International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://www.theaspd.com/ijes.php

Access Management In Smart Ecosystems: Pathways To Achieving Environmental Sustainability And Green SDGS

Aman Kumar Routh[1], Prabhat Ranjan[2]
[1 2] Department of Computer Science, Central University of South Bihar, Gaya, India
amanrouthmail@gmail.com[1], prabhatranjan@cub.ac.in[2]

Abstract
Smart Connected Ecosystems (SCEs), fusing large-scale IoT implementations with cloud and edge centers, do offer a very large and moving attack surface and swiftly changing cross-domain access requests. Therefore, these real-time requirements, as well as the advancement of Green SDGs, are not satisfied by the conventional discretionary, mandatory, static role models. This article systematically benchmarks thirteen traditional and hybrid paradigms; DAC, MAC, RBAC, ABAC, RAdAC, RABAC, FBAC, TBAC, and task-centric schemesagainst a set of seven operational metrics: flexibility, scalability, administrative complexity, decision latency, reliability, dynamicity, and quality of service. The results found with composite frameworks-in which RBAC deterministic hierarchies are combined with ABAC contextual attributes and RAdAC continuous-risk scoring-offer the best balance in terms of security–sustainability trade-off by reducing unnecessary activations and overhead in the cloud, energy consumption, and e-waste. The study concludes that adaptive, sustainability-aware access control must underpin future SCEs; emerging risk- and fuzzy-logic models should be refined toward attribute minimisation and federated policy orchestration to secure low-carbon, resilient digital infrastructure.

Keywords: *Smart Connected Ecosystems; Access Control; IoT Security; Green Sustainable Development; Energy-Efficient Computing; SDGs.*

1. INTRODUCTION

In the context of a smart, connected ecosystem, which encompasses diverse infrastructures, applications, and technological systems, the integration of advanced technologies, such as the Internet of Things (IoT), cloud computing (CC), and wireless sensor networks (WSN), is essential. These technologies facilitate real-time data exchange and resource optimisation, which are crucial for addressing various challenges in urban environments and achieving the United Nations' Sustainable Development Goals (SDGs) [1][2][3]. Specifically, smart cities exemplify this ecosystem by utilizing IoT devices and cloud computing to enhance urban living and implement sustainable practices across social, economic, and environmental dimensions. For instance, smart cities deploy intelligent transportation systems that utilize real-time data analytics to optimise public transportation routes and schedules, thereby alleviating traffic congestion and reducing pollution [2][4]. Advanced information and communications technology (ICT) plays a crucial role in this integration, providing the necessary backbone for seamless communication and data processing among

interconnected devices [1][3]. Moreover, smart street lighting systems equipped with motion sensors exemplify resource optimization. These systems adjust illumination based on pedestrian traffic, leading to substantial energy savings [1][3]. Thus, smart cities emerge as a functional model of a smart connected ecosystem, where the synergy among IoT technologies, cloud

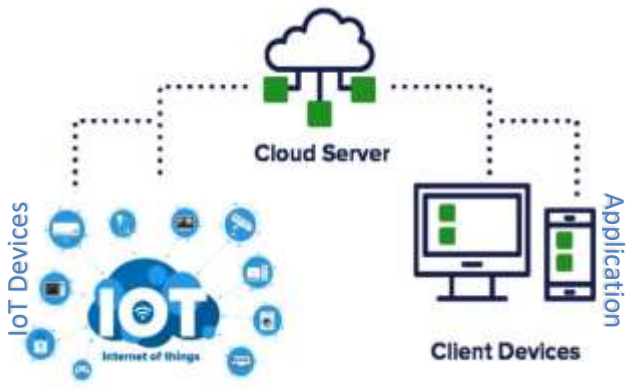
Figure 1 Typical Cloud-IoT enabled smart city

computing, and data analytics not only streamlines urban services but also sustainably manages resources to improve the quality of life [2][4]. The advancement of these interconnected infrastructures underscores their significance in achieving the SDGs and addressing the complexities of modern urban living.By embracing the concept of a smart connected ecosystem, a smart city aims to achieve SDGs such as sustainable urbanization (Goal 11), climate action (Goal 13), affordable and clean energy (Goal 7), and responsible consumption and production (Goal 12). The seamless integration of various smart systems allows the city to become more efficient, environmentally friendly, and responsive to the needs of its citizens, fostering a sustainable and connected community.

E-health, smart supply chain management, smart neighbourhood, etc., are just a few examples of the many types of smart infrastructures that can help build the linked communities necessary to reach the SDGs in the future. These dynamic alliances allow enterprises to make their data accessible across domains [5]. E.g. A patient's medical data may need to be shared between two or more hospitals, or an organization may need to share its financial data with Audit firms or analytics firms; in all these cases, one organization needs to access data from another organization. Smart-collaborative domains like IoT Cloud computing (CC) need extensive, fine-grained, and "active" security models to prohibit unauthorised access and operations and maintain the confidentiality, integrity, and availability of linked devices, applications, and systems. In order to permit or forbid operations, active security models factor in constraints based on context and the dynamic nature of the system. The security implications of these shifting relationships are not yet fully understood. Authentication and access control systems must be rethought with the least level of trust in order to accommodate users from different domains. Data from patients and businesses can be useful to medical experts and banks. Access control models are integral to smart connected ecosystems, providing comprehensive and fine-grained security measures. They safeguard critical infrastructure, protect sensitive data, and limit illegal access and operations, ensuring the confidentiality, integrity, and availability of linked devices, applications, and systems. By incorporating contextual limitations and adapting to changing dynamics, active security models contribute to achieving multiple sustainable development goals. They promote resilient infrastructure for industry and innovation (Goal 9), enhance privacy and trust in smart cities and communities (Goal 11), reduce environmental Impact through preventing malicious activities (Goal 13), foster strong institutions and stability (Goal 16), and facilitate secure collaborations and partnerships (Goal 17). Access control models are vital in creating safer, more efficient, and sustainable smart ecosystems[5] [6].

