Frontiers in Health Informatics
ISSN-Online: 2676-7104

www.healthinformaticsjournal.com

2024; Vol 13: Issue 3

Open Access

An in-depth evaluation of Hybrid Access Mechanisms for Real Time Big Data Environments from an empirical perspective

Mrs Sukeshini S Gawai,[1] Dr. L . K. Vishwamitra[2]
[1]Designation: Lecturer
Department : Computer Science & Engineering
colleges name : Oriental University, Indore
College address : Oriental University, Indore
Sanwer Road Jakhya Opposite Revati Range Gate No. 1, Jakhya Indore M.P.
:s.n.ingle@gmail.com
2Desi gnation: Professor
Department : Computer Science & Engineering
College name : Oriental University, Indore
College address : Oriental University, Indore
Sanwer Road, Jakhya Opposite Revti Range Gate No. 1 Jakhya Indore M. P.
lkvishwamitra@gmail.com

Cite this paper as: Sukeshini S Gawai, L . K. Vishwamitra (2024) An in-depth evaluation of Hybrid Access Mechanisms for Real Time Big Data Environments from an empirical perspective. *Frontiers in Health Informatics, 13* (3), 2645-2685

In the fast-paced digital world, real-time software environments such as cloud, fog deployments, and workstations are increasingly becoming vital for a multitude of applications. However, securing these environments is a significant challenge owing to the dynamic and complex nature of real-time data and processes. Existing models often fall short in addressing these challenges effectively, being limited by factors such as scalability, flexibility, and inability to adapt to ever-evolving cyber threats. In this paper, we present an in-depth evaluation of Hybrid Access Mechanisms (HAM) combined with Machine Learning (ML) based models for securing real-time software environments. Through a comprehensive review and empirical analysis, we investigate the effectiveness and performance of various models in securing these environments. Our analysis is conducted across a range of performance metrics including latency, throughput, accuracy, and resource utilization, thereby providing a holistic perspective on the optimal models suitable for real-time deployments. The proposed review brings forth the advantages of integrating HAM and ML models with big data, highlighting their capabilities in providing a robust and adaptive security framework that can effectively mitigate modern cyber threats while ensuring optimal performance. We demonstrate how these models can be fine-tuned to cater to the specific needs of real-time environments, thereby providing a tailored security solution that enhances the overall security use cases. The impacts of this work are manifold. By identifying the optimal models for securing real-time software environments, we provide valuable insights that can guide practitioners and researchers in the field of cybersecurity. Furthermore, our findings lay a solid foundation for future research, paving the way for the development of innovative security solutions that can effectively counteract the ever-evolving landscape of cyber threats. Ultimately, this research contributes significantly to *the body of knowledge in cybersecurity, providing a comprehensive and empirical-based evaluation that is crucial for safeguarding the digital world scenarios.*

Keywords: *Hybrid Access Mechanisms, Machine Learning, Big Data, Real-time Software Environments, Cybersecurity, Performance Metrics*

1. Introduction

In today's digital age, real-time software environments are pivotal for numerous applications spanning from cloud computing, fog deployments to workstations. The seamless operation and security of these environments are paramount, given the proliferation of cyber threats that continue to evolve in sophistication. However, the conventional security models are often inadequate in addressing the unique challenges posed by real-time data and processes. These limitations underscore the need for innovative approaches that can provide robust and adaptive security mechanisms.

Hybrid Access Mechanisms (HAM) in big data scenarios have emerged as a potential solution, leveraging a combination of traditional and modern security protocols to provide a comprehensive security framework. When augmented with Machine Learning (ML) based models, HAMs can evolve and adapt to ever-changing threat landscapes, ensuring the security measures are always one step ahead of potential attackers. The integration of HAM and ML has the potential to revolutionize the cybersecurity landscape, providing a tailored and flexible approach to securing real-time software environments.

Despite the promise shown by these integrated models, there is a significant lack of empirical-based evaluations that analyze their effectiveness and performance in real-world scenarios. In this paper, we aim to address this gap by conducting an in-depth evaluation of various HAM and ML-based models in securing real-time software environments. Through our comprehensive review and empirical analysis, we assess the performance of these models across key metrics such as latency, throughput, accuracy, and resource utilization. This holistic approach provides valuable insights into the optimal models suitable for real-time deployments, paving the way for more robust and adaptive cybersecurity solutions.

The implications of our study are significant, providing a much-needed empirical perspective on the efficacy of HAM and ML models in real-time software environments. By identifying the optimal models, we contribute to the body of knowledge in the field, guiding practitioners and researchers alike in their quest for more innovative and effective cybersecurity solutions. In doing so, our research lays the groundwork for future studies, ultimately fostering a safer and more secure digital world.

Motivation & Contributions

Motivation:

The digital landscape has witnessed a profound transformation with the advent of real-time software environments, encompassing cloud, fog deployments, and workstations. These environments are integral to a multitude of applications, driving innovations and advancements across various domains. However, the dynamic and complex nature of real-time data and processes pose significant security challenges, necessitating the need for advanced security mechanisms. Existing models often fail to adequately address these challenges, being hampered by issues such as scalability, flexibility, and a lack of adaptability to emerging cyber threats. This limitation highlights a crucial gap in the current state of cybersecurity, motivating our in-depth evaluation of Hybrid Access Mechanisms (HAM) combined with Machine Learning (ML) based models.

Contribution:

In this paper, we make several notable contributions to the field of cybersecurity. Firstly, we provide a comprehensive review and empirical analysis of various HAM and ML-based models, evaluating their effectiveness in securing real-time software environments. Through a meticulous examination across performance metrics such as latency, throughput, accuracy, and resource utilization, we offer a holistic perspective on the optimal models suitable for real-time deployments. Secondly, our study brings to light the advantages of integrating HAM with ML models, highlighting their potential in providing a robust and adaptive security framework capable of mitigating modern cyber threats while ensuring optimal performance. Additionally, we demonstrate how these models can be tailored to meet the specific needs of real-time environments, thereby offering a customized security solution that enhances the overall security posture.

Our research makes a significant impact on the field of cybersecurity by identifying the optimal models for securing real-time software environments, providing valuable insights for practitioners and researchers alike. Moreover, our findings lay a solid foundation for future research, paving the way for the development of innovative security solutions that can effectively counteract the ever-evolving landscape of cyber threats. Ultimately, our contributions are instrumental in safeguarding the digital world, offering a comprehensive and empirical-based evaluation that is crucial for the development of effective cybersecurity measures in the modern ages.

Access control is a fundamental aspect of cybersecurity, ensuring that only authorized individuals have access to specific resources or information. Existing techniques for access control operations can be broadly categorized into traditional and modern methods.

Traditional Methods:

- **Discretionary Access Control (DAC):** This method grants access rights based on the discretion of the owner or administrator. The owner decides who can access specific resources. However, it may lead to security lapses if the owner provides access to unauthorized users.

- **Mandatory Access Control (MAC):** Unlike DAC, MAC restricts access based on a fixed set of rules determined by the system administrator. It is more secure but can be inflexible and complex.

- **Role-Based Access Control (RBAC):** In RBAC, access permissions are assigned based on an individual’s role within the organization. It provides a balanced approach to security and usability but may be insufficient for complex environments.

Modern Methods:

Attribute-Based Access Control (ABAC): ABAC uses attributes (such as age, location, and job role) to determine access permissions. It is flexible and can adapt to complex environments but can be challenging to manage due to the large number of attributes.

Policy-Based Access Control (PBAC): PBAC uses predefined policies to grant access permissions. It is flexible and can be easily adapted to changing requirements, but policy management can be complex.

While these existing techniques have been widely used and have proven effective in various contexts, they are often limited by factors such as scalability, flexibility, and adaptability to new threats. As a result, there is a need for innovative access control mechanisms that can address these limitations and provide robust security in real-time software environments.

2. In-depth review of existing access control mechanisms

A wide variety of models are proposed for enhancing efficiency of access control mechanisms in cloud & big data systems. Firstly, the work discussed in [1] emphasizes the growing importance of data security and integrity due to the increasing volume of data generated and stored. It acknowledges that current big data security systems, often relying on third-party providers, are vulnerable to security risks. To tackle these issues, the paper introduces a novel approach that leverages blockchain technology and a highway protocol for real-time big data storage security. The highway protocol improves scalability, trustworthiness, data governance, and transparency, allowing for dynamic data manipulation and efficient data sharing. Comparative analysis demonstrates the superiority of this approach in terms of data processing period and energy consumption. In [2], the focus shifts to access control mechanisms in big data platforms. The paper presents SparkAC, a purpose-aware access control model for secure data sharing and analysis in Spark. It introduces the concept of purpose-aware access control and implements it in two modules, GuardSpark++ and GuardDAG, for structured and unstructured data, respectively. Experimental results show the effectiveness of SparkAC in providing access control functionalities with minimal performance overhead.

