforms in Smart Environments," pp. 1-15, 2018.

[5] A. Hamm, A. Willner and I. Schieferdecker, "Edge Computing: A Comprehensive Survey of Current Initiatives and a Roadmap for a Sustainable Edge Computing Development," in *15th International Conference on Wirtschaftsinformatik*, Potsdam, Germany, 2020.

[6] B. N. Silva, M. Khan and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities.," *Sustain*, p. 697–713, 2018.

[7] K. Mannanuddin, M. R. Kumar, S. Aluvala, Y. Nagender and S. Vishali, "Fundamental Perception of EDGE Computing," in *ICRAEM 2020*, 2020.

[8] R. d. S. Daniel, M. Roberto, R. S. Gustavo, M. W. Carla and B. W. Carlos, "A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud," *Networks and Management Laboratory*, pp. 1-28, 2016.

[9] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills and J. Daniel, "Developing an adaptive Risk-based access control model for the Internet of Things," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017.

[10] O. M. Al-Mendah and S. M. Alzahrani, "Cloud and Edge Computing Security Challenges, Demands, Known Threats, and Vulnerabilities," *Academic Journal of Research and Scientific Publishing*, vol. 2, no. 21, pp. 156-175, 2021.

[11] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher and V. Young, "Mobile Edge Computing: A key technology towards 5G," 2015. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing

[12] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin and X. Yang, "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, p. 6900–6919, 2018.

[13] J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, p. 439–449, 2018.

[14] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider and M. Hamdi, "A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things," pp. 1-18, 2020.

[15] V. Suhendra, "A Survey on Access Control Deployment," in *In Communications in Computer and Information Science*, vol. 259, Berlin/Heidelberg, Springer, 2011, pp. 11-20.

[16] H. Atlam, M. Alassafi, A. Alenezi, R. Walters and G. Wills, "XACML for Building Access Control Policies in Internet of Things.," in *the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018),*, Madeira, Portugal, 2018.

[17] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Alshdadi and A. Alenezi, "Risk-Based Access Control Model: A Systematic Literature Review," *future internet*, pp. 1-23, 2020.

[18] N. Metoui, "Privacy-Aware Risk-Based Access Control Systems," *Ph.D. Thesis, University of Trento*, 2018.

[19] Q. Wang and H. Jin, "Quantified risk-adaptive access control for patient privacy protection in health information systems," in *the 6th ACM Symposium on Information, Computer and Communications Security—ASIACCS '11*, Hong Kong, China, 2011.

[20] T. Brooks, C. Caicedo and J. Park, "Security Vulnerability Analysis in Virtualized Computing Environments.," *International Journal of Intell.igent Computer Resources*, p. 263–277, 2012.

[21] X. Ding, X. Jiang, H. Bi and J. Fang, "On the Access Control Mechanism of Wireless Sensor Network," pp. 52-62, 2017.

[22] L. Qiu, X. Sun and J. Xu, "Categorical quantum cryptography for access control in cloud computing," *Soft Computing*, vol. 22, p. 6363–6370, 2018.

[23] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren and Y. Zhang, "A Feasible Fuzzy-Extended Attribute-Based Access Control Technique," *Security and Communication Networks*, pp. 1-12, 2018.

[24] D. Lang, H. Jiang, W. Ding and Y. Bai, "Research on Docker Role Access Control Mechanism Based on DRBAC," in *CISAT 2018*, 2019.

[25] R. Chang, Z. Lin, Y. Sun and J. Xu, "MD-UCON: A Multi-Domain Access Control Model for SDN Northbound Interfaces," in *ISPECE*, 2019.

[26] A. S. M. Kayes, R. Kalaria, I. H. Sarker, M. S. Islam, P. A. Watters, A. Ng, M. Hammoudeh, S. Badsha and I. Kumara, "A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues," *Sensors*, pp. 1-34, 2020.

[27] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi and A. S. A.-M. AL-Ghamdi, "Blockchain Platforms and Access Control Classification for IoT Systems," *Symmetry*, pp. 1-17, 2020.

[28] Y. Chen, L. Meng, H. Zhou and G. Xue, "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection," *Wireless Communications and Mobile Computing*, pp. 1-12, 2021.

[29] J. Ma, H. Xue, F. Wang, Y. An, D. Han, D. Wang, M. Zhao and S. Bi, "A Data Access Control Method Based on Blockchain," in *ISAIC 2020*, 2021.

[30] L. Liqing and L. Hai, "An access control model based on matrix domain security label," in *IOP Conference Series Materials Science and Engineering*, 2021.

[31] X. Lu, S. Fu, C. Jiang and P. Lio, "A Fine-Grained IoT Data Access Control Scheme Combining Attribute-Based Encryption and Blockchain.," *Security and Communication Networks*, vol. 2021, pp. 1-13, 2021.

[32] X. Liu, Y.-g. Zheng and X.-z. Li, "A revocable attribute-based access control system using blockchain," in *2021 3rd International Conference on Electronic Engineering and Informatics (EEI 2021)*, Dali, China, 2021.

[33] C. I. Cybersecurity, "Framework for improving critical infrastructure cybersecurity," 2018. [Online]. Available: https://www.baltimorecityschools.org/sites/default/files/inline-files/NIST.CSWP_.04162018.pdf

[34] M. Garsoux, "ISACA COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing: An overview," 2023. [Online]. Available: https://www.academia.edu/42165806/COBIT_5_ISACA_COBIT_5_ISACAs_new_framework_for_IT_Governance_Risk_Security_and_Auditing_An_overview_M_Garsoux_COBIT_5_Licensed_Training_Provider_COBIT_5_ISACA

[35] ANSI/ISA, "Security for industrial automation and control systems: System security requirements and security levels," 2013. [Online]. Available: https://securityboulevard.com/2020/09/everything-you-need-to-know-about-nist-cybersecurity-frameworks-informative-references/

[36] S. N. V. Schweizerische, "Information technology - security techniques - information security management systems - requirements," 2013. [Online]. Available: https://eldritchdata.neocities.org/PDF/CS/SecManagmentSystemsReq.pdf

[37] D. O. Alao, F. Y. Ayankoya, O. F. Ajayi and O. B. Ohwo, "The Need to Improve DNS Security Architecture: An Adaptive Security Approach," *Information Dynamics and Applications*, vol. 2, no. 1, pp. 19-30, 2023.