1.1. Understanding the Smart Connected Ecosystem: IoT and Cloud Synergy

The Smart Connected Ecosystem represents the convergence of two groundbreaking technologies: the Internet of Things (IoT) and Cloud Computing. The Smart Connected Ecosystem is vital in advancing



Sustainable Development Goals (SDGs) through converging IoT and Cloud Computing technologies. IoT devices act as data sources in this ecosystem, continuously generating vast information streams. These devices can range from simple sensors and wearables to complex industrial machinery and smart appliances. The data collected by these devices is then sent to the cloud, where it is processed, analyzed, and stored. Cloud services enable the efficient handling of massive data volumes and provide advanced analytics capabilities to extract valuable insights from the raw data. The concept of the Smart Connected Ecosystem, where IoT devices, cloud platforms, and data analytics converge to create intelligent and interconnected systems, is expanding. In contrast to conventional computing domains, innovative and collaborative computing systems (SCSs) enable intricate interactions among users, devices, and organizations. They aim to foster resource sharing and streamline activities involving participating entities, such as smart objects, users, clouds, or edge computers. Within these SCSs, multiple participants collaboratively create, share, manage, and safeguard digital content and

Figure 2 Typical Cloud-based IoT architecture

other resources[7]. Due to the intricacy of these interactions, a sophisticated access control system is essential to govern these complex activities effectively[8].

General Cloud-based IoT architecture The Internet of Things (IoT) encompasses various architectures with distinct layers. These architectures generally consist of three fundamental layers: The Devices, Cloud Server, and Application/Client layers [9], [10]. The Device layer and application layer are common across all reviewed papers. While there may be differences in their specific functionalities, they share general similarities. The Devices layer is responsible for the physical devices or "things" in the IoT system. These devices collect data from the environment or perform specific actions. The application layer, on the other hand, deals with the user interface and the utilization of the data collected by the object layer. It is where the data is processed, analyzed, and used to create value for users. However, the cloud server layer in IoT architectures exhibits variability across different proposals. These layers can be subdivided, and various technologies may be suggested for their implementation. The cloud service layer's role is to facilitate communication and data processing between the object and application layers. When considering the overall architecture of cloud-based IoT, these layers come into play within the context of cloud computing. Cloud-based IoT leverages the cloud infrastructure to store, process, and manage the vast data IoT devices generate. The cloud provides scalability, flexibility, and accessibility to IoT applications. In summary, cloud-based IoT architectures typically consist of a devices layer responsible for physical devices, one or more processing layers facilitating data communication and processing, and an application layer handling data analysis and user interfaces. Depending on specific proposals and requirements, each layer's functionalities and technologies can vary.

a) The Devices Layer:

In cloud-based IoT, the Device layer (also referred to as the object layer) plays a crucial role in the ecosystem. Its main task is to identify objects, such as sensors and actuators, and collect data from the physical environment, encompassing parameters like location, humidity, temperature, motion, and more. This layer utilizes a pervasive and heterogeneous set of devices, producing significant non-structured or semi-structured data. However, these devices typically have limited computational power and storage capacity. The collected data is securely transferred to a more capable layer in the Cloud Server Layer to overcome these constraints. Here, the data can be processed, analyzed, and managed efficiently to provide added functionality and value to IoT applications. One major challenge lies in seamlessly integrating a diverse array of devices with varying operating conditions, functionalities, and resolutions. This issue can hinder object interoperability and slow down the development of a unified reference model for the IoT. Nevertheless, addressing these challenges is crucial for unlocking the full potential of cloud-based IoT and enabling a more connected and intelligent world [11] [12] [13].

b) The Cloud Service Layer:

The Iot cloud service layer acts as a central hub, providing essential functions for the system. With smart objects expected to reach 80 billion by 2023, managing data influx is critical. It handles data access, storage, and processing, ensuring smooth operation. This layer employs sophisticated mechanisms for

storing and processing large data, which is used for smart monitoring, actuation, and visualization, offering meaningful insights. Policymakers and admins use this visualized data to make informed decisions, enabling policy updates stored in the cloud [9]. The cloud services layer helps IoT devices handle resource limits for intensive tasks by offloading computations, boosting system efficiency and enabling complex analyses. It manages data exchange between applications and IoT objects, ensuring smooth interactions and better access. Clouds can connect and collaborate across local and federated systems, allowing IoT devices to share information and collaborate to achieve shared goals [14]. In summary, the cloud service layer in IoT is a sophisticated and crucial component that efficiently manages data, enables advanced computations, and fosters seamless communication among various IoT entities, fostering a robust and interconnected IoT ecosystem.

c) The Application Layer:

In cloud-based IoT, the Application layer is the interface that provides services and functionalities to users. It presents information in a user-friendly way by analyzing data from the Cloud service layer, enabling remote communication with IoT devices and access to relevant data. It creates models, graphs, and flowcharts for insights and decision-making.

This layer uses various technologies to build responsive applications with real-time data access. It integrates visualization, analytics, and interfaces for an intuitive experience. Cloud resources support storage, processing, scalability, and security through authentication and encryption. As Iot complexity grows, the Application layer evolves to meet new needs, serving as a bridge between the cloud infrastructure and end-users for better decision-making, automation, and user experience experiences.

2. Challenges and Vulnerabilities in Smart Connected Ecosystems

In smart, connected ecosystems aligned with SDGs, addressing IoT-cloud security is vital for secure, sustainable growth. Access control mechanisms manage diverse IoT devices by establishing standardized protocols for authentication and authorization. Enforcing precise access policies reduces risks like unauthorized access, data breaches, and resource exhaustion attacks, ensuring fair resource allocation and ecosystem stability [15]. The resource-constrained nature of many IoT devices poses another vulnerability. Access control can be pivotal in managing resource allocation within the cloud environment, optimizing access permissions, and imposing usage limits on devices with limited resources. This prevents resource exhaustion attacks and guarantees fair resource distribution among legitimate devices, thereby enhancing the overall security and stability of the IoT Cloud ecosystem [16]. Privacy and security are crucial in the IoT Cloud due to constant data exchange. Blockchain can record decentralised security but isn't suitable for IoT, as it needs high energy and computing power, which IoT devices lack. Access control enforces encryption, protecting data during transmission and storage, and limits access to authorized users, reducing leaks [9]. The increasing number of communication interfaces in IoT devices introduces potential attack surfaces. Access control can manage and secure these interfaces by employing firewall rules, network segmentation, and access policies tailored to each device's communication needs. This proactive approach reduces the exposure of IoT devices to potential cyber threats, minimizing the chance of unauthorized network access and malicious attacks [16]. Ensuring timely security updates is vital for IoT Cloud security. Access control enables centralized update management, allowing quick, secure distribution of patches to IoT devices. It maintains ecosystem integrity by controlling software updates, preventing vulnerabilities. Overall, access control addresses IoT security challenges by managing device access, resource use, data privacy, network communication, and updates, strengthening security and fostering trust in IoT integration domains.