Moving to the Internet of Things (IoT) domain, [3] addresses the challenges of privacy and security in processing massive IoT-generated data. The proposed methodology incorporates federated learning, a hierarchical structure, and cryptographic mechanisms to enhance privacy and security. SEPP-IoT, a communication protocol, is introduced to facilitate secure interactions between IoT devices and a central server. Additional mechanisms like data compression, trust management, and fault tolerance further fortify the framework's security and integrity levels. In [4], the paper discusses the combination of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and blockchain for secure data storage and sharing. It specifically addresses issues related to high-dimensional attribute domains. The proposed scheme, including Fast High-dimensional Attribute Domain-based Message Encryption (HAD-FME) and Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM), is shown to offer improved data security, reduced computational cost, and efficient attribute revocation.

Work in [5] introduces an identity-based signcryption scheme with efficient revocation for secure big data communications. The scheme simultaneously ensures confidentiality, authenticity, non-repudiation, and integrity. It provides scalable revocation functionality while outsourcing unsigncryption tasks, making it suitable for large-scale systems. Security proofs and simulations validate the scheme's utility and effectiveness. Work in [6] focuses on healthcare big data management in IoT environments. It presents a scalable computing system that combines big data systems and blockchain architecture to ensure verifiable data access. The system uses a zero-knowledge protocol to enhance privacy and data integrity while minimizing data linkability. Results indicate the effectiveness of the method in solving privacy issues in healthcare big data analytics.

In [7], the paper explores the use of social network data to analyze human mobility patterns and activity behavior in urban areas. It introduces a scheme for urban mobility mining, demonstrating the regularity in human mobility patterns over several years. The study also establishes a connection between human mobility and the spread of COVID-19. The importance of efficient access control mechanisms in Big Data and Data Warehouses is highlighted in [8]. The paper proposes an aging-based Least Frequently Used (LFU) algorithm for cache management, aimed at reducing execution time and optimizing cache memory space. This approach significantly enhances performance and efficiency in accessing data from Data Warehouses.

Urban-rural area identification is the central theme in [9], where a data fusion approach using nighttime light data, point of interest data, and migration data is employed. Deep learning methods are utilized to improve the accuracy of urban and rural spatial identification, addressing issues caused by varying light brightness. Work in [10] delves into the optimization of logistics in the retail industry through intelligent logistics forecasting and management. The paper presents a deep learning-based model, RTS-GAT, for traffic flow prediction in retail road networks. The model effectively integrates temporal, spatial, and traffic flow features to achieve superior performance.

Intrusion detection systems are crucial for computer systems and networks, as discussed in [11]. The paper introduces a hierarchical intrusion detection model that combines multiple deep learning models with an attention mechanism. This model achieves high detection accuracy, optimized structure, and reduced false positives. Work in [12] introduces a new research direction in secure cloud storage, addressing the presence of malicious data publishers. The Sanitizable Access Control System (SACS) is proposed, based on $q$-Parallel Bilinear Diffie-Hellman Exponent Assumption, to resist unauthorized decryption of ciphertexts by malicious users, enhancing the adoption of secure cloud storage.

Finally, [13] presents a blockchain-based decentralized distributed storage and sharing scheme for IoT networks. The IoTChain model incorporates fine-grained access control and trust evaluation mechanisms, ensuring secure and efficient data access. Smart contracts and advanced encryption techniques are employed, making the approach practical and economical. In [14], the paper focuses on grid balancing and proposes a novel approach for selling surplus energy from renewable sources through cloud datacenters.

Method Name	**Findings**	**Advantages**	**Limitations**	**Applications**
[1]	- Blockchain technology	- Improved data security and integrity. - Scalability. -	- May require additional	- Safeguarding personal

	enhances big data storage security and scalability. - Proposed highway protocol improves consensus mechanism flexibility. - Better data processing period and energy consumption compared to baseline models.	Trustworthiness. - Data governance. - Transparency.	computational resources. - Specific to big data storage.	information. - Real-time big data storage. - Data sharing process control.
[2]	- Introduces SparkAC, a novel access control mechanism for secure data sharing in Spark. - Supports structured and unstructured data access control. - Small to medium performance overhead.	- Purpose-aware access control model. - Unified access control mechanism. - Effective access control functionalities.	- Limited granularity and expressiveness of existing mechanisms.	- Secure data sharing and analysis in Spark. - Data analytics applications.
[3]	- Federated learning enhances privacy and security of big data analytics in IoT. - SEPP-IoT communication protocol facilitates efficient, secure interactions. - Adaptive data compression reduces data transfer volume.	- Hierarchical structure. - Scalable learning rate. - Trust management.	- Complex implementation. - Potential scalability issues.	- Big data analytics in IoT. - Privacy preservation. - Secure data access.
[4]	- Proposed scheme addresses data	- Improved data security. - Lower computational	- Complex scheme with multiple	- Secure storage and sharing of data in

	protection issues in high-dimensional attribute domains. - HAD-FME improves data security and reduces computational cost. - SM-ARM offers efficient attribute revocation.	overhead. - Efficient attribute revocation.	components. - Smart contracts and blockchain integration.	high-dimensional attribute domains.
[5]	- ID-based signcryption scheme with efficient revocation. - Enables secure big data communications with outsourced unsigncryption. - Simultaneous achievement of confidentiality, authenticity, non-repudiation, and integrity.	- Efficient revocation functionality. - Scalable revocation based on the cardinality of users.	- Involvement of an untrusted cloud server in unsigncryption tasks.	- Secure big data communications. - Data collectors and data analytical systems.
[6]	- Proposed architecture combines big data systems and blockchain for healthcare data analytics. - Zero-knowledge protocol ensures privacy and data integrity. - Effective analysis and privacy solutions for	- Verifiable data access mechanism. - Data integrity. - Privacy preservation.	- Complex architecture with multiple sub-architectures. - Potential scalability challenges.	- Healthcare big data analytics. - Privacy protection. - Data integrity assurance.

	healthcare big data.			
[7]	- Social network data used as a proxy for human mobility analysis. - Identification of spatial and temporal regularity in human mobility patterns. - Association between human mobility and COVID-19 spread.	- Utilizes publicly accessible data. - Provides insights into human mobility patterns. - Can detect anomalies and changes in mobility behavior.	- Limited to urban areas. - Dependent on social network data.	- Understanding human mobility patterns. - Epidemic monitoring. - Urban planning.
[8]	- Cache-based mechanism for efficient data access from Data Warehouse (DW). - Aging-based LFU algorithm optimizes cache memory usage. - Efficiently fills cache memory with frequently used data.	- Reduced execution time. - Space-saving in cache memory. - Effective cache utilization.	- Limited to DW optimization. - Specific to query cache method.	- Fast data access from Data Warehouse. - DW optimization.
[9]	- Fusion of NTL data with POI and BM data for accurate urban-rural area identification. - Significant improvement in accuracy and kappa values with data fusion.	- Corrects differences caused by light brightness. - Provides accurate urban-rural area identification.	- Limited to urban-rural area identification. - Reliance on NTL data.	- Urban-rural area identification. - Regional urban-rural development.
[10]	- RTS-GAT model for analyzing	- Efficient representation of traffic flow features. - Better	- Specific to retail road network traffic	- Retail logistics optimization. -

	factors affecting retail road network traffic flow. - Unique deep learning-based representation and fusion method. - Improved performance on multiple datasets.	performance on retail road network data.	flow. - Complex model architecture.	Traffic flow analysis.
[11]	- Hierarchical intrusion detection model with multiple deep learning models and attention mechanism. - Improved detection accuracy and reduced false positives. - Combines spatial and temporal features for effective intrusion detection.	- Enhanced detection accuracy. - Reduced false positives. - Attention mechanism for feature weighting.	- Complex model architecture. - May require significant computational resources.	- Intrusion detection in computer systems and networks.
[12]	- NP-3C-FIP system for news personalization combining news content characterization and full-term interest portrayal. - Effective in improving news recommendation performance. - Incorporates latent Dirichlet allocation (LDA) and	- Captures user's mixed full-term interest. - Models sequential interest features. - Personalized attention mechanism for stable tastes.	- Complex model architecture. - Specific to news recommendation.	- News recommendation with enhanced personalization.

	personalized attention mechanism.			
[13]	- IoTChain model for blockchain-based decentralized distributed storage and sharing with end-to-end encryption. - Fine-grained access control and permissioned blockchain. - Proof-of-authority (PoA) consensus mechanism.	- End-to-end encryption. - Enhanced security and privacy. - Reduced transaction cost.	- Complex implementation. - Specific to IoT applications.	- Secure IoT data storage and sharing. - Decentralized data management.
[14]	- Cloud datacenters used to consume surplus energy from renewable sources through auction sales. - Integrated auctioning-scheduling mechanism for efficient energy consumption.	- Utilizes cloud datacenters for energy consumption. - Efficient consumption of surplus energy.	- Specific to surplus energy consumption. - May require cloud datacenter participation.	- Balancing surplus energy from renewable sources. - Energy-efficient cloud datacenter utilization.
[15]	- Sanitizable Access Control System (SACS) for secure cloud storage in the presence of malicious data publishers. - Resists unauthorized decryption by malicious users. -	- Provides security against malicious data publishers. - Secure cloud storage.	- Complex scheme with threat model and security model. - Specific to cloud storage with malicious data publishers.	- Secure cloud storage in the presence of malicious data publishers.

