Shodh Sari-An International Multidisciplinary Journal

@2024 International Council for Education Research and Training 2024, Vol. 03, Issue 02, 138-166
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7693

COLLABORATIVE AUDITING IN OSMOTIC COMPUTING ENVIRONMENTS: OPPORTUNITIES AND CHALLENGES

Ganapathy, Venkatasubramanian

Faculty in Auditing Department,

Southern India Regional Council of the Institute of Chartered Accountants of India (SIRC of ICAI), Chennai, Tamil Nadu, Bharat

Abstract

As organizations increasingly embrace digital transformation and interconnected ecosystems, the need for effective auditing mechanisms becomes paramount. This research paper delves into the emerging paradigm of collaborative auditing within osmotic environments, exploring both the opportunities and challenges associated with this novel approach. Osmotic environments characterized by their permeable boundaries, allowing the seamless flow of information across diverse platforms, devices, and networks. The opportunities presented by collaborative auditing in osmotic environments are manifold. By leveraging collective intelligence and distributed resources, organizations can achieve more comprehensive and real-time audits. This paper investigates how collaborative auditing fosters a synergistic relationship between human auditors and automated tools, enhancing the accuracy and efficiency of the auditing process. Moreover, the study explores the potential for cross-organizational collaboration, enabling shared insights and threat intelligence to bolster security postures across industries. However, the implementation of collaborative auditing in osmotic environments is not without its challenges. Privacy concerns arise as sensitive information traverses' porous boundaries, demanding robust encryption and access controls. Additionally, the heterogeneity of platforms and technologies poses interoperability challenges addressed for effective collaboration. This research scrutinizes the technical, legal, and ethical hurdles associated with collaborative auditing, offering insights into strategies for mitigating these challenges. The paper also investigates the role of artificial intelligence (AI) and machine learning (ML) in enhancing collaborative auditing capabilities. It explores how these technologies can facilitate anomaly detection, predictive analysis, and

@2024 International Council for Education Research and Training 2024, Vol. 03, Issue 02, 138-166
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7693

automated risk assessment in real-time. The study delves into the ethical considerations surrounding the use of AI in auditing and proposes frameworks for responsible and transparent AI-driven auditing processes. Furthermore, the research examines the human factor in collaborative auditing, emphasizing the importance of training and awareness programs for auditors to adapt to this evolving paradigm. It explores how human-machine collaboration optimized to leverage the strengths of both, fostering a symbiotic relationship that maximizes the effectiveness of auditing processes. In conclusion, this research paper provides a comprehensive analysis of collaborative auditing in osmotic environments, shedding light on the transformative potential of this approach for organizations navigating the complexities of modern interconnected landscapes. By embracing collaborative auditing, organizations can harness the collective intelligence of distributed networks, fortify their cybersecurity postures, and navigate the challenges inherent in osmotic environments. As technology continues to advance, collaborative auditing emerges as a pivotal strategy to ensure the integrity, security, and compliance of digital ecosystems.

Keywords: Osmotic computing, Collaborative Auditing, Encryption and access control, Cyber Security, Artificial Intelligence (AI), Machine Learning (ML).

I. INTRODUCTION

Osmotic computing aims to support the efficient execution of Internet of Things (IoT) services and applications at the network edge. It involves the concept of a "membrane" as an abstraction that represents a virtual environment based on the underlying infrastructure, whether it be cloud or edge computing. This virtual environment allows for the migration of microservices across cloud data centers and edge devices through a software-defined membrane, similar to the diffusion of solvent molecules through a partially permeable membrane in osmosis in chemistry.

The concept of osmotic computing takes analogy from the phenomenon of osmosis in chemistry, where the diffusion of solvent

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

molecules takes place through a partially permeable membrane from a region of higher solvent concentration to a region of lower solvent concentration. Similarly, in osmotic computing, microservices have not confined to a specific infrastructure; instead, they can migrate across cloud data centers and edge devices through a software-defined membrane called osmotic membrane.

Osmotic computing has its roots in the growing need for seamless integration of various computing resources, such as data, applications, and services, across different devices and platforms. As the use of mobile devices, cloud computing, and Internet of Things (IoT) technologies has become more prevalent, there has been a growing demand for a more flexible and efficient computing environment that can adapt to the needs of users and applications.

Collaborative auditing involves the participation and cooperation of various stakeholders, such as auditors, audit clients, and other relevant parties, in the auditing process. It emphasizes open communication, sharing of information, and seeking input or feedback from audit clients during audits. This approach aims to reduce duplication, save costs and resources, and create a more efficient and effective audit process. It can also involve collaborative accounting, where accounting professionals work closely with clients to create friction-free client experiences and reduce the time spent chasing client data.

In the context of internal audits and external audits, collaborative auditing has seen as an essential part of maintaining and improving an effective collaborative relationship management system. It enhances the overall audit process and contributes to the development of a collaborative audit culture.

Examples of Collaborative Auditing:

- In a collaborative audit culture, the audit teams can proactively schedule a time to listen to control owners' questions and make them aware of their findings and recommendations.
- Transparent and collaborative auditing involves taking samples, performing tests, and requesting additional time to perform high-level tests requiring observation, while also considering the audit clients' input and needs.
- Medicaid Program Integrity initiatives involve collaboration with auditors from

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

selected states, where auditors share findings and collaborate with the Centers for Medicare & Medicaid Services (CMS).

- Auditing and reporting a B2B collaboration user in Microsoft Entra involve using access reviews and audit logs to verify and monitor user activities, demonstrating a collaborative approach to user management and security.
- Successful collaborations in internal audit involve working with stakeholders to identify improvements to processes and controls, highlighting the collaborative nature of internal audit activities.

These examples illustrate how collaborative auditing encompasses proactive communication, stakeholder involvement, and shared responsibilities to enhance the effectiveness and transparency of the audit process.

II. RESEARCH QUESTION

"What are the opportunities and challenges associated with collaborative auditing in osmotic computing environments, and how can effective mechanisms be developed to ensure secure and transparent information sharing among interconnected entities in these dynamic and decentralized systems?"

III. TARGETED AUDIENCE

Faculties and students of Institute of Chartered Accountants of India (ICAI), Institute of Cost and Managements Accountants of India (ICMA), Institute of Company Secretaryship of India (ICSI), Indian Institute of Management (IIM), Indian Institute of Technology (IIT), National Institute of Information Technology (NIIT), Research Scholars, UG/PG students, working professionals and those who are interested in Techno-Auditing field.

IV. OBJECTIVES OF THE STUDY

- To provide a comprehensive understanding of osmotic computing and its principles, thereby understanding its potential applications in collaborative auditing.
- To evaluate the effectiveness of osmotic computing in enhancing the efficiency and accuracy of collaborative auditing processes.
- To examine the potential benefits and challenges associated with the integration of osmotic computing in collaborative auditing.
- To suggest recommendations on how osmotic computing, effectively applied in collaborative auditing to maximize benefits and overcome potential challenges.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

V. RESEARCH METHODOLOGY

Systematic Review Analysis used in this research work. Systematic reviews involve a comprehensive and systematic analysis of all relevant studies on a particular topic. These reviews aim to synthesize the existing evidence to provide a comprehensive summary of the state of knowledge on a specific question.