The researchers approached cloud computing security innovatively. As the environment constantly evolves, quick identification and resolution of security issues are crucial. Many studies have classified these concerns, focusing on architecture, people, processes, and technology. Some emphasise data security and privacy, while others consider broader security issues. There's an urgent need to address new security threats in cloud computing. Table 1 summarises relevant surveys and papers on cloud security computing.

Table 1. Summary of related work.

Year	Authors	Focus	Key Features & Limitations

2018	Basu et al.[17]	Cloud models Security	• Explored diverse cloud characteristics and frameworks, with a particular focus on security aspects. • Presented an innovative approach to counter cloud security issues and meet specific requirements. • Lacks emphasis on forthcoming research directions concerning the cloud in the context of IoT, leaving a potential research gap in this domain.
2018	Witti et al.[18]	Security and privacy in IoT, Edge, cloud and fog	• Evaluated privacy and security management in diverse IoT contexts, including IoT edge, IoT cloud, and fog environment. • Conducted a systematic mapping study to examine data securitization approaches and privacy-preserving methods in IoT research. • Does not encompass all emerging developments and scenarios in the rapidly evolving IoT landscape. • Findings were influenced by the selection of research studies.
2019	Akshaya et al.[19]	Cloud security, attacks and risks	• Examined eight common consequences of attacks on cloud services, impacting confidentiality, availability, and integrity of services. • Provided a taxonomy of attacks based on network categories, attack categories, attack techniques, and protection technologies. • Lacks a general or universal taxonomy for classifying cloud security threats, potentially leaving room for further research and standardization.
2019	Neshenko et al.[20]	IoT Vulnerabilities and mitigations	• Conducted exploratory studies on the time from IoT vulnerability discovery to patch deployment to improve risk management in critical CPS environments. Investigated links between weak programming practices and vendors, platforms, device types, and deployment environments to choose reliable vendors and promote secure coding. • Implemented stringent IoT programming standards and developed automated code tools to remediate IoT software vulnerabilities, bolstering IoT security and resiliency.
2020	Yang et al.[21]	Data Security and privacy issues in cloud storage	• Provided a survey on data security and privacy in cloud storage, covering encryption technologies and countermeasures. Analyzed eight key elements, including confidentiality,

			integrity, availability, access control, and privacy protectionn. • The paper does not address potential trade-offs between data security measures and performance, which could be crucial in real-world cloud storage implementations.
2020	Fernandez et al.[22]	Access control for Cloud-IoT architectures	• Addressed privacy threats from web services and IoT apps due to extensive data collection. Explored privacy-preserving architectures for cloud-IoT using "privacy-by-design." Proposed an integrated data collection and access control model for hybrid architectures like DataBank. • The proposed architectures may face scalability challenges when dealing with large volumes of data and numerous users.
2020	H. Alnajrani et al.[23]	Privacy and data protection in mobile cloud computing	• Demonstrated data privacy threats, attacks, and solutions, along with the metrics and measures used to assess privacy solutions in MCC. • Identified research types and contribution types used in MCC and emphasizes the ongoing research issues in encryption, authentication, security, trust, privacy, architectures, attacks, energy consumption, and testing. • The filtering process for selecting primary studies might introduce biases in the selection of relevant research.
2020	Hao Chen et al.[24]	Access control based on blockchain for IoT	• Proposed a Task-Attribute-Based Access Control scheme for the IoT via blockchain, combining the advantages of task-based and attribute-based access controls. • Utilized blockchain technology to ensure data authenticity, integrity, and decentralization, addressing the single point of failure problem, dynamically assigning user privileges and enabling real-time access requests. • The security analysis might not cover all potential threats and vulnerabilities, requiring continuous evaluation with evolving security measures. • The performance analysis demonstrated the model's acceptability, but its efficiency and resource usage in various IoT scenarios need to be explored further.

2021	J.park et al.[7]	Activity centric access control for SCSs	• Presented the Activity Control (ACON) concept for complex access needs in Smart and Collaborative Computing Systems (SCSs). Proposed an extended ACON framework to handle dynamic SCSs with multiple authorities. Laid the groundwork for secure SCS design, including security models, architectures, and prototypes. • The applicability and effectiveness of the proposed ACON framework in diverse smart and collaborative computing systems need evaluation. The paper focuses on activity control within SCSs, and further research may be needed to explore its integration with other access control mechanisms.
2021	A.Tahirkheli et al.[25]	Challenges of Cloud Computing over Smart City Networks	• Explored security and privacy issues in cloud computing, focusing on smart city tech, IoT devices, and related platforms. Various models, approaches, and frameworks for safeguarding security and privacy have been examined. • The paper doesn't cover all security aspects of CC-enabled IoT and edge computing, needing further research for a comprehensive analysis. The survey may miss recent advancements if the literature search is time-restricted framee.
2021	Alwakeel et al.[11]	Security and privacy issues threaten cloud and edge computing	• Reviewed the security and privacy features of fog and edge computing. Demonstrated common and environment-specific attacks. Presented strategies to reduce impact assaults. • The paper states that fog and edge computing security is inadequate and needs improvement. While some pattern suggestions exist for fog computing, a comprehensive security reference architecture is missing, which could bolster security computing.
2021	W.Ahmad et al.[10]	Cyber-security in IoT-Based Cloud	• The cloud security concerns in IoT were categorised into four major categories: data, network and service, applications, and people-related security issues. • Analysed recent cloud-based IoT attack advancements and discussed major security issues and limitations in AI and deep learning perspectives.
2022	D.Saini et al.[14]	Metric-based security for cloud	• Defined cloud computing as a model offering on-demand network access to configurable resources, highlighting its benefits