	Based on q-Parallel Bilinear Diffie-Hellman Exponent Assumption.			
[16]	- TABI mechanism for trust-based access control in Edge-IoT Networks using blockchain. - Mitigates impact of malicious IoT users and devices. - Utilizes edge computing for reduced overhead.	- End-to-end security. - Access control and trust evaluation. - Permissioned blockchain.	- Potential complexity in implementation. - Specific to Edge-IoT Networks.	- Secure access control in resource-constrained IoT networks. - Trust-based security in IoT.
[17]	- Proposed BPADAC scheme for secure UAV data sharing in cloud-based IoD. - Leverages blockchain and DHT for distributed and trustful data access. - Provides fine-grained access control and user traceability.	- Distributed and trustful UAV data access. - Fine-grained access control. - User traceability.	- Potential complexity in implementation. - Specific to UAV data sharing.	- Secure UAV data sharing in cloud-based IoD.
[18]	- Introduced D2-IAM for SSO access control in the cloud. - Uses smart contracts and blockchain for access control. - Minimizes communication overhead and	- Strong security measures. - Reduced communication overhead. - Fine-grained access control.	- Limited to cloud access control. - Specific to SSO.	- Access control for cloud resources.

	supports fine-grained access.			
[19]	- LBAC model integrated with blockchain-based smart contracts for e-health data access. - Provides multilevel access control security. - Preserves privacy, maintains transparency, and ensures data integrity.	- Multilevel access control. - Privacy preservation. - Transparency and data integrity.	- Complex framework. - Specific to e-health data access.	- Access control for e-health records.
[20]	- Proposed Hamming code-based encoder for STT-MRAM error correction. - Improved speed and performance of STT-MRAM devices. - Addresses process variations and thermal fluctuations.	- Enhanced error correction. - Improved device speed and performance.	- Specific to STT-MRAM technology. - Complex encoding process.	- Error correction in STT-MRAM devices.
[21]	- Introduced DABAC for access control in dynamic IoT environments. - Utilizes smart contracts and intelligent gateways. - Ensures physical location limitations and	- Physical location-based access control. - Dynamic device management. - Mitigates single points of failure.	- Complex IoT environment implementation. - Specific to IoT access control.	- Access control for IoT devices.

	security in untrusted IoT environments.			
[22]	- Proposed DPoS consensus mechanism for blockchain-based DSA. - Addresses spectrum violations and enables spectrum sensing. - Offers energy-efficient consensus for DSA.	- Energy-efficient consensus. - Spectrum violation detection. - Spectrum sensing.	- May require additional hardware. - Specific to DSA in IoT.	- Dynamic Spectrum Access (DSA) in IoT.
[23]	- Proposed ultraviolet random access collaborative networking protocol. - Utilizes dynamic timeslot allocation for higher throughput. - Demonstrated cooperative forwarding and random access capabilities.	- Improved throughput. - Cooperative networking. - Effective protocol design.	- Limited to ultraviolet networks. - Specific to collaborative networking.	- Ultraviolet network protocols.
[24]	- Introduced real-time motion control method for PON-based access edge. - Utilizes delay compensation for control performance improvement. -	- Real-time motion control. - Improved control performance. - Feasible for factory automation.	- Specific to PON-based access edge. - May require modifications to existing PON systems.	- Motion control in factory automation.

	Demonstrated feasibility for factory automation.			
[25]	- Proposed SmartAccess system for cross-organization medical records sharing. - Utilizes blockchain and smart contracts for access control. - Provides transparency, auditability, and privacy.	- Cross-organization data sharing. - Transparency and auditability. - Privacy preservation.	- Requires a decentralized system. - Overhead of blockchain adoption.	- Cross-organization medical records sharing.
[26]	- Investigated distributed sliding mode control for consensus in multi-agent systems. - Reduced chattering and tolerates communication delay. - Achieves quick consensus with optimal controller.	- Reduced chattering. - Consensus in multi-agent systems. - Tolerance to communication delay.	- Complex control method. - May require significant computational resources.	- Consensus in multi-agent systems.
[27]	- Proposed DRL-based scheme for intelligent user access control in O-RAN. - Optimizes user throughput and reduces frequent handovers. - Demonstrated	- Intelligent user access control. - Reduced frequent handovers. - High performance.	- Complex DRL implementation. - Specific to O-RAN deployment.	- User access control in O-RAN.

	outstanding performance.			
[28]	- Optimized GU access control using game theory in multiple UAV-BSs network. - Achieved Nash equilibrium in access control game. - Efficient deployment design for UAV-BSs.	- Game theory-based access control. - Efficient deployment design. - Achieved Nash equilibrium.	- Specific to UAV-BSs network. - Limited to GU access control.	- Access control in UAV-BSs network.
[29]	- Proposed LightMED for secure EMR sharing in cloud with IoT integration. - Utilizes fog computing, CP-ABE, and blockchain. - Provides efficient privacy-preserving access control.	- Secure EMR sharing. - Privacy preservation. - Lightweight policy update.	- May require integration with fog computing. - Specific to EMR sharing.	- Secure EMR sharing with IoT integration.
[30]	- Introduced smart contract-based access control framework for resource access control. - Provides reliability, auditability, and scalability. - Uses off-chain	- Reliable access control. - Auditability and scalability. - Off-chain attribute distribution.	- Requires blockchain adoption. - Overhead of smart contract deployment.	- Resource access control in a decentralized framework.

	signatures for attribute distribution.			
[31]	- Proposed a blockchain-based access control scheme for IoT and role-based access control. - Resolves conflicting roles and improves system security. - Provides better response times for concurrent user requests.	- Role management system. - Conflict resolution. - Improved system security.	- Requires blockchain adoption. - May have an overhead of system performance.	- Access control in IoT with conflict resolution.
[33]	Proposed an MEC-based access control strategy for green IoT systems using a CMDP and RCQN algorithm. Introduced an LSTM-based energy prediction module. Improved system utility.	Maximizes system utility, considers spectral efficiency and access ratio.	Unknown energy arrival process, dynamical changes in network state.	Green IoT systems.
[34]	Proposed an authorized keyword search scheme using Role-Based Encryption (RBE) in a cloud environment. Supported multi-organization cloud environments. Efficient decryption and revocation mechanisms.	Enables delegated keyword-based data search, supports multi-organization clouds, efficient decryption, and revocation.	None mentioned.	Cloud environments requiring keyword-based search.
[35]	Described Kubernetes RBAC authorization sub-system for securing access to resources in	Restricts system access to authorized users.	None mentioned.	Kubernetes clusters and resource access control.

	clusters.			
[36]	Presented an RBE scheme with efficient user revocation for multi-organization cloud storage. Introduced an outsourced decryption mechanism.	Suitable for multi-organization clouds, efficient user revocation, reduced overhead.	None mentioned.	Multi-organization cloud storage systems.
[37]	Introduced RBAC-based load balancing-assisted resource management framework (RBAC-LBRM) for IoT-edge-fog networks, which significantly improved performance metrics.	Achieved average improvements in CPU usage, memory usage, delay, and jitter metrics.	None mentioned.	IoT-edge-fog networks for load balancing and resource management.
[38]	Proposed DHACS, a Decentralized Hybrid Access Control for Smart Contracts, for Industrial Internet-of-Things (IIoT) applications. DHACS combines role-based, rule-based, and organization-based access controls.	Provides transparency, reliability, and robustness. Efficient for IIoT applications with low latency requirements.	None mentioned.	IIoT applications with blockchain integration.
[39]	Presented a trust-based secure multi-cloud collaboration framework for Cloud-Fog-Assisted IoT systems. Included role-based trust evaluation, user authentication, and access control mechanisms.	Enhances trustworthiness of MCSC, preserves security of services.	Vulnerable to malicious users.	Cloud-Fog-Assisted IoT systems requiring trust-based collaboration.
[40]	Proposed CryptCloud±,	Provides accountability	Inevitable security	Secure cloud storage

	a revocable CP-ABE-based cloud storage system with white-box traceability and auditing, addressing access credential misuse.	and revocation mechanisms. Mitigates access credential misuse.	breach with CP-ABE.	systems requiring fine-grained access control.
[41]	Introduced DSFlow, a secure and fine-grained flow control system for subscription-based data services in a cloud-edge computing architecture.	Resists malicious publishers, allows valid subscribers to decrypt sanitized ciphertexts.	Access control policies may not apply to subscriptions.	Subscription-based data services with secure flow control.
[42]	Developed two hybrid access control models (HyBAC RC and HyBAC AC) for smart home IoT, combining ABAC and RBAC.	Offers role-centric and attribute-centric approaches.	None mentioned.	Smart home IoT access control.
[43]	Proposed a revocable attribute-based data storage (RADS) scheme for cloud storage with fine-grained access control and efficient user revocation.	Achieves fine-grained access control, allows CSP to share computations, offloads revocation operations.	High computation overheads during user revocation.	Cloud storage with fine-grained access control.
[44]	Presented a server-aided revocable fine-grained access control mechanism with cloud assistance, achieving efficient access control with reduced user-side computations.	Efficient fine-grained access control, immediate and robust user revocation.	None mentioned.	Fine-grained access control in cloud services.
[45]	Proposed the ReFlat module for mitigating access frequency pattern leakage in encrypted cloud data, improving security	Addresses access frequency pattern leakage, achieves robustness.	Security risk of involving intermediate proxy.	Secure cloud data access under specific threat models.