VI. DATA COLLECTION METHOD

As the study is Systematic Review Analysis, secondary data used for the study, collected from e-journals, e-magazines, e-books and the websites of Osmotic Computing and Collaborative Auditing domains,

VII. LITERATURE REVIEW

Osmotic computing introduced in 2016 as a new promising paradigm for the integration between a centralized Cloud Layer, Fog, Edge and IoT Layers. The concept of Osmotic Computing introduced by **Prof. Omer Rana and his colleagues in 2016**.

No.	Author's Name	Year	Study	Focus on Study	Algorithms/Tools used	Findings
1	Smith. et al.	2018	Collaborative Auditing in Osmotic Computing Environments	Security and Performance in Osmotic Computing	RSA (Rivest, Shamir, Adleman-inventors of this algorithms), OsmoAudit	Improved Security; increased performance
2	H. Zhang et.al.	2018	Osmotic Computing in Collaborative Auditing	Osmotic Computing Framework	Proposed a new framework for collaborative Auditing using Osmotic Computing (Cloud+Fog+Edge	Demonstrated its effectiveness in improving audit efficiency and accuracy

@2024 International Council for Education Research and Training 2024, Vol. 03, Issue 02, 138-166
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7693

					+ IoT Layers)	
3	Patel, A. and Lee.S	2019	Distributed Auditing in Osmotic Clouds	Scalability and Fault Tolerance	SHA-256 (Symmetric Algorithm), OsmoVerifier	Enhanced Scalability; Robust Fault Tolerance
4	Y. Wang et.al.	2019	Collaborative Auditing in Osmotic Computing Environment	To check transparency and trust in audit processes	Blockchain and Consensus Algorithms	Implemented a collaborative auditing systems using Blockchain and Consensus algorithms in an Osmotic Computing environment showed an improved transparency and trust in audit processes.
5	Garcia. et.al.	2020	Dynamic Auditing Approaches	Dynamic Adaptability	Merkle Tree, OsmoGuard	Flexible Auditing; Adaptation to

@2024 International Council for Education Research and Training 2024, Vol. 03, Issue 02, 138-166
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7693

			for Osmotic Systems			changing environments.
6	S.Li et.al.	2020	Osmotic Computing for secure and efficient Collaborative Auditing	Developed a secure and efficient Collaborative Auditing System using Osmotic Computing	Homomorphic Encryption, Secure multiparty Computation	Demonstrated the effectiveness of homomorphic encryption and secure multiparty computation in preserving data privacy and integrity during audits.
7	Wang, Y. and Chen, L.	2021	Privacy-Preserving Auditing in Osmotic Edge Networks	Privacy Concerns	Homomorphic Encryption	Enhanced privacy protection; secure auditing.
8	Kim, H. and Park, S.	2022	Energy-Efficient Auditing in Osmotic Computing	Energy Consumption	Proof-of-Work, OsmoEnergy	Reduced energy consumption: Efficient Auditing.

VIII.OVERVIEW OF OSMOTIC COMPUTING

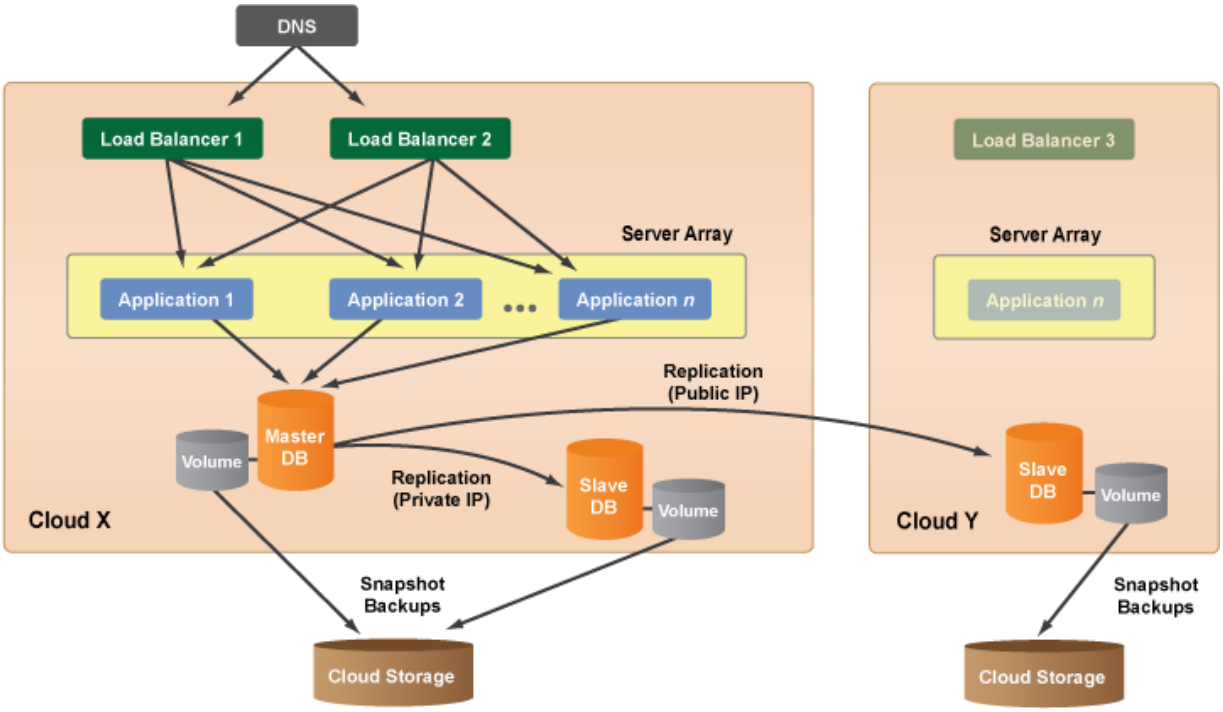
In the context of osmotic computing, the terms cloud, edge, fog, and IoT sensors are integral to understanding the distributed

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

computing models and the seamless deployment of services across various infrastructures.

- **Cloud Computing**:

Architecture of Cloud Computing



Cloud computing involves the delivery of computing services, including servers, storage, databases, networking, software, and analytics, over the internet ("the cloud"). It offers on-demand access to a shared pool of configurable computing resources, which provisioned and released with minimal management effort or service provider interaction.