			and data security concerns. The authors propose a security evaluation methodology for cloud services to assist data migration decisions metrics. • The proposed security assessment model may have limitations in accurately predicting future attacks or addressing all aspects of cloud security comprehensively.
2022	M.Khalid et al.[6]	blockchain-based trust management approaches for cloud-based	• Conducted a review of blockchain-based trust management approaches for cloud systems, comparing them on established parameters. Identifies cloud computing challenges like centralization, overhead, trust, adaptiveness, and accuracy, and proposes blockchain solutions for decentralization and security. The research may not cover scalability and performance issues when integrating blockchain into large-scale IoMT applicationss.
2022	J. Zou et al.[27]	blockchain-based security services	• Investigated the integration of cloud computing and blockchain, including possible architectures and roles of cloud computing in blockchain networks. • Classified and discussed the recent works on different blockchain-based security services in the cloud computing model. • The article mainly focuses on integrating blockchain and cloud computing from a security perspective, and other aspects may not be covered extensively.
2023	Y.Ding et al.[28]	Fine-grained access control based on blockchain	• Introduced BLOCCESS, a blockchain-based, fine-grained access control framework. Developed tamper-proof protocols for untrustworthy environments like Iot and extended them for hybrid blockchain structures. Conducted semi-formal analysis and security evaluation of Bloccess model. • The inherent limitations of blockchain still restrict Bloccess. The research may not address all scenarios and challenges of implementing fine-grained access control in distributed systems contextss.
2023	J. Zhang et al.[29]	Trust-based framework for multi-cloud	• Proposed a trust-based secure multi-cloud collaboration framework for Cloud-Fog-Assisted IoT systems. • Developed of a role-based trust evaluation method to enhance the trustworthiness of Multi-Cloud Service Composition (MCSC).

The primary responsibility for ensuring security in the cloud lies with the cloud providers. Many enterprises have been migrating their operational procedures, data storage, and software applications to the cloud computing paradigm [30]. Recent developments show malicious entities targeting cloud services, viewing them as attractive targets. This visual aid assists in analysing weaknesses within the cloud ecosystem. Concerns about data loss and theft arise because user data is secretly sent to third-party providers. Information regarding weak authentication, stolen passwords, account hacks, data breaches, and other related issues is constantly thrown at the public. The IoT makes use of cloud computing's features to make data storage and sharing more convenient [31]. The cloud, in its essence, functions as a centralised server that provides unfettered access to computer resources in a perpetually available manner. Cloud computing offers a highly convenient and efficient approach for transmitting voluminous data packages generated by the internet of things (IoT). In contrast to conventional internet connections that rely on physical links connecting web pages, the Internet of Things (IoT) paradigm necessitates data integration for situation detection. The traits of IoT-based cloud attacks are outlined in Table 2.

Table 2 : IoT-based Cloud attacks metrics Affecting Environmental Sustainability [18][21][32][33]

Metrics	Description
Cybersecurity Incidents	Deliberate attacks on cloud systems that disrupt IoT environmental monitoring and control services, impairing sustainability efforts.
Data Compromises	Unauthorized access to sensitive environmental data in the cloud, leading to breaches that can misguide sustainability actions.
Data Leakage	Unintentional or deliberate exposure of critical environmental or sustainability-related information, damaging trust and operations.
Account Compromise	Unauthorized control of cloud services for IoT devices managing environmental resources, risking system misuse or sabotage.
Software and Interface Exploitation	Exploitation of vulnerabilities resulting in tampering with environmental monitoring or response systems.
Insider Threat	Employees or individuals with privileged access to cloud resources who misuse their access for malicious purposes.
Misuse of Cloud Services	Abuse of cloud resources for unauthorized activities that disrupt or degrade sustainable operations and management.
Disruption of Smart Grid Operations	Targeted attacks on cloud-managed smart grids or renewables, causing energy instability and greater environmental footprint.

The access control models play a pivotal role as the first line of defense in securing a smart connected ecosystem against a wide range of attack metrics. By efficiently managing cybersecurity incidents, data compromises, account compromises, and other threats, these models ensure the confidentiality, integrity, and availability of linked devices, applications, and systems. As a result, access control models contribute significantly to achieving Sustainable Development Goals (SDGs) by strengthening industry innovation, protecting sensitive data in sustainable cities and communities, mitigating the Impact of climate-related attacks, fostering solid institutions, and promoting secure partnerships. Their implementation is vital for creating a safe, resilient, and sustainable smart ecosystem that can effectively address emerging challenges and achieve sustainable development objectives[25] [34].

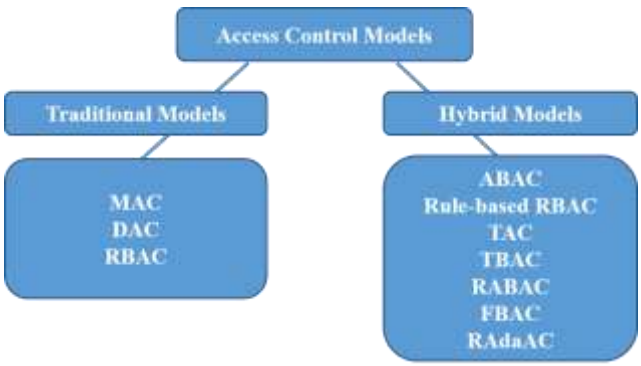
3. Access Control Models Fundamental Requirements for The Smart Connected Ecosystem

In the context of achieving Sustainable Development Goals (SDGs) through the smart connected ecosystem, fundamental requirements play a crucial role in designing access control models and enforcement architectures. These requirements ensure the ecosystem's seamless and secure functioning while contributing to SDG-related objectives [7]. These requirements are essential to ensure smart connected ecosystems' seamless and secure functioning.

Reliability: The smart connected ecosystem's reliability is critical to achieving SDGs. Consistent and dependable performance of IoT devices and cloud infrastructure instills confidence in users and applications, minimizing the risk of errors or failures that could hinder progress towards SDG targets.
Real-Time Response: Real-time response is essential in the smart connected ecosystem to support timely decision-making and actions related to SDGs. Rapid processing and analysis of vast data generated by IoT devices enable quick access to critical information, facilitating the implementation of real-time applications and services for sustainable development initiatives.
Dynamicity- Modern cyber-physical systems, including IoT and cloud technologies, must be dynamic and adaptive. As conditions change and new situations arise, these systems should be able to adjust their workflows and processes accordingly. The ability to dynamically adapt to varying variables ensures optimal performance and flexibility in the face of changing requirements [9].
Scalability- Adaptability to impromptu adjustments and shifting behaviours is a must for access control systems. New users, devices, and granular or complicated security policies require an access control mechanism that can grow with the system. In addition, these systems must understand which devices are networked together and which assets are at their disposal.
Flexible Administration- When the resource owner has agency over which attributes or other authorization parameters activities, relationships, etc.define resource access, it builds confidence between the resource owner and other entities in the connected systems [4].
Quality of Service- For a real-time linked network of devices, the Quality of Service must be high enough that access choices may be made with minimal latency. It's uncommon to come across a system that can immediately transition to a decentralized design. Local or edge-based access control mechanisms and parallel architectures can be used to expedite the process of acquiring secure access to the resources of the interconnected ecosystem [4].
By addressing these fundamental requirements, designers and stakeholders can ensure a robust and efficient smart connected ecosystem that optimizes the potential of IoT and cloud synergy.