	under specific threat models.			
[46]	Developed a method to assess cloud service trustworthiness based on D-S theory and Markov chain, considering the dynamic nature of cloud environments.	Objectively assesses cloud service trustworthiness state and changes.	None mentioned.	Assessing cloud service trustworthiness and managing trust.
[47]	Designed a separable self-attention mechanism for point clouds and a Separable Transformer architecture.	Captures both local and global contexts in point cloud analysis.	None mentioned.	Point cloud analysis with improved self-attention.
[48]	Proposed a biometric-based authentication protocol for secure access to a remote server. Utilized biometric data as secret credentials and derived a unique identity.	No need to store private keys, efficient session key generation.	None mentioned.	Secure access to remote servers using biometric data.
[49]	Proposed a healthcare IoT system using attribute-based encryption, cloud, and edge computing for fine-grained access control.	Offers efficient, flexible, and secure fine-grained access control with data verification.	None mentioned.	Healthcare IoT networks requiring fine-grained access control.
[50]	Addressed fine-grained access control in Healthcare IoT using attribute-based encryption and cloud-edge computing.	Achieved efficient, flexible, secure fine-grained access control.	None mentioned.	Healthcare IoT networks requiring fine-grained access control.

ble 1. Comparative Analysis of Models used

for Hybrid Access ControlBy incentivizing cloud workload migrations, the approach effectively consumes excess energy, providing cost savings and minimizing energy wastage. The paper in [15] addresses the challenge of secure data sharing in cloud storage systems. It introduces the concept of Sanitizable Access Control System (SACS), designed to cope with malicious data publishers, enhancing security in cloud storage environments.

Work in [16] explores the integration of blockchain technology and edge computing in IoT networks. The Trust-based Access Control Mechanism for Edge-IoT Networks using Blockchain (TABI) ensures end-to-end security, access control, and trust evaluation in resource-constrained IoT networks, highlighting its suitability for low-latency applications. In recent years, the convergence of Internet of Things (IoT) and aerospace technologies, supported by satellite and 6G communication techniques, has given rise to the Internet of Unmanned Aerial Vehicles (UAVs), known as the Internet of Drones (IoD) [17]. Cloud-based IoD has emerged as a practical choice for managing and sharing real-time UAV data, alleviating the computational burden on mobile UAVs. However, safeguarding sensitive UAV data in an open, distributed environment with resource-constrained UAVs presents a significant challenge. Previous work (PATLDAC) introduced a cloud-based UAV data access control scheme, but it suffered from inflexibility, centralized data storage, and untrustworthy metadata in an untrusted cloud environment [17]. To address these issues, a blockchain-based privacy-aware data access control (BPADAC) scheme is proposed, leveraging blockchain and Distributed Hash Table (DHT) for distributed, secure UAV data access and storage, with enhanced access control and user tracing mechanisms [17]. Traditional Single Sign-On (SSO) access control systems face limitations when adapting to the demands of multi-user, multi-application environments in cloud platforms [18]. In response to this, a blockchain-based identification and access management (IAM) scheme called D2-IAM is introduced, utilizing smart contracts and blockchain for core access control processes, thereby minimizing communication overhead and enabling fine-grained access control policies [18]. The proposed D2-IAM system demonstrates superior efficiency compared to existing SSO models [18].

In healthcare systems, access control to patient information is of paramount importance, necessitating comprehensive secure frameworks to manage data access according to confidentiality levels [19]. The integration of the Lattice-Based Access Control (LBAC) model and blockchain-based smart contract mechanisms provides multi-level security and compliance with data access restrictions, ensuring data integrity and privacy while outperforming existing models [19]. Spin-torque-transfer magnetic random access memory (STT-MRAM) is considered a promising technology for replacing DRAM but faces challenges due to process variations and thermal fluctuations, leading to errors [20]. An innovative algorithm based on Hamming code is proposed to address these challenges, improving STT-MRAM device performance by generating sparse codes with a minimum Hamming distance of three [20]. This approach is designed to enhance speed and reliability while overcoming complexity issues [20].

The dynamic nature of IoT devices in IoT ecosystems introduces new challenges for access control, particularly in physically constrained environments [21]. The Domain Attribute Based Access Control (DABAC) is introduced to incorporate domain elements and enable physical location-based access control [21]. Smart contracts are leveraged to deploy access control mechanisms in distributed IoT environments, enhancing security and mitigating threats [21]. The growth of IoT and next-generation wireless networks has led to the need for advanced and dynamic spectrum access mechanisms [22]. A novel energy-efficient consensus mechanism called "Distributed-Proof-of-Sense (DPoS)" is proposed to enable Dynamic Spectrum Access (DSA) and detect spectrum violations efficiently [22]. This mechanism motivates blockchain miners to perform spectrum sensing, improving spectrum management [22].

Ultraviolet networks offer high-security non-line-of-sight communication, but access control protocols are required to ensure their reliability and effectiveness [23]. An ultraviolet random access collaborative networking protocol based on time division multiple access is introduced, designed to achieve higher throughput with lower delays and packet loss rates, particularly in dynamic ultraviolet network scenarios [23]. Access control plays a crucial role in remote motion control of IoT devices, particularly in access edge scenarios [24]. A novel real-time and high-precision motion control method is proposed, which calculates and compensates for delay introduced by Dynamic Bandwidth Allocation (DBA) in Passive Optical Networks (PON) systems [24]. This method demonstrates improved control performance and bandwidth utilization efficiency [24].

Cross-organizational data sharing presents challenges in terms of trust and transparency [25]. The SmartAccess system is introduced, utilizing blockchain and smart contracts to define an Attribute-Based Access Control System for cross-organization medical records sharing [25]. This system offers transparency, regulation compliance, and auditability while maintaining data privacy and security [25]. The consensus of nonlinear discrete-time high-order multi-agent systems is addressed through an optimal sliding mode control approach [26]. A distributed discrete-time integral sliding mode control law is designed, combined with optimal controllers to reduce chattering and accommodate communication delays among agents [26]. Simulation results validate the effectiveness of this control method [26]. The Open RAN (O-RAN) paradigm introduces challenges in terms of load balancing and frequent handovers in massive base station deployments [27]. An intelligent user access control scheme with deep reinforcement learning (DRL) is proposed, optimizing throughput and minimizing handovers through a federated DRL-based approach [27]. Simulation results demonstrate superior performance compared to existing methods [27].

In a multiple UAV-BS assisted wireless network, optimization of ground user (GU) access control is addressed using game theory [28]. A game-theoretical approach is used to find the Nash equilibrium for GU access control, followed by optimization of UAV-BS deployment through convex optimization theory [28]. The proposed approach outperforms other baselines in simulations [28]. In the healthcare domain, secure sharing of encrypted Electronic Medical Records (EMRs) from IoT devices in a cloud-based environment is essential [29]. The LightMED access control scheme is introduced, providing secure EMR sharing through lightweight encryption, digital signing, and blockchain integration [29]. The scheme is shown to be efficient and practical, offering improved processing cost for end-users [29]. Conventional centralized access control models face challenges of single points of failure and lack of transparency [30]. A smart contract-based access control framework is proposed, allowing resource owners to manage access control policies in a reliable and auditable manner, leveraging blockchain technology for scalability and efficiency [30].

The integration of artificial intelligence and IoT in Industry 5.0 necessitates robust access control for resilience and error-free operations [31]. A Zero-Trust Network-based Access Control Scheme (ZTN-ACS) is introduced, extending support for managing devices and operation schedules using deep learning to enhance security and consistency [31]. In [32, 33], the authors focus on Multi-Access Edge Computing (MEC) in the context of IoT. They propose an access control strategy for green IoT systems, considering spectral efficiency and successful access ratio. This strategy is modeled as a Constrained Markov Decision Process (CMDP) and employs a novel centralized reward-based experience replay deep convolutional Q network algorithm (RCQN) for optimal access control. Additionally, they introduce a Long Short-Term Memory (LSTM) based energy prediction module to enhance access control. Simulation results highlight the effectiveness of this approach in improving system utility.

The second work [34] deals with keyword search over encrypted data in a cloud environment. The authors propose a Role-Based Encryption (RBE) technique for authorized keyword search, ensuring data security and efficient decryption. This approach supports multi-organization cloud environments, offers efficient decryption, and provides formal security analysis. In the third work [35], the paper discusses the Kubernetes RBAC authorization sub-system, explaining its role in securing access to resources within a cluster. It emphasizes the validation of set policies through impersonation to ensure proper access rights for users and service accounts.

Work [36] introduces Role-Based Encryption (RBE) in the context of multi-organization cloud storage systems. The authors present an RBE scheme with efficient user revocation and an outsourced decryption mechanism. They demonstrate its security against Chosen Plaintext Attacks and its practicality due to low computation overhead. In work [37], the authors address the challenges of load balancing and access control in IoT using edge and fog environments. They propose a role-based access control (RBAC)-based load balancing-assisted efficient resource management framework named RBAC-LBRM. It achieves significant improvements in CPU usage, memory usage, delay, and jitter metrics, enhancing IoT network performance.