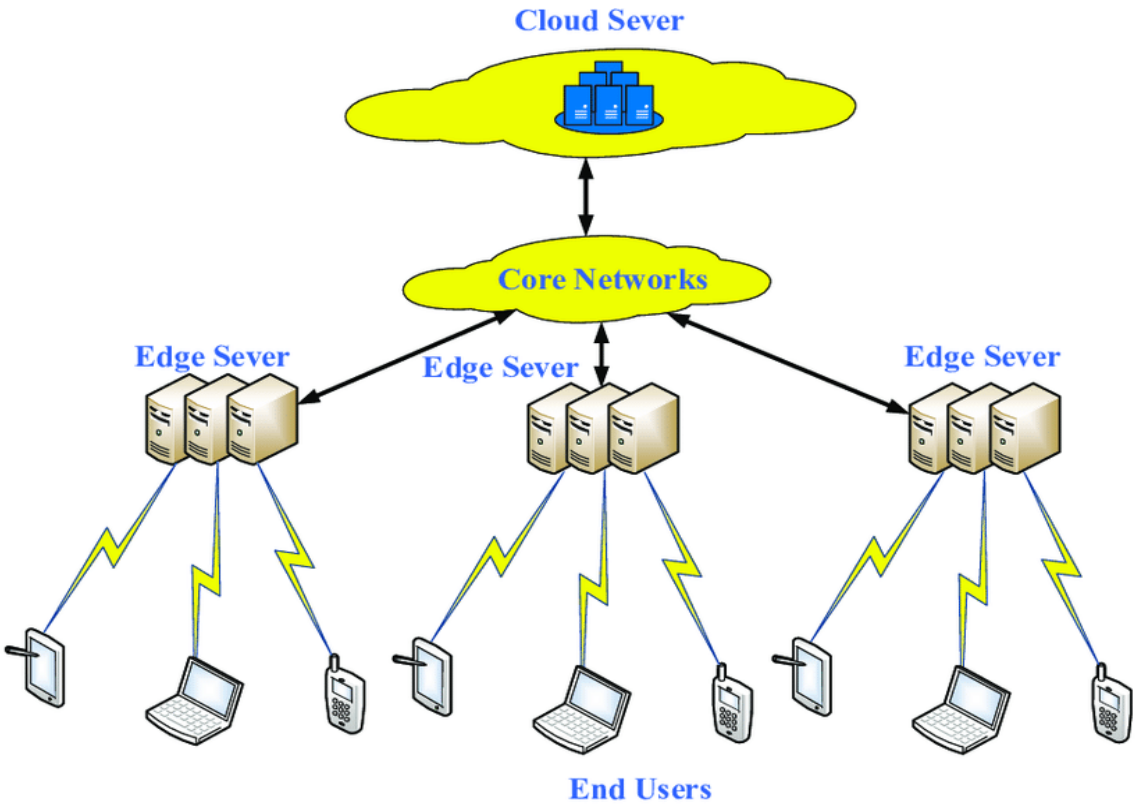
- **Edge Computing**:

Edge computing is a networking philosophy focused on bringing computing as close to the source of data as possible in order to reduce latency and bandwidth use. In simpler terms, edge computing means running fewer processes in the cloud and moving those processes to local places, such as on a user's computer, an IoT device, or an edge server. Bringing computation to the network's edge minimizes the amount

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

of long-distance communication that has to happen between a client and server.

Architecture of Edge Computing:



Edge computing refers to the practice of processing data near the edge of the network, where the data generated, instead of relying on a centralized data-processing warehouse. This approach can improve response times and save bandwidth by processing data locally.

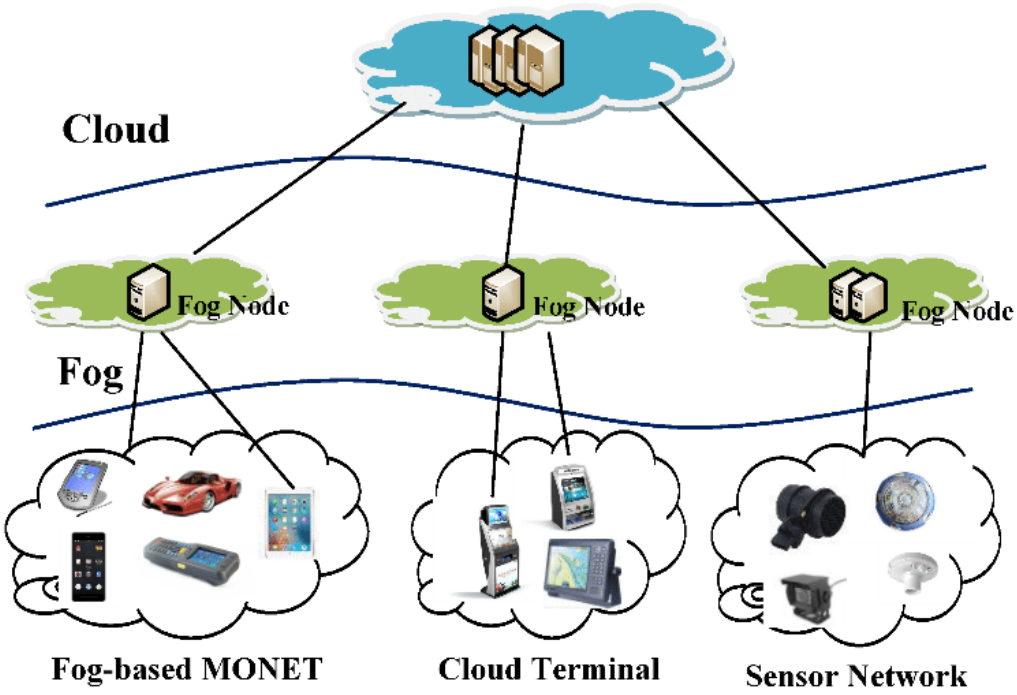
- **Fog Computing:**

Fog computing is a decentralized computing system that extends cloud computing capabilities to better accommodate the Internet of Things (IoT) ecosystem. It aims to bring intelligence, processing, and storage closer to the network's edge to provide quicker and more localized computing services for

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

the connected smart devices that make up the IoT.

Three-Layer Fog Computing Architecture



MONET = Mobile Ad hoc Networks

Fog computing extends cloud computing and services to the edge of the network, bringing the advantages and power of the cloud closer to where data is created and acted upon. It aims to improve efficiency and reduce the amount of data transferred to the cloud for processing, analysis, and storage.

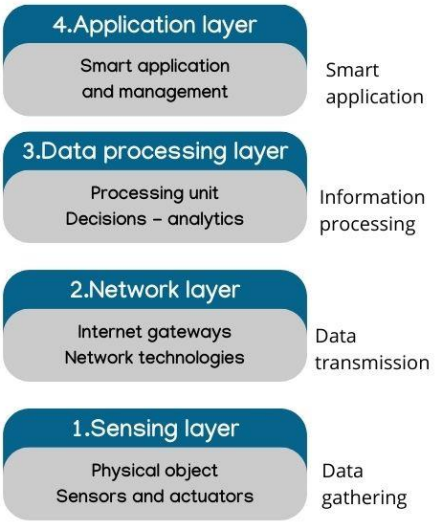
- **IoT Sensors**:

  IoT sensors are physical devices embedded with electronics, software, and sensors that enable them to collect and exchange data over the internet. These sensors are a fundamental component of the Internet of Things (IoT) ecosystem, enabling the collection of real-time data from the environment, which used for various applications, including smart homes, industrial automation, and environmental monitoring.