3.1. Access Control Models for Smart Connected Ecosystems

Access Control Models for smart, connected ecosystems play a vital role in achieving the relevant Sustainable Development Goals (SDGs) by ensuring the security, efficiency, and sustainability of these interconnected systems. Access control models are the first line of defense in smart ecosystems, regulating user, application, and device rights to prevent unauthorized access and data breaches. This safeguards infrastructure and sensitive information, supporting Goal 9 and Goal 11 by ensuring ecosystem resilience and trust [13]. Access Control Models prevent cyberattacks, data breaches, and unauthorized resource manipulation in smart ecosystems. They regulate access decisions, ensuring security and integrity of interconnected components. Security administrators implement these models, defining requirements, features, workflow, users, and resources [35]. Secondly, access control models facilitate efficient resource allocation and usage within the ecosystem. By optimizing access permissions and imposing usage limits on resource-constrained devices, they prevent resource exhaustion attacks and ensure fair distribution of resources. This efficient resource management supports Goal 7 (Affordable and Clean Energy) and Goal 13 (Climate Action) by promoting energy efficiency and reducing the environmental Impact of



interconnected devices and cloud infrastructure. Access control models are crucial in safeguarding data privacy and integrity in smart ecosystems. By enforcing encryption and limiting access, they support Goal 16 by building trust. Unauthorized access can cause disruptions, affecting Goal 1 and Goal

Figure 3 Access Control Models for Smart Connected Ecosystems

10. These models must be flexible to adapt to evolving devices and services, ensuring ongoing security. Effective access control promotes security, efficiency, and sustainability, aiding SDGs. Lack of such control hampers progress by increasing risks and privacy issues. Thus, robust access control measures are essential for successfully integrating smart connected ecosystems in achieving sustainable development objectives. Generally, these access controls are categorized in two categories[36], Traditional and Hybrid as shown in Figure 3 .

3.1.1. Traditional Models

Traditionally, there have been three major types of access control models: discretionary (DAC), mandatory (MAC), and role-based (RBAC). Although these techniques are distinct from one another, they are not incompatible and can be used in tandem inside a company [37].

Mandatory Access Control (MAC)

This model centralises authority, controlling access rights based on security classifications, with secure clearances checked against object class to verify privileges. Unlike DAC, MAC enforces uniform policies across users, preventing permission changes. However, it has downsides: a single entity controls access, risking a point of failure, delays, and reduced flexibility in policy implementation.

Discretionary Access Control (DAC)

DAC is an access control mechanism that allocates access privileges according to user-defined rules. The fundamental concept of DAC is that entities can decide who can access their resources. This model utilizes Access Control Lists (ACLs) and capability tables [39].

Access Control Lists: Each list aligns with a resource and denotes the group of entities assigned to it along with their access permissions. Access Control Capability Lists: Each list aligns with an entity and denotes the group of resources accessible to that entity along with their corresponding permissions.

Role-Based Access Control (RBAC)

The RBAC model assigns roles to users, linking them to specific permissions. This setup allows users to access resources based on their roles. A middle layer, the roles, sits between users and permissions, making access management more efficient by splitting it into user-to-role and role-to-permission mapping. It also supports role inheritance, simplifying management. In addition, RBAC's distinct architecture improves the safety of access control management [40]. However, the RBAC architecture is unfit for settings where dynamic and granular control over user-permission mapping is required. The dynamic nature of this setting necessitates constant reevaluation of the connections between users, roles, and permissions.

3.1.2. Hybrid Models

In this section, we explained various hybrid models that are extensions of traditional access control models

Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) offers fine-grained control, flexibility, and dynamism. It operates based on attributes assigned by authorities, using a Boolean formula to define access policies. This model negates the need for creating numerous roles or access control lists for each member in an organization. The attributes enable automatic decision-making for access control. However, ABAC comes with complexity issues that amplify with an increase in the number of attributes. Despite this, it provides a robust solution that addresses limitations found in Role-Based Access Control (RBAC). Decisions are made in real time based on the observed attribute values or user IDs. Ultimately, ABAC bases its functionality on device policy, documents, and procedural rules, allowing for a flexible system that doesn't necessitate creating additional roles with new members [41].

Rule-Based Access Control (Rule-based ABAC)

The rule-based RBAC model adapts the conventional RBAC, functioning similarly. Rules activate automatically to map users to roles, and permissions are assigned to roles as in traditional RBAC. Its

unique feature is dynamic user role assignment, verified by a process matching user and role attributes. When attributes match, assignment occurs; otherwise, it does not. This flexibility ensures only users with specific attributes receive roles and permissions [42].

Task-Based Access Control (TAC)

Task-Attribute-Based Access Control (TAC) grants permissions based on task attributes rather than roles, allowing finer, dynamic control. However, managing TAC is complex, as its granular assignments can cause gaps and require significant resources to define and maintain. The model's complexity can also heighten the risk of errors and security threats if improperly implemented [24].

Trust-Based Access Control (TBAC)

TBAC is an access control model that relies on trustworthiness, assigning trust levels to users or systems to determine resource access. It evaluates behavior to adjust trust levels but faces challenges. Trust is subjective and dynamic, making assessments difficult and potentially inaccurate. If a trusted user or system gets compromised, security risks increase. The model's complexity demands constant monitoring and adjustment, complicating its use [43].

Role-Based Access Control with Attributes (RABAC)

RABAC merges RBAC and ABAC principles, using user attributes for role assignments, combining ABAC's flexibility with RBAC's structure. This offers nuanced access control, where permissions are role-based and also depend on attributes. It handles complex requirements while remaining manageable, creating a versatile model. However, integrating attribute rules complicates the design and management system [9].

Feasible Fuzzy-Extended ABAC (FBAC)

Though progressive, ABAC often lacks adaptable validation and efficiency, especially in resource use and business response. FBAC, however, offers better efficiency and flexibility for critical authorization, improving resource use and business fit. It has also been tested for risk, usability, and effectiveness evaluations. Being an extended variant of ABAC, the model isn't perfect when it comes to offering the strictest security and the least privilege, despite its efficiency and adaptability [44].