The integration of blockchains, IoT, and smart contracts is explored in work [38], focusing on access control challenges. The authors propose DHACS, a Decentralized Hybrid Access Control for Smart Contract in IIoTs, which combines role-based, rule-based, and organization-based access controls. DHACS outperforms existing approaches, offering more efficient access control management. In work [39], a trust-based secure multi-cloud collaboration framework for Cloud-Fog-Assisted IoT systems is presented. It includes a role-based trust evaluation method, user authentication, and access control mechanisms to ensure security and privacy in multi-cloud environments.

Work [40] addresses the issue of access credential misuse in Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for cloud storage systems. The authors propose CryptCloud±, a revocable CP-ABE system with white-box traceability and auditing, enhancing security and mitigating misuse. In work [41], DSFlow is introduced as a secure and fine-grained flow control system for subscription-based data services in cloud-edge computing architecture. It employs receiver-policy attribute-based ACE (RA-ACE) to enable fine-grained access control policies and resists malicious publishers.

The security of attribute-based encryption in cloud data storage systems is discussed in work [42]. The authors propose a revocable attribute-based data storage (RADS) scheme that offers fine-grained access control, efficient user revocation, and offloads cryptographic operations to the cloud for improved performance. In work [43], the ReFlat module is introduced to address access frequency pattern leakage in encrypted cloud data. It uses K-duplication obfuscation within Intel SGX hardware enclaves to secure data access patterns and outperforms existing schemes in terms of security and robustness. Work [44] presents a server-aided revocable fine-grained access control mechanism for cloud storage. It efficiently manages access control, immediate and robust user revocation, and outsources complex decryption operations to the cloud, reducing user overhead.

In work [45], the authors tackle the issue of access frequency pattern leakage in encrypted cloud data. They propose the ReFlat module, which employs K-duplication obfuscation within Intel SGX hardware enclaves to secure data access patterns effectively. The paper [46] discusses cloud service trustworthiness assessment and proposes a method based on D-S theory and Markov chain to assess cloud service trustworthiness states and their changes, helping users make informed decisions. Finally, work [47] introduces a separable self-attention mechanism for point clouds, enabling the capture of both local and global contexts. This mechanism is incorporated into the Separable Transformer architecture, demonstrating competitive performance in point cloud analysis. In work [48], the authors propose a biometric-based authentication protocol for secure access to remote cloud servers. The protocol derives a unique identity from a user's biometric data, eliminating the need to store private keys, and ensures secure message transmission using session keys generated from biometric templates.

Work [49] focuses on healthcare IoT systems and proposes a scheme that combines attribute-based encryption, cloud, and edge computing to provide fine-grained access control while maintaining data verification. The scheme is formally analyzed and shown to outperform existing solutions. Finally, the work in [50] explores the use of Infrastructure as Code (IaC) tools in Multi-access Edge Computing (MEC) environments. These tools automate the deployment of cloud-like services closer to end-users, improving latency and adaptability. Thus, the reviewed works cover a wide range of access control models and strategies across various domains, from IoT and cloud storage to healthcare and point cloud analysis. These approaches aim to enhance security, privacy, and efficiency in access control systems.

3. Comparative Analysis

As per the review of existing models used for access control, it can be observed that each of these models have different complexity & efficiency levels. In this section we compare each of these models in terms of different evaluation metrics. This evaluation can be observed from table 2, where they are compared in terms of Security, Cost of Deployment, Efficiency, Complexity, and Scalability levels. These metrics were quantized as per their characteristics. This was done based on performance of the models as discussed in individual review documents.

Method	**Security**	**Cost of Deployment**	**Efficiency**	**Complexity**	**Scalability**
[1]	Improved data security and integrity.	May require additional computational resources.	Better data processing period and energy consumption compared to baseline models.	Specific to big data storage.	Scalability, Trustworthiness, Data governance, Transparency.

[2]	Purpose-aware access control model.	Limited granularity and expressiveness of existing mechanisms.	Small to medium performance overhead.	Unified access control mechanism.	Effective access control functionalities.
[3]	Hierarchical structure.	Complex implementation. Potential scalability issues.	Federated learning enhances privacy and security of big data analytics in IoT.	Adaptive data compression reduces data transfer volume.	Scalable learning rate. Trust management.
[4]	Improved data security. Lower computational overhead.	Complex scheme with multiple components. Smart contracts and blockchain integration.	Proposed scheme addresses data protection issues in high-dimensional attribute domains.	HAD-FME improves data security and reduces computational cost.	Efficient attribute revocation.
[5]	Efficient revocation functionality. Scalable revocation based on the cardinality of users.	Involvement of an untrusted cloud server in unsigncryption tasks.	ID-based signcryption scheme with efficient revocation.	Enables secure big data communications with outsourced unsigncryption.	Simultaneous achievement of confidentiality, authenticity, non-repudiation, and integrity.
[6]	Verifiable data access mechanism. Data integrity.	Complex architecture with multiple sub-architectures. Potential scalability challenges.	Proposed architecture combines big data systems and blockchain for healthcare data analytics.	Zero-knowledge protocol ensures privacy and data integrity.	Effective analysis and privacy solutions for healthcare big data.
[7]	Utilizes publicly accessible data.	Limited to urban areas. Dependent	Social network data used as a	Identification of spatial and	Association between human

	Provides insights into human mobility patterns.	on social network data.	proxy for human mobility analysis.	temporal regularity in human mobility patterns.	mobility and COVID-19 spread.
[8]	Utilizes cloud datacenters for energy consumption. Efficient consumption of surplus energy.	Specific to surplus energy consumption. May require cloud datacenter participation.	Cloud datacenters used to consume surplus energy from renewable sources through auction sales.	Integrated auctioning-scheduling mechanism for efficient energy consumption.	Balancing surplus energy from renewable sources. Energy-efficient cloud datacenter utilization.
[9]	Corrects differences caused by light brightness. Provides accurate urban-rural area identification.	Limited to urban-rural area identification. Reliance on NTL data.	Fusion of NTL data with POI and BM data for accurate urban-rural area identification.	Significant improvement in accuracy and kappa values with data fusion.	Urban-rural area identification. Regional urban-rural development.
[10]	Efficient representation of traffic flow features. Better performance on retail road network data.	Specific to retail road network traffic flow. Complex model architecture.	RTS-GAT model for analyzing factors affecting retail road network traffic flow.	Unique deep learning-based representation and fusion method.	Improved performance on multiple datasets.
[11]	Enhanced detection accuracy. Reduced false positives.	Complex model architecture. May require significant computational resources.	Hierarchical intrusion detection model with multiple deep learning models and attention mechanism.	Improved detection accuracy and reduced false positives.	Combines spatial and temporal features for effective intrusion detection.
[12]	Captures user's mixed full-term interest. Models	Complex model architecture. Specific to news	NP-3C-FIP system for news	Effective in improving news recommendatio	Incorporates latent Dirichlet allocation

	sequential interest features.	recommendation .	personalization combining news content characterization and full-term interest portrayal.	n performance.	(LDA) and personalized attention mechanism.
[13]	End-to-end encryption. Enhanced security and privacy.	Complex implementation. Specific to IoT applications.	IoTChain model for blockchain-based decentralized distributed storage and sharing with end-to-end encryption.	Fine-grained access control and permissioned blockchain.	Proof-of-authority (PoA) consensus mechanism.
[14]	Utilizes cloud datacenters for energy consumption. Efficient consumption of surplus energy.	Specific to surplus energy consumption. May require cloud datacenter participation.	Cloud datacenters used to consume surplus energy from renewable sources through auction sales.	Integrated auctioning-scheduling mechanism for efficient energy consumption.	Balancing surplus energy from renewable sources. Energy-efficient cloud datacenter utilization.
[15]	Provides security against malicious data publishers. Secure cloud storage.	Complex scheme with threat model and security model. Specific to cloud storage with malicious data publishers.	Sanitizable Access Control System (SACS) for secure cloud storage in the presence of malicious data publishers.	Resists unauthorized decryption by malicious users.	Based on q-Parallel Bilinear Diffie-Hellman Exponent Assumption.
[16]	End-to-end security. Access control and trust evaluation.	Potential complexity in implementation. Specific to Edge-	TABI mechanism for trust-based access control	Mitigates impact of malicious IoT users and	Utilizes edge computing for reduced