The layers of IoT architecture encompass a range of components, such as the **sensing/perception layer**,

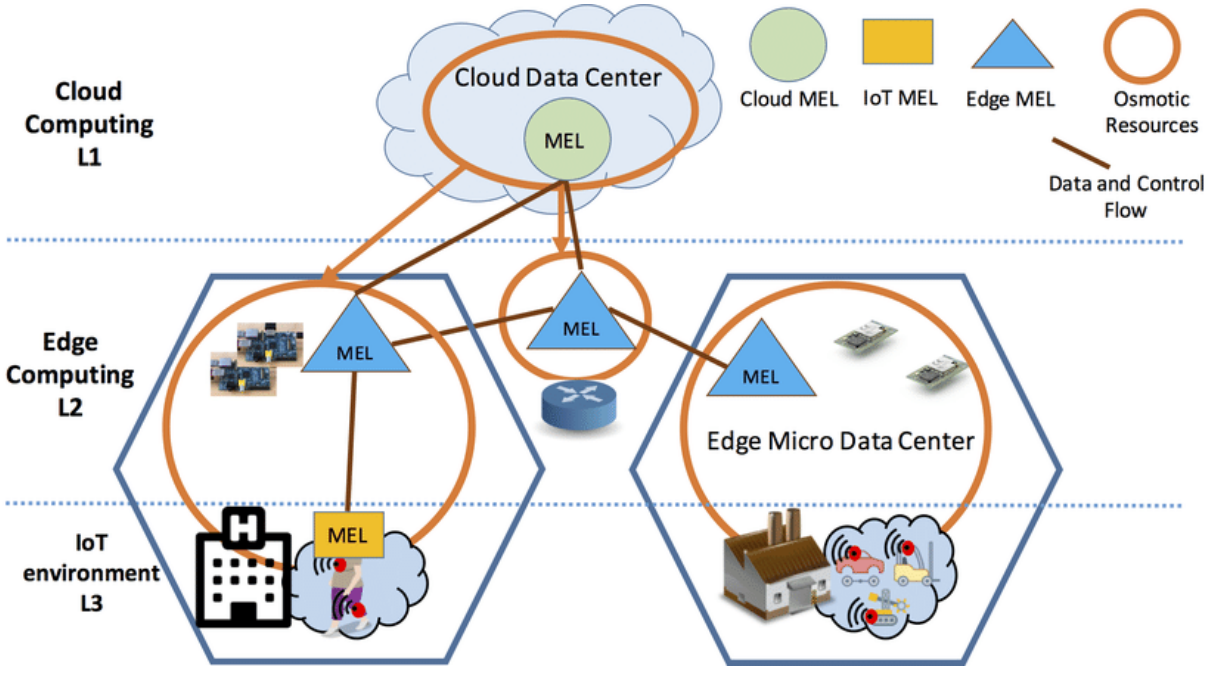
@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

network/connectivity layer, **data processing layer** and **user interface or application layer**. These constitute an all-encompassing framework for joining up devices with their users.



In the context of osmotic computing, these components play a crucial role in the dynamic migration and management of microservices across different infrastructures, contributing to the seamless deployment of IT services and the efficient utilization of resources. Osmotic computing aims to integrate these distributed computing models to ensure service migration and service heterogeneity, thereby excelling as a new generation computing paradigm.

Osmotic Computing as distributed multi-agent system with Edge Layers

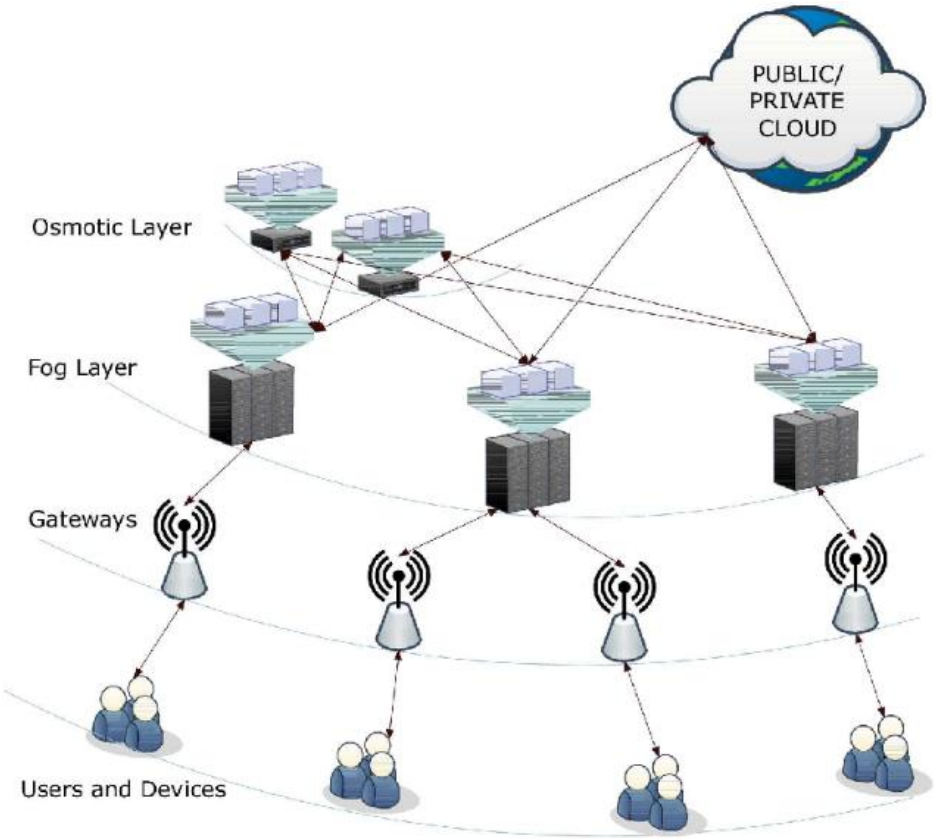


@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

In the context of edge computing, osmotic computing can enable the deployment of computational resources closer to the edge of the network, allowing for faster processing and reduced latency for edge devices. This can be particularly useful for applications that require real-time data processing, such as IoT devices, autonomous vehicles, industrial automation and auditing.

Osmotic computing works with edge layers is by leveraging edge devices to offload computational tasks from the cloud or centralized data centers, reducing the strain on the network and improving overall performance. It achieved through intelligent resource management and dynamic workload distribution across edge nodes.