Risk-Adaptive Access Control (RAdAC)

RAdAC is a hybrid access control model combining elements like RBAC and ABAC to create a dynamic, context-aware system. It uses risk scores to adjust access policies based on current risk levels. In high-risk situations, it tightens controls; in low-risk cases, it relaxes them, balancing security and usability. Its main drawback is complexity, as implementing and maintaining accurate risk scores can be challenging, risking inappropriate access if flawed decisions [45].

In smart connected ecosystems, strong security is essential as gadgets, apps, and systems work together. Access control models define who can access resources, protecting data and infrastructure while reducing cyber threats. Table 3 compares models to see how they meet security needs. Understanding each model's strengths and limitations helps create a secure, sustainable connected world. This integration enhances both security and development, supporting ecosystem success. Each access control model has advantages and disadvantages; the choice depends on organisational needs like security, scalability, and ease of use. Some organizations may use a combination of these models to provide a multi-layered security approach[46].

Table 3 - Comparison of Traditional & Hybrid Access Control Model on 7 essential Metrics

Models	Flexibility	Scalability	Complexity	Speed	Reliability	Dynamicity	QoS
MAC	**L-** access is based on system-wide policies	**M-** scalable but can be difficult to manage	**H-** policy management can be complex	**M-** depends on policy complexity	**H-** strict policy enforcement ensures reliability	**L-** does not adapt to changing contexts	**H-** Policies ensure quality.

DAC	**H**- owners have discretion over permissions	**H**- scales well with number of resources and users	**M**- Resources and users determine complexity.	**H**- Quick decisions based on owner's discretion	**M**- Owners decide reliability	**M**- can adapt to changes made by owners	**M**- Owners decide quality.
RBAC	**M**- roles and permissions are predefined	**H**- adding new roles or users is easy	**M**- managing many roles can be complex	**H**- decisions are made quickly based on roles	**H**- role-based decisions are reliable	**L**- does not adapt to changing contexts	**H**- Quality is assured by role adherence
Rule-Based RBAC	**M**- roles and permissions are predefined	**H**- adding new roles or users is easy	**H**- complex managing roles & rules	**M**- dependent on roles and rules	**H**- access is strictly controlled by rules	**L**- does not adapt to changing contexts	**H**- Strict rules ensure quality
RAdAC	***H**- adapts to changing risks*	***M**- dependent on risk assessment capacity*	***H**- risk assessments add complexity*	***L**- risk assessments may delay decisions*	***H**- risk-based decisions enhance reliability*	***H**- inherently dynamic due to risk adaptiveness*	***H**- Quality is assured by continuous risk assessments*
RABAC	**H**- attributes offer flexible control	**H**- attributes scale well with users and resources	**M**- depends on the number of attributes	**H**- decisions are made quickly based on attributes	**H**- attribute-based decisions are reliable	**H**- can adapt to changes in attributes	**H**- Quality is assured by attribute adherence
ABAC	**H**- attributes offer flexible control	**H**- attributes scale well with users and resources	**M**- depends on the number of attributes	**H**- decisions are made quickly based on attributes	**H**- attribute-based decisions are reliable	**M**- can adapt changes in attributes but less than RABAC	**H**- Quality is assured by attribute adherence
FBAC	**H**- fuzzy logic offers flexible control	**H**- fuzzy attributes scale well with users and resources	**M**- depends on the number of fuzzy attributes and rules	**H**- fuzzy logic decisions are made quickly	**H**- fuzzy attribute-based decisions are reliable	**H**- fuzzy logic adapts to many attributes	**H**- Quality is assured by fuzzy attribute adherence

TAC	**M**- access is based on specific tasks	**H**- adding new tasks or users is easy	**L**- task-specific rules simplify management	**H**- decisions are made quickly based on tasks	**H**- task-based decisions are reliable	**L**- does not adapt to changing contexts	**H**- Quality is assured by task adherence
TBAC	**L**- trust levels are typically predefined	**H**- scales well as trust can be easily computed for new users	**L**- management is straightforward with trust-based decisions	**H**- decisions are made quickly based on trust	**M**- reliability depends on accurate trust computation	**L**- does not adapt quickly to changing contexts	**M**- Quality depends on accurate trust computation
ABAC	**H**- attributes offer flexible control	**H**- attributes scale well with users and resources	**M**- depends on the number of attributes	**H**- decisions are made quickly based on attributes	**H**- attribute-based decisions are reliable	**M**- can adapt changes in attributes but less than RABAC	**H**- Quality is assured by attribute adherence
FBAC	**H**- fuzzy logic offers flexible control	**H**- fuzzy attributes scale well with users and resources	**M**- depends on the number of fuzzy attributes and rules	**H**- fuzzy logic decisions are made quickly	**H**- fuzzy attribute-based decisions are reliable	**H**- fuzzy logic adapts to many attributes	**H**- Quality is assured by fuzzy attribute adherence

- **H**- High **L**-Low **M**- Medium

4. Enhancing Sustainability and Environmental Stewardship in Smart Connected Ecosystems

4.1. Integrating Access Control for Environmental Sustainability

The potential of smart connected ecosystems (SCEs) extends far beyond digital efficiency and operational security; their thoughtful implementation can drive substantial progress toward sustainability and environmental responsibility. Access control mechanisms, traditionally established to protect data and authenticate users, now play a significant role in facilitating and monitoring sustainability outcomes within these digital frameworks.

4.2. Key Areas Where Access Control Boosts Sustainability

Resource Optimization:

Tailored access controls in IoT-enabled smart grids, energy management systems, and sensor networks ensure that only authorized users can interact with devices or adjust configurations. This prevents misuse, reduces unnecessary energy consumption, and supports automated processes that curtail waste.

Sustainable Data Sharing:

Data sharing frameworks, fortified through fine-grained access control (e.g., ABAC, RBAC), encourage collaboration among stakeholders cities, companies, innovators without exposing sensitive information. By managing permissions, these systems enable ecosystem partners to exchange environmental datasets efficiently, promoting collective progress on SDGs related to climate action, smart agriculture, pollution tracking, and biodiversity.