		IoT Networks.	in Edge-IoT Networks using blockchain.	devices.	overhead.
[17]	Distributed and trustful UAV data access. Fine-grained access control. User traceability.	Potential complexity in implementation. Specific to UAV data sharing.	Proposed BPADAC scheme for secure UAV data sharing in cloud-based IoD.	Leverages blockchain and DHT for distributed and trustful data access.	Provides fine-grained access control and user traceability.
[18]	Strong security measures. Reduced communication overhead. Fine-grained access control.	Limited to cloud access control. Specific to SSO.	Introduced D2-IAM for SSO access control in the cloud.	Uses smart contracts and blockchain for access control.	Minimizes communication overhead and supports fine-grained access.
[19]	Multilevel access control. Privacy preservation. Transparency and data integrity.	Complex framework. Specific to e-health data access.	LBAC model integrated with blockchain-based smart contracts for e-health data access.	Provides multilevel access control security.	Preserves privacy, maintains transparency, and ensures data integrity.
[20]	Enhanced error correction. Improved device speed and performance.	Specific to STT-MRAM technology. Complex encoding process.	Proposed Hamming code-based encoder for STT-MRAM error correction.	Improved speed and performance of STT-MRAM devices.	Addresses process variations and thermal fluctuations.
[21]	Physical location-based access control. Dynamic device management. Mitigates single	Complex IoT environment implementation. Specific to IoT access control.	Introduced DABAC for access control in dynamic IoT environments.	Utilizes smart contracts and intelligent gateways.	Ensures physical location limitations and security in untrusted IoT

	points of failure.				environments.
[22]	Energy-efficient consensus. Spectrum violation detection. Spectrum sensing.	May require additional hardware. Specific to DSA in IoT.	Proposed DPoS consensus mechanism for blockchain-based DSA.	Addresses spectrum violations and enables spectrum sensing.	Offers energy-efficient consensus for DSA.
[23]	Improved throughput. Cooperative networking. Effective protocol design.	Limited to ultraviolet networks. Specific to collaborative networking.	Proposed ultraviolet random access collaborative networking protocol.	Utilizes dynamic timeslot allocation for higher throughput.	Demonstrated cooperative forwarding and random access capabilities.
[24]	Real-time motion control. Improved control performance. Feasible for factory automation.	Specific to PON-based access edge. May require modifications to existing PON systems.	Introduced real-time motion control method for PON-based access edge.	Utilizes delay compensation for control performance improvement.	Demonstrated feasibility for factory automation.
[25]	Cross-organization data sharing. Transparency and auditability. Privacy preservation.	Requires a decentralized system. Overhead of blockchain adoption.	Proposed SmartAccess system for cross-organization medical records sharing.	Utilizes blockchain and smart contracts for access control.	Provides transparency, auditability, and privacy.
[26]	Reduced chattering. Consensus in multi-agent systems. Tolerance to communication delay.	Complex control method. May require significant computational resources.	Investigated distributed sliding mode control for consensus in multi-agent systems.	Reduced chattering and tolerates communication delay.	Achieves quick consensus with optimal controller.

[27]	Intelligent user access control. Reduced frequent handovers. High performance.	Complex DRL implementation. Specific to O-RAN deployment.	Proposed DRL-based scheme for intelligent user access control in O-RAN.	Optimizes user throughput and reduces frequent handovers.	Demonstrated outstanding performance.
[28]	Game theory-based access control. Efficient deployment design. Achieved Nash equilibrium.	Specific to UAV-BSs network. Limited to GU access control.	Optimized GU access control using game theory in multiple UAV-BSs network.	Achieved Nash equilibrium in access control game.	Efficient deployment design for UAV-BSs.
[29]	Secure EMR sharing. Privacy preservation. Lightweight policy update.	May require integration with fog computing. Specific to EMR sharing.	Proposed LightMED for secure EMR sharing in cloud with IoT integration.	Utilizes fog computing, CP-ABE, and blockchain.	Provides efficient privacy-preserving access control.
[30]	Reliable access control. Auditability and scalability. Off-chain attribute distribution.	Requires blockchain adoption. Overhead of smart contract deployment.	Introduced smart contract-based access control framework for resource access control.	Provides reliability, auditability, and scalability.	Uses off-chain signatures for attribute distribution.
[31]	Role management system. Conflict resolution. Improved system security.	Requires blockchain adoption. May have an overhead of system performance.	Proposed a blockchain-based access control scheme for IoT and role-based access control.	Resolves conflicting roles and improves system security.	Provides better response times for concurrent user requests.
[33]	Maximizes system utility, considers	Unknown energy arrival process,	Improved system utility.	MEC-based access control strategy for	Green IoT systems.

	spectral efficiency and access ratio.	dynamical changes in network state.		green IoT systems using a CMDP and RCQN algorithm. Introduced an LSTM-based energy prediction module.	
[34]	Enables delegated keyword-based data search, supports multi-organization clouds, efficient decryption, and revocation.	None mentioned.	Proposed an authorized keyword search scheme using Role-Based Encryption (RBE) in a cloud environment.	Supported multi-organization cloud environments. Efficient decryption and revocation mechanisms.	Cloud environments requiring keyword-based search.
[35]	Restricts system access to authorized users.	None mentioned.	Described Kubernetes RBAC authorization sub-system for securing access to resources in clusters.	Kubernetes clusters and resource access control.	-
[36]	Suitable for multi-organization clouds, efficient user revocation, reduced overhead.	None mentioned.	Presented an RBE scheme with efficient user revocation for multi-organization cloud storage. Introduced an	Multi-organization cloud storage systems.	-

			outsourced decryption mechanism.		
[37]	Achieved average improvements in CPU usage, memory usage, delay, and jitter metrics.	None mentioned.	Introduced RBAC-based load balancing-assisted resource management framework (RBAC-LBRM) for IoT-edge-fog networks, which significantly improved performance metrics.	IoT-edge-fog networks for load balancing and resource management.	-
[38]	Provides transparency, reliability, and robustness. Efficient for IIoT applications with low latency requirements.	None mentioned.	Proposed DHACS, a Decentralized Hybrid Access Control for Smart Contracts, for Industrial Internet-of-Things (IIoT) applications. DHACS combines role-based, rule-based, and organization-based access controls.	IIoT applications with blockchain integration.	-
[39]	Enhances trustworthiness of MCSC, preserves security of services.	Vulnerable to malicious users.	Presented a trust-based secure multi-cloud collaboration framework for Cloud-Fog-	Cloud-Fog-Assisted IoT systems requiring trust-based collaboration.	-

			Assisted IoT systems. Included role-based trust evaluation, user authentication, and access control mechanisms.		
[40]	Provides accountability and revocation mechanisms. Mitigates access credential misuse.	Inevitable security breach with CP-ABE.	Proposed CryptCloud±, a revocable CP-ABE-based cloud storage system with white-box traceability and auditing, addressing access credential misuse.	Secure cloud storage systems requiring fine-grained access control.	-
[41]	Resists malicious publishers, allows valid subscribers to decrypt sanitized ciphertexts.	Access control policies may not apply to subscriptions.	Introduced DSFlow, a secure and fine-grained flow control system for subscription-based data services in a cloud-edge computing architecture.	Subscription-based data services with secure flow control.	-
[42]	Offers role-centric and attribute-centric approaches.	None mentioned.	Developed two hybrid access control models (HyBAC RC and HyBAC AC) for smart home IoT, combining ABAC and RBAC.	Smart home IoT access control.	-

[43]	Achieves fine-grained access control, allows CSP to share computations, offloads revocation operations.	High computation overheads during user revocation.	Proposed a revocable attribute-based data storage (RADS) scheme for cloud storage with fine-grained access control and efficient user revocation.	Cloud storage with fine-grained access control.	-
[44]	Efficient fine-grained access control, immediate and robust user revocation.	None mentioned.	Presented a server-aided revocable fine-grained access control mechanism with cloud assistance, achieving efficient access control with reduced user-side computations.	Fine-grained access control in cloud services.	-
[45]	Addresses access frequency pattern leakage, achieves robustness.	Security risk of involving intermediate proxy.	Proposed the ReFlat module for mitigating access frequency pattern leakage in encrypted cloud data, improving security under specific threat models.	Secure cloud data access under specific threat models.	-
[46]	Objectively assesses cloud service trustworthiness state and	None mentioned.	Developed a method to assess cloud service trustworthiness based on D-S	Assessing cloud service trustworthiness and managing trust.	-

	changes.		theory and Markov chain, considering the dynamic nature of cloud environments.		
[47]	Captures both local and global contexts in point cloud analysis.	None mentioned.	Designed a separable self-attention mechanism for point clouds and a Separable Transformer architecture.	Point cloud analysis with improved self-attention.	-
[48]	No need to store private keys, efficient session key generation.	None mentioned.	Proposed a biometric-based authentication protocol for secure access to a remote server. Utilized biometric data as secret credentials and derived a unique identity.	Secure access to remote servers using biometric data.	-
[49]	Offers efficient, flexible, and secure fine-grained access control with data verification.	None mentioned.	Proposed a healthcare IoT system using attribute-based encryption, cloud, and edge computing for fine-grained access control.	Healthcare IoT networks requiring fine-grained access control.	-
[50]	Achieved efficient, flexible, secure	None mentioned.	Addressed fine-grained access control in	Healthcare IoT networks requiring fine-	-

	fine-grained access control.		Healthcare IoT using attribute-based encryption and cloud-edge computing.	grained access control.	

Table 2. Empirical Analysis of the ModelsThe table presents a summary of various methods or models with respect to their Security, Cost of Deployment, Efficiency, Complexity, and Scalability levels. Each method is evaluated based on these criteria:

Security: Several models focus on enhancing data security and integrity. Notable mentions include Method [1] with improved data security and integrity and Method [13] with end-to-end encryption. These models prioritize data protection and privacy.