Osmotic Computing as distributed multi-agent system with Fog Layer



@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

In the context of fog computing principles, osmotic computing used to optimize the use of resources across the fog layers, including edge devices, fog nodes, and cloud servers. It achieved with intelligent resource management and allocation algorithms that dynamically distribute computing and storage tasks based on the availability and capacity of resources in different layers.

For example, osmotic computing can enable edge devices to offload certain tasks to nearby fog nodes when their resources are under heavy load, and fog nodes can in turn offload tasks to cloud servers when their resources are insufficient. This dynamic resource allocation and sharing can improve overall system performance and efficiency in fog computing environments.

(A). COMPONENTS OF OSMOTIC COMPUTING

1. Osmotic Membrane: In osmotic computing, microservices not confined to a specific infrastructure. They can migrate across cloud data centers and edge devices through a software-defined membrane called the osmotic membrane. This membrane facilitates the migration of microservices from a region of higher concentration to a region of lower concentration, similar to the diffusion of solvent molecules in osmosis.

2. Microservices: Microservices are the building blocks of osmotic computing. The small, independent processes that communicate with each other to form a complete application not tie to a specific infrastructure and migrate across different nodes of the osmotic infrastructure, contributing to the dynamic nature of osmotic computing.

3. Software Defined Membrane (SDMem): The Software Defined Membrane (SDMem) in the OSMOSIS architecture acts as a crucial component. It facilitates the migration of microservices and plays a significant role in the dynamic management of IT services in osmotic computing.

4. Osmotic Resource: The main components that make up the system include the osmotic resource, which is essential for the dynamic resource

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

management in osmotic computing. This resource is pivotal in addressing service heterogeneity in latency-sensitive applications.

5. Osmotic Component: Osmotic computing involves various well-defined software components, such as database servers, which contribute to reducing deployment complexities. These components are integral to the functioning of osmotic computing and play a role in the migration and management of microservices.

6. Execute Component: It serves as the starting point of the orbit in osmotic computing. It plays a crucial role in the workflow and execution of tasks within the osmotic computing framework.

7. Osmotic Membrane Component for Security Management: A component of the osmotic membrane developed specifically for security management. This component is crucial for ensuring the security of the migrating microservices and plays a vital role in the overall security framework of osmotic computing.

These components collectively form the foundation of osmotic computing, enabling the dynamic migration and management of microservices across various infrastructures, thereby improving computational infrastructure and addressing service heterogeneity in latency-sensitive applications.

(B). PRINCIPLES OF OSMOTIC COMPUTING

- **Membrane Abstraction:** Osmotic computing utilizes the concept of Membrane Abstraction, which represents a virtual environment based on the underlying infrastructure, such as cloud or edge computing.
- **Unified Computing Model:** Osmotic computing focuses on the design and implementation of a unified computing model that leverages the capabilities of various distributed systems.
- **Resource Management**: Osmotic computing concentrates on techniques to increase IoT services utilizing edge and cloud resources by identifying, designing, and implementing a computing model. It aims to balance load and proper utilization

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

of resources between servers without hindering service deliveries and performances.

- **Application in Various Scenarios**: Osmotic computing has made its hold in many scenarios, ranging from smart cities to smart healthcare, connected cars to industry 4.0. It creates a framework for a dynamic ecosystem.
- **Secure and Dependable Systems**: Osmotic computing can help organizations improve access control systems through consensus mechanisms and underlying features, such as Blockchain technology.

Osmotic computing works by orchestrating a Software Defined Membrane (SDMem) that leverages Blockchain facilities, obeying the osmosis, it sets out the principles and algorithms for simplifying infrastructure heterogeneity and demonstrates the potential in various applications.

These principles and workings form the basis of osmotic computing, which aims to address the dynamic management of IT services and resource allocation in various distributed computing environments.

(C). FEATURES OF COLLABORATIVE AUDITING IN OSMOTIC COMPUTING ENVIRONMENTS:

- **Decentralized Auditing:**

In osmotic computing, which often involves decentralized or distributed architectures, auditing processes distributed across multiple nodes or components. Each node may contribute to the overall audit process, sharing information and findings with others.

- **Consensus Mechanisms:** Collaborative auditing may utilize consensus mechanisms to ensure that audit results agreed upon by the participating entities. This could involve voting, quorum systems, or other techniques to achieve consensus on the state of the system.
- **Shared Information and Transparency**:

Osmotic computing environments may emphasize the sharing of information between different components or layers. Collaborative auditing leverages this characteristic to ensure transparency and enable all entities to have access to relevant audit information.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

- **Dynamic Trust Management**:

Osmotic computing environments often deal with dynamic and evolving systems. Collaborative auditing in such environments may incorporate dynamic trust management mechanisms to adapt to changes in the system and adjust trust levels accordingly.

- **Security and Privacy Considerations**:

Given the collaborative nature, security and privacy concerns are crucial. Collaborative auditing frameworks in osmotic computing should implement robust security measures to protect sensitive audit information and ensure the confidentiality and integrity of the audit process.

- **Smart Contracts or Automated Verification:**

Depending on the level of automation in osmotic computing, smart contracts or automated verification processes used for auditing. This can enhance efficiency and reduce the need for manual intervention.

- **Audit Trail and Logging:**

Maintaining a comprehensive audit trail is essential. In osmotic computing, where interactions between various components are intricate, having detailed logs and an audit trail helps in tracking the flow of information and identifying potential security or compliance issues

(D). GUIDE ON CONDUCTING COLLABORATIVE AUDITING IN OSMOTIC COMPUTING ENVIRONMENTS

- **Understand Osmotic Computing:**

Familiarize with the principles of osmotic computing. This involves understanding how resources allocated and managed in a decentralized and adaptive manner.

- **Identify Audit Objectives:**

Clearly define the objectives of the collaborative audit. These may include security assessments, compliance checks, performance evaluations, and other relevant criteria.

- **Establish Collaboration Framework:**

Define the framework for collaboration among different entities in the osmotic computing environment. This could involve multiple nodes, devices, or components that contribute to the overall system.

- **Define Audit Policies and Standards:**

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

Establish audit policies and standards that align with the goals of osmotic computing. This includes security policies, data integrity standards, and any industry or regulatory compliance requirements.

- **Implement Secure Communication Channels:**

  Ensure that secure communication channels established among the nodes or components participating in the osmotic computing environment. This is crucial for transmitting audit data securely.

- **Integrate Audit Mechanisms**:

  Implement audit mechanisms within the osmotic computing infrastructure. This involves embedding audit functionalities into the components to track and record relevant events and activities.

- **Distributed Logging and Monitoring:**

  Set up a distributed logging and monitoring system to capture real-time information about the osmotic computing environment. This enables auditors to detect and respond to security incidents promptly.

- **Collaborative Decision-Making:**

  Facilitate collaborative decision-making processes among the entities involved in the osmotic computing environment. This may include shared insights, risk assessments, and recommendations for enhancing security and compliance.