Enabling Green Innovations:
Blockchain-based and risk-adaptive access control models empower secure experimentation and scaling of green technologies in connected ecosystems. For instance, blockchain-secured access to distributed renewable energy resources increases grid reliability while reducing carbon footprints.
Real-Time Monitoring and Compliance:
Dynamic access control supports real-time surveillance of environmental parameters and infrastructure health. Authorized regulators and researchers gain timely access to sensor data for faster response to environmental risks. Rule-based and adaptive models also enable compliance with evolving sustainability standards.
Reducing Physical and Digital Waste:
Efficient, policy-driven access management reduces computational redundancies, limits unnecessary device activations, and streamlines cloud usage leading to reduced e-waste and energy expenditure across the ecosystem.
Access Control and the SDGs: The Path Forward
Aligning access control mechanisms with Sustainable Development Goals (SDGs) is paramount for future-ready smart connected ecosystems:

- SDG 7 (Affordable and Clean Energy): Securing access to distributed energy resources through role-based and attribute-based control ensures equitable, sustainable energy management.
- SDG 11 (Sustainable Cities and Communities): Access controls guard public safety infrastructures and facilitate smarter mobility systems with minimal environmental footprints.
- SDG 13 (Climate Action): Enabling the secure, selective sharing of climate and environmental data catalyzes innovation in climate mitigation and adaptation efforts.

As these examples show, access control is no longer just a technological safeguard it's a catalyst for sustainable transformation. Future research and system designs should increasingly focus on integrating adaptive, scalable, and environmentally aware access control frameworks to maximize their contributions to global sustainability initiatives.

5. CONCLUSION

The article provides a comprehensive examination of access control models as foundational enablers for secure, sustainable smart connected ecosystems, particularly in alignment with the Sustainable Development Goals (SDGs). It articulates how the integration of IoT and cloud computing forms a complex yet essential infrastructure requiring sophisticated access control mechanisms to safeguard data, manage resource allocation, and mitigate diverse cyber threats in real time. By analyzing various access control paradigms from traditional models like DAC and RBAC to advanced hybrid and adaptive schemes such as ABAC, RABAC, and fuzzy-based models the paper highlights their respective strengths and limitations across key dimensions including flexibility, scalability, reliability, and dynamic adaptability.
Crucially, the article underscores how effective access control extends beyond conventional security objectives to significantly contribute to environmental sustainability and the broader SDG agenda. Managed access to IoT-enabled smart grids, environmental sensor networks, and cloud platforms optimizes energy consumption, facilitates responsible data sharing, and ensures regulatory compliance for sustainable development initiatives. This strategic alignment fosters resilience, innovation, and trust within smart ecosystems, enabling secure collaboration among diverse stakeholders for smart cities, climate action, and sustainable infrastructure. Furthermore, the dynamic nature of smart connected ecosystems demands access control models that are capable of real-time response, contextual agility, and continuous evolution amidst growing device heterogeneity and environmental complexity. Emerging adaptive frameworks like risk-based and fuzzy logic access control demonstrate promising avenues for balancing stringent security with operational flexibility and environmental stewardship. In conclusion, the article positions access control as a pivotal enabler of not only secure but also sustainable smart connected ecosystems that can effectively address the intertwined challenges of cyber risk and

environmental impact. The evolution and refinement of access control mechanisms will be critical to unlocking the full potential of IoT-cloud synergies, safeguarding vital infrastructures, and accelerating progress toward global sustainable development goals. As technology advances and smart ecosystems proliferate, access control models must remain agile, context-aware, and aligned with sustainability imperatives to architect the secure, green, and inclusive connected communities of the future. Access control models will play a vital role in creating the future of secure and interconnected communities as technology improves and smart ecosystems expand, contributing to the broader aims of global sustainable development.

REFERENCES

[1] P. Masek *et al.*, "A Harmonized Perspective on Transportation Management in Smart Cities: The Novel IoT-Driven Environment for Road Traffic Modeling," *Sensors*, vol. 16, no. 11, Nov. 2016, doi: 10.3390/S16111872.

[2] E. Park, A. P. del Pobil, and S. J. Kwon, "The Role of Internet of Things (IoT) in Smart Cities: Technology Roadmap-oriented Approaches," *Sustainability*, vol. 10, no. 5, May 2018, doi: 10.3390/SU10051388.

[3] P. Lynggaard and K. E. Skouby, "Complex IoT Systems as Enablers for Smart Homes in a Smart City Vision," *Sensors*, vol. 16, no. 11, Nov. 2016, doi: 10.3390/S16111840.

[4] A. S. Ibrahim, K. Y. Youssef, H. Kamel, and M. Abouelatta, "Traffic modelling of smart city internet of things architecture," *IET Commun.*, vol. 14, no. 8, pp. 1275–1284, May 2020, doi: 10.1049/IET-COM.2019.1252.

[5] G. Ali, N. Ahmad, Y. Cao, Q. Ejaz, and F. Azim, "Journal of Network and Computer Applications BCON : Blockchain based access CONtrol across multiple conflict of interest domains," vol. 147, no. September, 2019.

[6] M. Khalid *et al.*, "Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review," vol. 2022, 2022.

[7] J. Park, R. Sandhu, M. Gupta, and S. Bhatt, "Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems," *IEEE Access*, vol. 9, pp. 151004–151022, 2021, doi: 10.1109/ACCESS.2021.3126201.

[8] M. Gupta and R. Sandhu, *Towards activity-centric access control for smart collaborative ecosystems*, vol. 1, no. 1. Association for Computing Machinery, 2021. doi: 10.1145/3450569.3463559.

[9] M. U. Aftab *et al.*, "Secure and Dynamic Access Control for the Internet of Things (IoT) Based Traffic System," *PeerJ Comput. Sci.*, vol. 7, pp. 1–26, 2021, doi: 10.7717/PEERJ-CS.471.

[10] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electron. 2022, Vol. 11, Page 16*, vol. 11, no. 1, p. 16, Dec. 2021, doi: 10.3390/ELECTRONICS11010016.

[11] A. M. Alwakeel, "An overview of fog computing and edge computing security and privacy issues," *Sensors*, vol. 21, no. 24, pp. 1–20, 2021, doi: 10.3390/s21248226.

[12] 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," *Proc. - 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, vol. 2018-January, pp. 655–661, Jan. 2018, doi: 10.1109/ITHINGS-GREENCOM-CPSCOM-SMARTDATA.2017.103.

[13] A. Alshehri and R. Sandhu, "Access control models for cloud-enabled internet of things: A proposed architecture and research Agenda," *Proc. - 2016 IEEE 2nd Int. Conf. Collab. Internet Comput. IEEE CIC 2016*, pp. 530–538, 2017, doi: 10.1109/CIC.2016.081.