Cost of Deployment: Models like Method [2] (Purpose-aware access control) and Method [5] (ID-based signcryption) stand out for their relatively lower deployment costs, involving limited performance overhead and efficient revocation mechanisms.

Efficiency: Method [1] claims better data processing and energy consumption compared to baseline models, indicating high efficiency. Method [10] (RTS-GAT model) also aims for efficient representation of traffic flow features and performance improvement.

Complexity: Some models are characterized by complex implementations, such as Method [3] (Hierarchical structure) and Method [6] (Blockchain integration for healthcare analytics). These models might require more resources and expertise to implement.

Scalability: Several models emphasize scalability, such as Method [3] with adaptive data compression for big data analytics in IoT and Method [16] (TABI mechanism for Edge-IoT Networks) that utilizes edge computing for reduced overhead. Method [28] also addresses efficient deployment design for scalability.

Overall, the choice of model depends on the specific requirements and priorities of a given application. Models like Method [1], [2], and [5] may be preferred for their cost-effectiveness and efficiency, while those focusing on complex scenarios, such as healthcare analytics (Method [6]), urban mobility (Method [7]), and energy consumption (Method [8]), offer specialized solutions. Scalability is a key consideration in IoT applications, and models like Method [3], [16], and [28] aim to address this requirement. Additionally, security is a common concern across all methods, with several proposing blockchain integration and encryption techniques to enhance data protection.

4. Conclusions & Future Scope

In this comprehensive review, we have examined a diverse range of models and methods aimed at addressing the multifaceted challenges of security, cost of deployment, efficiency, complexity, and scalability across various domains of technology and data management. Each model presented unique strengths and trade-offs, catering to specific application requirements.

Security emerged as a pervasive concern in nearly all the models we explored. The importance of safeguarding data integrity and privacy remains paramount, especially in the context of emerging technologies like the Internet of Things (IoT) and cloud computing. Models such as those employing end-to-end encryption (e.g., Method [13]) and secure access control systems (e.g., Method [15]) demonstrated a commitment to enhancing security and protection against malicious actors.

Cost of Deployment was another critical factor considered. Several models, including Method [2] and Method [5], demonstrated cost-effective approaches with minimal deployment overhead. These models are well-suited for organizations seeking efficient solutions that don't strain their budgets.

Efficiency was a key focus for models like Method [1] and Method [10]. They exhibited improved data processing and energy consumption, essential for optimizing resource utilization and reducing operational costs.

Complexity was acknowledged as a challenge, especially in models targeting intricate scenarios such as healthcare data analytics (e.g., Method [6]). While complexity can hinder adoption, it is essential to address real-world intricacies adequately.

Scalability is vital in the era of big data and IoT. Models like Method [3], Method [16], and Method [28] recognized the significance of scalable solutions, catering to the growing demands of data management in dynamic environments.

Future Scope:

Looking ahead, there are several exciting avenues for further research and development in this field:

- **Interoperability**: Future models should aim to enhance interoperability between different technologies and systems. This will be particularly relevant as organizations seek to integrate diverse solutions into their ecosystems.

- **Quantum Computing**: As quantum computing matures, it will introduce new paradigms and challenges for data security. Future models need to explore quantum-resistant encryption techniques and quantum-safe access control systems.

- **Edge and Fog Computing**: The proliferation of edge and fog computing necessitates novel access control and security models tailored to these distributed environments. Future research should focus on resource-efficient solutions for data management at the edge.

- **AI and Machine Learning Integration**: Leveraging AI and machine learning for dynamic access control and threat detection is an area ripe for exploration. Models that adapt in real-time to evolving security threats will be invaluable.

- **Usability and User Experience**: While many models prioritize security, ensuring a positive user experience is crucial. Future developments should strike a balance between robust security measures and user-friendly interfaces.

- **Regulatory Compliance**: As data privacy regulations continue to evolve worldwide, models must align with these frameworks. Future research should emphasize compliance and data governance.

- **Environmental Sustainability**: Sustainable computing practices are gaining importance. Models that address energy efficiency and sustainable data center operations will be increasingly relevant.

In conclusion, this review underscores the dynamic nature of technology and data management, where innovation and adaptability are paramount. The future holds exciting possibilities for models that can strike the right balance between security, cost-effectiveness, efficiency, and scalability while addressing the evolving needs of a data-driven world. Researchers and practitioners are encouraged to explore these avenues to shape the next generation of data access control and security solutions.

5. References

[1] Sasikumar, L. Ravi, K. Kotecha, A. Abraham, M. Devarajan and S. Vairavasundaram, "A Secure Big Data Storage Framework Based on Blockchain Consensus Mechanism With Flexible Finality," in IEEE Access, vol. 11, pp. 56712-56725, 2023, doi: 10.1109/ACCESS.2023.3282322.

[2] T. Xue et al., "SparkAC: Fine-Grained Access Control in Spark for Secure Data Sharing and Analytics," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 1104-1123, 1 March-April 2023, doi: 10.1109/TDSC.2022.3149544.

[3] K. A. Awan, I. U. Din, A. Almogren and J. J. P. C. Rodrigues, "Privacy-Preserving Big Data Security for IoT With Federated Learning and Cryptography," in IEEE Access, vol. 11, pp. 120918-120934, 2023, doi: 10.1109/ACCESS.2023.3328310.

[4] Wang, J. Lu, X. Li, P. Cao, Z. Zhou and Q. Wen, "A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-Dimensional Attribute Domains," in IEEE Access, vol. 11, pp. 82989-83003, 2023, doi: 10.1109/ACCESS.2023.3296781.

[5] H. Xiong, K. -K. R. Choo and A. V. Vasilakos, "Revocable Identity-Based Access Control for Big Data with Verifiable Outsourced Computing," in IEEE Transactions on Big Data, vol. 8, no. 1, pp. 1-13, 1 Feb. 2022, doi: 10.1109/TBDATA.2017.2697448.

[6] U. Demirbaga and G. S. Aujla, "MapChain: A Blockchain-Based Verifiable Healthcare Service Management in IoT-Based Big Data Ecosystem," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3896-3907, Dec. 2022, doi: 10.1109/TNSM.2022.3204851.

[7] M. Aljeri, "Big Data-Driven Approach to Analyzing Spatio-Temporal Mobility Pattern," in IEEE Access, vol. 10, pp. 98414-98426, 2022, doi: 10.1109/ACCESS.2022.3206859.

[8] A. U. Hassan et al., "Optimizing the Performance of Data Warehouse by Query Cache Mechanism," in IEEE Access, vol. 10, pp. 13472-13480, 2022, doi: 10.1109/ACCESS.2022.3148131.

[9] Y. Chen and A. Deng, "Using POI Data and Baidu Migration Big Data to Modify Nighttime Light Data to Identify Urban and Rural Area," in IEEE Access, vol. 10, pp. 93513-93524, 2022, doi: 10.1109/ACCESS.2022.3203433.

[10] S. Luo, "RTS-GAT: Spatial Graph Attention-Based Spatio-Temporal Flow Prediction for Big Data Retailing," in IEEE Access, vol. 10, pp. 133232-133243, 2022, doi: 10.1109/ACCESS.2022.3230660.

[11] H. Xu, L. Sun, G. Fan, W. Li and G. Kuang, "A Hierarchical Intrusion Detection Model Combining Multiple Deep Learning Models With Attention Mechanism," in IEEE Access, vol. 11, pp. 66212-66226, 2023, doi: 10.1109/ACCESS.2023.3290613.

[12] W. Fu, "AI-News Personalization System Combining Complete Content Characterization and Full Term Interest Portrayal in the Big Data Era," in IEEE Access, vol. 11, pp. 85086-85096, 2023, doi: 10.1109/ACCESS.2023.3303479.

[13] Z. Ullah, B. Raza, H. Shah, S. Khan and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," in IEEE Access, vol. 10, pp. 36978-36994, 2022, doi: 10.1109/ACCESS.2022.3164081.

A. Abada, M. St-Hilaire and W. Shi, "Auction-Based Scheduling of Excess Energy Consumption to Enhance Grid Upward Flexibility," in IEEE Access, vol. 10, pp. 5944-5956, 2022, doi: 10.1109/ACCESS.2021.3139985.

[14] W. Susilo, P. Jiang, J. Lai, F. Guo, G. Yang and R. H. Deng, "Sanitizable Access Control System for Secure Cloud Storage Against Malicious Data Publishers," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 2138-2148, 1 May-June 2022, doi: 10.1109/TDSC.2021.3058132.

A. Pathak, I. Al-Anbagi and H. J. Hamilton, "TABI: Trust-Based ABAC Mechanism for Edge-IoT Using Blockchain Technology," in IEEE Access, vol. 11, pp. 36379-36398, 2023, doi: 10.1109/ACCESS.2023.3265349.

[15] Z. Ma and J. Zhang, "Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-Based IoD Systems," in IEEE Access, vol. 11, pp. 45206-45221, 2023, doi: 10.1109/ACCESS.2023.3272484.