- **Automated Audit Tools:**

  Advantage automated audit tools and technologies that can analyze large datasets and provide insights into the overall health and compliance of the osmotic computing environment.

- **Continuous Monitoring and Assessment:**

  Implement continuous monitoring and assessment processes to adapt to the dynamic nature of osmotic computing. Regularly review audit logs, analyze security events, and update audit policies as needed.

- **Incident Response Planning:**

  Develop an incident response plan that outlines the steps taken in the event of a security breach or non-compliance. Collaborate on response strategies to address issues promptly.

- **Regular Auditing Meetings**:

  Schedule regular auditing meetings or forums where stakeholders can discuss audit findings, share insights, and

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

collectively work towards improving the security and compliance posture of the osmotic computing environment.

- **Documentation and Reporting:**

  Maintain comprehensive documentation of audit processes, findings, and remediation actions. Generate periodic reports to communicate the status of security and compliance to relevant stakeholders.

- **Adapt and Evolve:**

  Osmotic computing environments are likely to evolve over time. Keep in mind about advancements in technology, security practices and adapt the collaborative auditing approach accordingly.

- **Training and Awareness:**

  Conduct training sessions to enhance the awareness of individuals involved in the osmotic computing environment regarding security best practices and the importance of collaborative auditing.

  Remember that the field of osmotic computing is dynamic, and new developments may have occurred. It is advisable to stay updated with the latest research and industry practices in osmotic computing and collaborative auditing.

(E). PROBLEMS AND SOLUTIONS OF PRACTICIAL USE OSMOTIC COMPUTING IN COLLABORATIVE AUDITING

Identifying cloud usage: It is important to know which cloud services used by the osmotic computing system and what are the associated risks and controls. Solution is to use a cloud service broker that can monitor and manage the cloud service providers and their service level agreements.

- **Controlling and monitoring user access**: It is essential to ensure that only authorized users can access the data stored in the osmotic computing system and that they follow the principle of least privilege. Solution is to use a blockchain-based collaborative auditing scheme that can verify the identity and role of each user and record their access history in a tamper-proof ledger.
- **Controlling the security of access devices**: It is necessary to protect the devices used to access the osmotic computing system from malware and other threats. For controlling the security of access devices. It is better to use a device

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

management platform that can enforce security policies and update the devices remotely

- **Auditing the cloud service providers:** It is important to ensure that the cloud service providers comply with the security and privacy requirements of the osmotic computing system. Solution is to use a third-party auditor can perform regular audits and issue certificates of compliance.

- **Auditing the fog nodes**: It is crucial to ensure that the fog nodes, which are the intermediate devices between the cloud and the IoT devices, are secure and reliable. It is better to use a collaborative cached data auditing scheme that can enable the fog nodes to verify each other's data integrity and recover data from malicious nodes

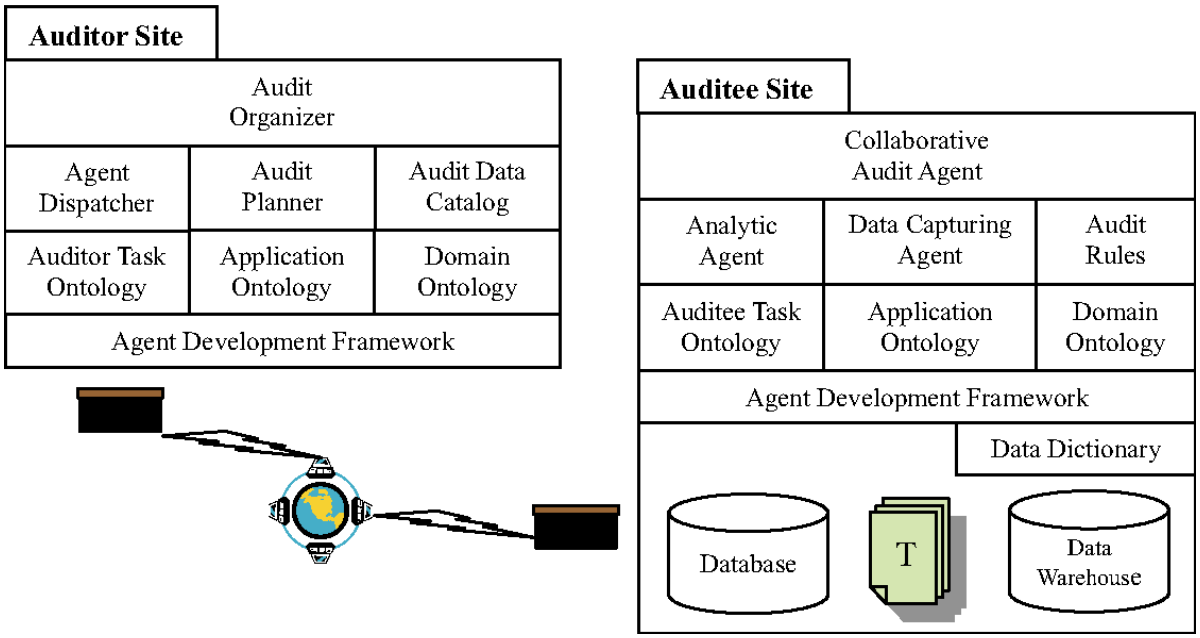
IX. COLLABORATIVE AUDITING IN OSMOTIC COMPUTING ENVIRONMENTS

In the context of osmotic computing, a collaborative continuous auditing model under service-oriented environments established to ensure the security and trustworthiness of resources across federated environments set up by different cooperating stakeholders. This model involves the joint management of Cloud, Edge, and IoT resources across federated environments, emphasizing the need for innovative solutions to manage security and trustworthiness in osmotic computing.

In summary, collaborative auditing in osmotic computing environments involves the joint examination and evaluation of resources across distributed environments to ensure the efficient execution of services and applications. The architecture of osmotic computing, based on service orchestration principles, supports the integration of Cloud and Edge layers, addressing challenges related to the rapid growth of IoT devices and the high volume of data generated by these devices at high speeds. Additionally, a collaborative continuous auditing model established to ensure the security and trustworthiness of resources across federated environments in osmotic computing.

On an agent-based architecture continuous for collaborative auditing

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693



Artificial Intelligence and Machine Learning in Collaborative Auditing

Artificial intelligence (AI) and machine learning (ML) are revolutionizing the Collaborative Auditing profession, offering significant potential for various aspects of the auditing process.

Enhanced Data Analysis and Anomaly Detection

AI and ML programs enable auditors to scan effectively through extensive financial data, swiftly detecting anomalies such as duplicate payments and fraud indicators. These technologies can process vast amounts of structured and unstructured data quickly and efficiently, allowing auditors to identify patterns, trends, and anomalies that may require further investigation.

Comprehensive Review and Analysis

AI can "read" and analyze data from contracts and internal notes, providing valuable insights during data analytics for financial statement audits. The comprehensive review and analysis facilitated by AI enhance the ability to identify both problems and opportunities.