[14] D. K. Saini, K. Kumar, and P. Gupta, "Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions," *Secur. Commun. Networks*, vol. 2022, no. iv, 2022, doi: 10.1155/2022/4943225.

[15] A. F. Alotaibi, M. A. Alzain, M. Masud, and N. Z. Jhanjhi, "A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 9, pp. 1978–1990, Apr. 2021, doi: 10.17762/TURCOMAT.V12I9.3662.

[16] S. Namane and I. Ben Dhaou, "Blockchain-Based Access Control Techniques for IoT Applications," pp. 1–29, 2022.

[17] S. Basu *et al.*, "Cloud computing security challenges & solutions-A survey," *2018 IEEE 8th Annu. Comput. Commun. Work. Conf. CCWC 2018*, vol. 2018-January, pp. 347–356, Feb. 2018, doi: 10.1109/CCWC.2018.8301700.

[18] M. WITTI and D. KONSTANTAS, "IOT and Security-Privacy Concerns: A Systematic Mapping Study," *Int. J. Netw. Secur. Its Appl.*, vol. 10, no. 6, pp. 25–33, 2018, doi: 10.5121/ijnsa.2018.10603.

[19] M. Swathy Akshaya and G. Padmavathi, *Taxonomy of Security Attacks and Risk Assessment of Cloud Computing*, vol. 750. Springer Singapore, 2019. doi: 10.1007/978-981-13-1882-5_4.

[20] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.

[21] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

[22] M. Fernández, A. F. Tapia, J. Jaimunk, M. M. Chamorro, and B. Thuraisingham, "A data access model for privacy-

preserving cloud-iot architectures," *Proc. ACM Symp. Access Control Model. Technol. SACMAT*, pp. 191–202, 2020, doi: 10.1145/3381991.3395610.
[23] H. M. Alnajrani, A. A. Norman, and B. H. Ahmed, "Privacy and data protection in mobile cloud computing: A systematic mapping study," *PLoS One*, vol. 15, no. 6, pp. 1–28, 2020, doi: 10.1371/journal.pone.0234312.
[24] H. Chen, W. Wan, J. Xia, S. Zhang, and J. Zhang, "Task-Attribute-Based Access Control Scheme for IoT via Blockchain," vol. 65, no. 3, pp. 2441–2453, 2020, doi: 10.32604/cmc.2020.011824.
[25] A. I. Tahirkheli *et al.*, "A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures and challenges," *Electron.*, vol. 10, no. 15, 2021, doi: 10.3390/electronics10151811.
[26] Q. Luo, S. Hu, C. Li, G. Li, and W. Shi, "Resource Scheduling in Edge Computing: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 4, pp. 2131–2165, 2021, doi: 10.1109/COMST.2021.3106401.
[27] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, "Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges," *ACM Comput. Surv.*, vol. 54, no. 8, 2022, doi: 10.1145/3456628.
[28] Y. Ding and H. Sato, *Bloccess : Enabling Fine - Grained Access Control Based on Blockchain*, vol. 5. Springer US, 2023. doi: 10.1007/s10922-022-09700-5.
[29] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," *IEEE Trans. Cloud Comput.*, 2022, doi: 10.1109/TCC.2022.3147226.
[30] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4291–4300, 2021, doi: 10.1109/TITS.2020.3025875.
[31] W. Ahmed *et al.*, "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 115932–115950, 2021, doi: 10.1109/ACCESS.2021.3105450.
[32] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, "An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles," *IEEE Trans. Ind. Informatics*, vol. 17, no. 6, pp. 4288–4297, 2021, doi: 10.1109/TII.2020.3022759.
[33] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.
[34] T. Mawla, M. Gupta, and R. Sandhu, *BlueSky: Activity Control: A Vision for "active" Security Models for Smart Collaborative Systems*, vol. 1, no. 1. Association for Computing Machinery, 2022. doi: 10.1145/3532105.3535017.
[35] D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "IEEE Transactions on Cloud Computing Cloud-Trust -a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," vol. 5, no. 3, pp. 523–536, 1109, [Online]. Available: http://www.ieee.org/publications_standards/publications/rights/index.html
[36] A. K. Routh and P. Ranjan, "A Comprehensive Review on Granularity Perspective of the Access Control Models in Cloud Computing," *2024 IEEE Int. Conf. Interdiscip. Approaches Technol. Manag. Soc. Innov. IATMSI 2024*, vol. 2, pp. 1–6, 2024, doi: 10.1109/IATMSI60426.2024.10503154.
[37] J. Lopez and J. E. Rubio, "Access control for cyber-physical systems interconnected to the cloud," *Comput. Networks*, vol. 134, pp. 46–54, 2018, doi: 10.1016/j.comnet.2018.01.037.
[38] G. Karataş and A. Akbulut, "Survey on access control mechanisms in cloud computing," *J. Cyber Secur. Mobil.*, vol. 7, no. 3, pp. 1–36, 2018, doi: 10.13052/jcsm2245-1439.731.
[39] E. Ferrari, "Discretionary Access Control for Advanced Data Models," pp. 37–47, 2010, doi: 10.1007/978-3-031-01836-7_3.
[40] H. Qi, X. Di, and J. Li, "Formal definition and analysis of access control model based on role and attribute," *J. Inf. Secur. Appl.*, vol. 43, pp. 53–60, Dec. 2018, doi: 10.1016/J.JISA.2018.09.001.
[41] S. Bhatt, T. K. I. M. Pham, and M. Gupta, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," vol. 9, 2021.
[42] M. U. Aftab *et al.*, "Traditional and Hybrid Access Control Models: A Detailed Survey," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/1560885.
[43] V. Takalkar and P. N. Mahalle, "Trust-Based Access Control in Multi-role Environment of Online Social Networks," *Wirel. Pers. Commun.*, vol. 100, no. 2, pp. 391–399, May 2018, doi: 10.1007/S11277-017-5078-2.
[44] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "A Feasible Fuzzy-Extended Attribute-Based Access Control Technique," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/6476315.
[45] K. Ma, G. Yang, and Y. Xiang, "RCBAC: A risk-aware content-based access control model for large-scale text data," *J. Netw. Comput. Appl.*, vol. 167, p. 102733, Oct. 2020, doi: 10.1016/J.JNCA.2020.102733.
[46] M. Whaiduzzaman, M. N. Haque, M. Rejaul Karim Chowdhury, and A. Gani, "A study on strategic provisioning of cloud computing services," *Sci. World J.*, vol. 2014, 2014, doi: 10.1155/2014/894362.