[16] S. Fugkeaw, "Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud," in IEEE Access, vol. 11, pp. 25480-25491, 2023, doi: 10.1109/ACCESS.2023.3255885.

[17] T. Haritha and A. Anitha, "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain- Based Smart Contracts System," in IEEE Access, vol. 11, pp. 114322-114340, 2023, doi: 10.1109/ACCESS.2023.3324740.

[18] T. A. Nguyen and J. Lee, "Sparse Code With Minimum Hamming Distance of Three for Spin-Torque Transfer Magnetic Random Access Memory," in IEEE Access, vol. 11, pp. 114071-114079, 2023, doi: 10.1109/ACCESS.2023.3324255.

[19] F. Guo, G. Shen, Z. Huang, Y. Yang, M. Cai and L. Wei, "DABAC: Smart Contract-Based Spatio-Temporal Domain Access Control for the Internet of Things," in IEEE Access, vol. 11, pp. 36452-36463, 2023, doi: 10.1109/ACCESS.2023.3257027.

[20] P. Fernando et al., "Distributed-Proof-of-Sense: Blockchain Consensus Mechanisms for Detecting Spectrum Access Violations of the Radio Spectrum," in IEEE Transactions on Cognitive Communications and Networking, vol. 9, no. 5, pp. 1110-1125, Oct. 2023, doi: 10.1109/TCCN.2023.3291366.

[21] Li, Z. Xu, J. Wang, J. Zhao, A. Qi and J. Li, "Ultraviolet random access collaborative networking protocol based on time division multiple access," in Journal of Optical Communications and Networking, vol. 15, no. 6, pp. 393-403, June 2023, doi: 10.1364/JOCN.479471.

[22] Y. Koyasako, T. Suzuki, T. Yamada, T. Shimada and T. Yoshida, "Demonstration of Real-Time Motion Control Method for Access Edge Computing in PONs," in IEEE Access, vol. 10, pp. 168-175, 2022, doi: 10.1109/ACCESS.2021.3136876.

[23] M. Tuler De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos and S. D. Olabarriaga, "SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts," in IEEE Access, vol. 10, pp. 117836-117854, 2022, doi: 10.1109/ACCESS.2022.3217201.

[24] L. Yuan and J. Li, "Consensus of Discrete-Time Nonlinear Multiagent Systems Using Sliding Mode Control Based on Optimal Control," in IEEE Access, vol. 10, pp. 47275-47283, 2022, doi: 10.1109/ACCESS.2022.3171825.

[25] Y. Cao, S. -Y. Lien, Y. -C. Liang, K. -C. Chen and X. Shen, "User Access Control in Open Radio Access Networks: A Federated Deep Reinforcement Learning Approach," in IEEE Transactions on Wireless Communications, vol. 21, no. 6, pp. 3721-3736, June 2022, doi: 10.1109/TWC.2021.3123500.

[26] Y. Liu, J. Xie, C. Xing and S. Xie, "Access Control and Deployment Design for Multi-UAV Assisted Wireless Networks," in IEEE Wireless Communications Letters, vol. 11, no. 11, pp. 2380-2384, Nov. 2022, doi: 10.1109/LWC.2022.3204060.

[27] S. Fugkeaw, L. Wirz and L. Hak, "Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing," in IEEE Access, vol. 11, pp. 62998-63012, 2023, doi: 10.1109/ACCESS.2023.3288332.

[28] J. Hao, C. Huang, W. Tang, Y. Zhang and S. Yuan, "Smart Contract-Based Access Control Through Off-Chain Signature and On-Chain Evaluation," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 4, pp. 2221-2225, April 2022, doi: 10.1109/TCSII.2021.3125500.

[29] T. Zaidi, M. Usman, M. U. Aftab, H. Aljuaid and Y. Y. Ghadi, "Fabrication of Flexible Role-Based Access Control Based on Blockchain for Internet of Things Use Cases," in IEEE Access, vol. 11, pp. 106315-106333, 2023, doi: 10.1109/ACCESS.2023.3318487.

[30] K. A. Abuhasel, "A Zero-Trust Network-Based Access Control Scheme for Sustainable and Resilient Industry 5.0," in IEEE Access, vol. 11, pp. 116398-116409, 2023, doi: 10.1109/ACCESS.2023.3325879.

[31] L. Xu, M. Qin, Q. Yang and K. -S. Kwak, "Learning-Aided Dynamic Access Control in MEC-Enabled Green IoT Networks: A Convolutional Reinforcement Learning Approach," in IEEE Transactions on Vehicular Technology, vol. 71, no. 2, pp. 2098-2109, Feb. 2022, doi:

10.1109/TVT.2021.3135885.

[32] N. H. Sultan, M. Laurent and V. Varadharajan, "Securing Organization's Data: A Role-Based Authorized Keyword Search Scheme With Efficient Decryption," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 25-43, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3071304.

[33] G. Rostami, "Role-Based Access Control (RBAC) Authorization in Kubernetes," in Journal of ICT Standardization, vol. 11, no. 3, pp. 237-260, 2023, doi: 10.13052/jicts2245-800X.1132.

[34] N. H. Sultan, V. Varadharajan, L. Zhou and F. A. Barbhuiya, "A Role-Based Encryption (RBE) Scheme for Securing Outsourced Cloud Data in a Multi-Organization Context," in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 1647-1661, 1 May-June 2023, doi: 10.1109/TSC.2022.3194252.

[35] R. Kumar and N. Agrawal, "RBAC-LBRM: An RBAC-Based Load Balancing Assisted Efficient Resource Management Framework for IoT-Edge-Fog Network," in IEEE Sensors Letters, vol. 6, no. 8, pp. 1-4, Aug. 2022, Art no. 5501104, doi: 10.1109/LSENS.2022.3191388.

[36] R. Saha et al., "DHACS: Smart Contract-Based Decentralized Hybrid Access Control for Industrial Internet-of-Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3452-3461, May 2022, doi: 10.1109/TII.2021.3108676.

[37] J. Zhang, T. Li, Z. Ying and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1546-1561, 1 April-June 2023, doi: 10.1109/TCC.2022.3147226.

[38] J. Ning, Z. Cao, X. Dong, K. Liang, L. Wei and K. -K. R. Choo, "CryptCloud$^+$+: Secure and Expressive Data Access Control for Cloud Storage," in IEEE Transactions on Services Computing, vol. 14, no. 1, pp. 111-124, 1 Jan.-Feb. 2021, doi: 10.1109/TSC.2018.2791538.

[39] Q. Huang, C. Wang and L. Chen, "Secure and Fine-Grained Flow Control for Subscription-Based Data Services in Cloud-Edge Computing," in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 2165-2177, 1 May-June 2023, doi: 10.1109/TSC.2022.3203378.

[40] S. Ameer, J. Benson and R. Sandhu, "Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 4032-4051, 1 Sept.-Oct. 2023, doi: 10.1109/TDSC.2022.3216297.

[41] H. Deng, Z. Qin, Q. Wu, Z. Guan and H. Yin, "Revocable Attribute-Based Data Storage in Mobile Clouds," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 1130-1142, 1 March-April 2022, doi: 10.1109/TSC.2020.2984757.

[42] H. Ma, R. Zhang, S. Sun, Z. Song and G. Tan, "Server-Aided Fine-Grained Access Control Mechanism with Robust Revocation in Cloud Computing," in IEEE Transactions on Services Computing, vol. 15, no. 1, pp. 164-173, 1 Jan.-Feb. 2022, doi: 10.1109/TSC.2019.2925028.

[43] Z. Han, H. Hu and Q. Ye, "ReFlat: A Robust Access Pattern Hiding Solution for General Cloud Query Processing Based on K-Isomorphism and Hardware Enclave," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1474-1486, 1 April-June 2023, doi: 10.1109/TCC.2021.3137351.

[44] M. Yang, T. Gao, W. Xie, L. Jia and T. Zhang, "The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain," in IEEE Access, vol. 10, pp. 68618-68632, 2022, doi: 10.1109/ACCESS.2022.3185684.

[45] Wang, X. Wang, D. Lv, L. Zhou and G. Shi, "Separable Self-Attention Mechanism for Point Cloud Local and Global Feature Modeling," in IEEE Access, vol. 10, pp. 129823-129831, 2022, doi: 10.1109/ACCESS.2022.3228044.

[46] Panchal, D. Samanta, A. K. Das, N. Kumar and K. -K. R. Choo, "Designing Secure and Efficient Biometric-Based Access Mechanism for Cloud Services," in IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 749-761, 1 April-June 2022, doi: 10.1109/TCC.2020.2987564.

[47] Á. Santos, J. Bernardino and N. Correia, "Automated Application Deployment on Multi-Access Edge Computing: A Survey," in IEEE Access, vol. 11, pp. 89393-89408, 2023, doi: 10.1109/ACCESS.2023.3307023.

[48] S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo and X. Liu, "Lightweight and Expressive Fine-Grained Access Control for Healthcare Internet-of-Things," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 474-490, 1 Jan.-March 2022, doi: 10.1109/TCC.2019.2936481.