Automation and Quality Improvement

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

AI and ML have the potential to change the way audits performed and enabling auditors to avoid the trade-off between speed and quality. Machine learning algorithms can provide firms with opportunities to review an entire population for anomalies, allowing audit teams to work on the entire data population in a more directed and intentional manner.

Future Impact and Transformation

AI used to transform the audit through automating procedures and enhancing audit quality. As AI and ML deployment intensifies, it will be imperative for auditors to address the challenges posed by this progressively invasive technology, such as data security, the possibility of automated and institutionalized unequal treatment, and mass production of incorrect or discriminatory decisions.

In collaborative auditing, AI and ML play a crucial role in streamlining data analysis, enhancing anomaly detection, and automating procedures, ultimately contributing to the overall quality and efficiency of the auditing process.

Machine Learning Algorithms used in Collaborative Auditing under Osmotic Computing Environment:

Machine learning used in collaborative auditing, including those that might be relevant in an osmotic computing environment:

1. Anomaly Detection Algorithms:

- Isolation Forests
- One-Class SVM (Support Vector Machines)
- Autoencoders

2. Clustering Algorithms:

- K-Means
- Hierarchical Clustering

3. Classification Algorithms:

- Decision Trees
- Random Forests
- Support Vector Machines

4. Ensemble Learning:

- Bagging and boosting techniques for combining multiple models

5. Deep Learning:

- Neural Networks for complex pattern recognition

6. Natural Language Processing (NLP):

- If auditing involves analyzing textual data, NLP techniques could be beneficial.

7. Blockchain Technology:

- While not a machine learning algorithm, blockchain technology integrated to

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

enhance the security and transparency of the auditing process.

The choice of algorithms would depend on the specific requirements of the collaborative auditing task, the types of data involved, and the characteristics of the osmotic computing environment.

X. OPPORTUNITIES AND CHALLENGES OF COLLABORATIVE AUDITING IN OSMOTIC COMPUTING ENVIRONMENTS

Opportunities:

- **Distributed Nature of Osmotic Computing**

  Osmotic computing involves a distributed and decentralized architecture where computing resources spread across various devices and platforms. Collaborative auditing takes advantage of this distribution by allowing multiple nodes to participate in the audit process. This can enhance the overall visibility and assessment of the entire osmotic computing environment.

- **Dynamic Resource Allocation:**

  Osmotic computing environments characterized by dynamic resource allocation, where resources allocated based on demand and availability. Collaborative auditing can help in real-time monitoring and assessment of the dynamically changing resource landscape, ensuring that security and compliance measures are adapted to the evolving conditions.

- **Data Integrity and Privacy:**

  Collaborative auditing can address concerns related to data integrity and privacy in osmotic computing. Multiple parties can collectively verify the integrity of shared data and ensure that privacy policies adhered to across the distributed environment. This is particularly important as data may be processed and stored on various devices.

- **Trust Establishment and Management**:

  Collaborative auditing contributes to the establishment and management of trust in osmotic computing. By allowing different entities to participate in the auditing process, ensuring trust through consensus and validation mechanisms. This is crucial for ensuring the overall security and reliability of the osmotic computing environment.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

- **Risk Assessment and Mitigation**:

Osmotic computing introduces new challenges and risks, including issues related to resource availability, network conditions, and data movement. Collaborative auditing provides an opportunity to collectively assess these risks and implement mitigation strategies. It allows for a more comprehensive understanding of potential vulnerabilities and threats in the distributed system.

- **Cross-Platform Compatibility**:

Osmotic computing involves interactions across various platforms, including different operating systems and device types. Collaborative auditing frameworks designed to be cross-platform compatible, enabling seamless cooperation between diverse entities in the auditing process.

- **Regulatory Compliance**:

Osmotic computing environments often operate in regulated sectors where compliance with industry and legal standards is essential. Collaborative auditing facilitates the verification of compliance across the distributed system, ensuring that all nodes adhere to the relevant regulations and standards.

- **Decentralized Security Controls**:

Collaborative auditing allows for the implementation of decentralized security controls. Instead of relying on a single point of control, multiple entities can contribute to the enforcement of security measures, making it more robust and adaptable to the dynamic nature of osmotic computing.

Challenges

- **Dynamic and Decentralized Nature**:

In osmotic computing, systems are dynamic and decentralized, with resources and components constantly changing and adapting. This makes it challenging to establish a stable auditing framework, as traditional auditing methods may struggle to keep up with the dynamic nature of the environment.

- **Security and Trust**:

Ensuring the security and trustworthiness of collaborative auditing processes is crucial. Entities participating in the audit need to trust each other, and mechanisms must be in place to prevent malicious actors from compromising the audit or providing false information.

- **Data Privacy and Confidentiality:**

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

Collaborative auditing involves the exchange of sensitive information among multiple entities. Maintaining data privacy and confidentiality is a significant challenge, as information shared during the auditing process may include sensitive configurations, logs, or other data.

- **Interoperability:**

  Osmotic computing environments often involve heterogeneous systems and technologies. Ensuring interoperability between different components and systems during the auditing process can be complex, especially when there are variations in communication protocols and data formats.

- **Scalability:**

  The scalability of collaborative auditing becomes crucial, as osmotic computing environments can be highly scalable themselves. Auditing mechanisms need to scale seamlessly with the growth of the system, ensuring that the audit remains effective and efficient even as the environment expands.

- **Consistency and Synchronization**:

  Maintaining consistency and synchronization across distributed components is a challenge in osmotic computing. Audit results and logs need synchronized to provide an accurate representation of the system's state, and ensuring this consistency in a dynamic and decentralized environment is not trivial.

- **Resource Constraints**:

  Osmotic computing environments may have resource-constrained devices or nodes. Collaborative auditing mechanisms designed to operate efficiently within these resource limitations, ensuring that the auditing process does not adversely result in the overall performance of the system.

- **Adaptability to Change:**

  Osmotic computing environments designed to adapt to changing conditions. Collaborative auditing mechanisms should be able to adapt to changes in the environment, such as the addition or removal of nodes, without compromising the overall audit process.

Addressing these challenges requires innovative solutions and a deep understanding of the specific characteristics of osmotic computing environments. Implementing robust security measures, designing flexible and scalable auditing protocols, and leveraging technologies such as blockchain for transparency and trust are

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

some potential strategies to overcome these challenges. Additionally, ongoing research and development in the field will likely contribute to the evolution of effective collaborative auditing solutions for osmotic computing.

XI. FINDINGS

- **Improved scalability:** Osmotic computing allows for the seamless integration of multiple computing resources, which can significantly improve the scalability of collaborative auditing processes. This means that auditors can easily access and analyze large volumes of data from various sources, without limited by the capacity of a single computing resource.
- **Enhanced data processing capabilities**: Osmotic computing enables auditors to leverage the combined processing power of multiple computing resources, leading to improved data processing capabilities. This allows for faster and more efficient analysis of audit data, leading to more timely and accurate audit findings.
- **Enhanced data security:** By leveraging multiple computing resources, osmotic computing can enhance the security of audit data. For example, auditors can use Edge computing resources to process sensitive data locally, reducing the risk of data breaches and unauthorized access.
- **Improved collaboration:** Osmotic computing can facilitate better collaboration among auditors by providing a unified computing environment that allows for seamless sharing and analysis of audit data. This can lead to more effective communication and collaboration among audit teams, ultimately leading to better audit findings.
- **Cost savings**: By leveraging a combination of cloud, edge, and fog computing resources, osmotic computing can potentially lead to cost savings for organizations conducting collaborative audits. This is because organizations can optimize their use of computing resources, avoiding unnecessary expenses associated with over-provisioning or underutilization of resources.

XII. RECOMMENDATIONS

- **Clear Objectives and Scope**:

  - Define the specific objectives and scope of the collaborative auditing process within the osmotic computing context.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

- Clearly articulate the goals, such as ensuring security, trust, and compliance with regulations.

- **Dynamic Auditing Framework:**

  - Develop a flexible and dynamic auditing framework that can adapt to the dynamic nature of osmotic computing environments.

  - Account for the constant migration of services and data in an osmotic system.

- **Real-Time Monitoring**:

  - Implement real-time monitoring capabilities to detect and respond to security incidents promptly.

  - Utilize tools and mechanisms that allow continuous monitoring of the osmotic environment.

- **Decentralized Auditing Mechanisms**:

  - Design auditing mechanisms that are distributed and decentralized to align with the decentralized nature of osmotic computing.

  - Distribute audit logs and responsibilities across the network to avoid single points of failure.

- **Interoperability Standards:**

  - Establish interoperability standards for collaborative auditing to ensure seamless communication and data exchange between different components in the osmotic system.

  - Adhere to existing standards where applicable and propose new standards if necessary.

- **Trust Management:**

  - Implement trust management mechanisms to evaluate and establish trust levels among different entities in the osmotic computing environment.

  - Consider reputation systems or blockchain technology to enhance trust.

- **Privacy-Preserving Techniques:**

  - Incorporate privacy-preserving techniques to protect sensitive information during the auditing process.

  - Use encryption, anonymization, and other privacy-enhancing technologies.

- **Automated Auditing Processes:**

  - Integrate automated auditing processes to handle the scale and complexity of osmotic computing environments.

  - Utilize machine learning or artificial intelligence to identify anomalies and potential security threats.

- **Collaboration Mechanisms**:

  - Define clear collaboration mechanisms between different entities involved in the auditing process.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

- Foster communication and information sharing among components to enhance the effectiveness of collaborative auditing.

- **Scalability Considerations**:
  - Ensure that the auditing framework is scalable to accommodate the growth and expansion of osmotic computing environments.
  - Consider the impact of scalability on performance and resource utilization.
- **Incident Response and Remediation**:
  - Develop a robust incident response plan that outlines the steps taken in the event of a security breach.
  - Include mechanisms for quick remediation and recovery from security incidents.
- **Accountability User and Administrator:**
  - Incorporate mechanisms to establish accountability among users and administrators in the osmotic computing environment.
  - Clearly define roles and responsibilities to ensure proper oversight.

Continuous Improvement:

- Establish a feedback loop for continuous improvement of the collaborative auditing framework.
- Learn from security incidents and adapt the auditing mechanisms accordingly.

- **Education and Training:**
  - Provide education and training for users, administrators, and auditors to enhance awareness of security best practices within osmotic computing.

By incorporating these suggestions, you can develop an effective collaborative auditing framework that addresses the unique challenges of osmotic computing environments while promoting security, trust, and compliance.

XIII. FUTURE RESEARCH

- **Security and Auditing Mechanisms**: Exploring the security of auditing mechanisms for secure cloud storage in the context of osmotic computing. This could involve developing innovative approaches to ensure the security and integrity of data in osmotic computing environments.
- **Machine Learning and Algorithms**: Investigating new computing approaches for implementing machine learning algorithms and other useful algorithms in Industrial Internet of Things (IIoT) to prevent costs associated with having to

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

install state-of-the-art edge analytic devices. This may include collaborative edge computing and could provide insights into the auditing requirements for such collaborative environments.

- **Distributed Multi-Agent Systems:** Exploring osmotic computing as a distributed multi-agent system, particularly in the context of the latest technological advancements that have changed the centralized Cloud Computing model, going through Edge and Internet of Things (IoT). This could involve studying the implications of distributed multi-agent systems on auditing mechanisms in osmotic computing.

- **Smart Orchestration Architecture:** Investigating smart orchestration architectures for enabling osmotic computing from the cloud to edge and IoT. This could involve studying the implications of smart orchestration on auditing processes in osmotic computing environments.
- **Handling Security-Critical and Latency-Sensitive Data:** Exploring osmotic computing in association with related computing paradigms (cloud, fog, and edge) as a promising solution for handling security-critical as well as latency-sensitive data generated by digital devices. This could involve researching the auditing requirements for handling such data in osmotic computing environments.

XIV. CONCLUSION

In conclusion, the application of osmotic computing in collaborative auditing environments offers a range of significant benefits. By seamlessly integrating multiple computing resources, osmotic computing enhances the scalability, data processing capabilities, security, collaboration, and potential cost savings of collaborative auditing processes. This results in more efficient and effective audit findings, ultimately improving the overall quality and reliability of audit outcomes. As organizations continue to embrace digital transformation and seek innovative solutions for their auditing needs, osmotic computing presents a promising approach to optimizing collaborative auditing processes in a rapidly evolving digital landscape.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 02, 138-166
DOI: https://doi.org/10.59231/SARI7693

REFERENCES

1. Osmotic Computing Laboratory. https://osmotic.org/osmotic-computing-principles/
2. ACM Digital Library. https://dl.acm.org/doi/10.1145/3488247
3. *Auditboard*. https://www.auditboard.com/blog/collaborative-audit-culture/
4. Institute of Electrical and Electronics Engineers. Xplore. https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=osmotic%20computing
5. A publication of ThellA.org – Internal auditor. https://internalauditor.theiia.org/en/voices/2023/building-a-better-auditor-transparent-and-collaborative-auditing/#content
6. Ganapathy, V. (2024). Recent advances and applications of deep learning (DL) in the accounting profession. *Edumania-An International Multidisciplinary Journal*, *02*(1), 77–104. https://doi.org/10.59231/edumania/9020
7. Ganapathy, V. (2023). AI in auditing: A comprehensive review of applications, benefits and challenges. *Shodh Sari-An International Multidisciplinary Journal*, *02*(4), 328–343. https://doi.org/10.59231/SARI7643

Received on Jan 08, 2024
Accepted on Feb 18, 2024
Published on April 01, 2024