USER-CENTRIC PRIVACY CONTROL IN IDENTITY MANAGEMENT AND ACCESS CONTROL WITHIN CLOUD-BASED SYSTEMS

Kelvin Ovabor and Travis Atkison

Department of Computer Science, University of Alabama, USA

ABSTRACT

The ability to effectively implement user-centric privacy controls in cloud-based identity access management (IAM) systems is crucial in today's age of rapidly rising data and increased privacy concerns. The study tackles the scalability issue inside cloud-based IAM systems, where user-centric privacy controls are paramount. The study aims to guarantee effective system performance despite growing numbers of users and data items by following a carefully crafted approach that uses user-centric privacy algorithms. The findings are expected to increase scalability while maintaining security and user privacy, significantly improving current cloud security and IAM techniques. This study provides significant findings for businesses adapting to the changing environment of cloud-based access and identity management, enhancing the security and privacy aspects of the online environment.

KEYWORDS

Cloud-based System, Identity Management, Access Control, Security, user-centric privacy

1. INTRODUCTION

Adopting and using technology has helped organizations achieve better storage solutions, improved data security, and enhanced customer experience. This involves using cloud-based systems for data security and storage. Cloud-based systems offer flexible and highly dependable data backups, aiding recovery after disaster strikes and enhancing business continuity [1]. Cloud-based systems have also allowed organizations to maintain flexibility, scale up, and focus their operations for enhanced profits.

As cloud systems become popular and commonly used by businesses, data privacy and protection discussions have become overly crucial [2]. In the adoption of cloud technologies, security is a critical issue. Reviewing the literature on security and privacy in cloud computing established that there are different security flaws [3]. The researchers demonstrated the need for research to address the need for more flexibility and issues with the current approaches used to mitigate privacy and security threats in cloud computing. In prior research, there were three security constructs in the cloud environment: identity, transformation, and infrastructure.

Incorporating private enhancing technologies (PETs) into IAM systems in cloud computing environments has received little attention in studies and practical applications, given the growing importance placed on user-focused privacy management. Current privacy patterns emphasize the significance of Privacy Enhancing Technologies in protecting identifiable data. However, there needs to be more comprehensive knowledge regarding integrating these innovations into IAM

remedies. This integration aims to improve user-focused control over privacy while ensuring accessibility, adaptability, and conformity to developing privacy laws.

2. RELATED WORKS

This section will consider the related works in the field of privacy in identity management and access control within cloud-based Systems with emphasis on the current state of the art. This will enable the researcher to acknowledge the gaps in previous research works.

2.1. Identity Management and Access control

Cloud computing provides on-demand storage and computing capabilities to consumers using technology. However, the benefits may pose significant security threats concerning data and computational breaches [4]. Therefore, to improve the security assurances of cloud systems, cloud providers must ensure that cloud customers can trust their systems.

In cloud systems, identity management includes managing people's identities, authentication, authorization, roles, privileges, and permission across and within systems to enhance productivity and increase security while reducing operational costs [5]. Thus, the capabilities of cloud-based systems are based on their ability to ensure and maintain individual identities. An organization can use a private cloud for its businesses, increasing its operations' security and trustworthiness, as illustrated in Figure 1.

Enterprise P can opt to employ either the on-premises private cloud or the externally hosted private cloud.

Private clouds refer to distributed networks that operate on privately owned architecture that allow customers to allocate computer resources dynamically. Alternative approaches to the pay-as-you-go framework inside private cloud environments may exist, whereby the use of cloud resources is effectively regulated, and the corresponding invoicing is allocated proportionately among several departments or divisions within a business. Therefore, Enterprise P would benefit from the use of a private cloud in that their sensitive data would only be utilized within their systems. In the context of private cloud environments, security risks are mitigated due to the absence of files and confidential data transfer outside the confines of the private network.
Digital identity management is crucial in fostering accountability, customizing user experience, and complying with regulations on technological applications. Different approaches have been developed to ensure privacy and control access to cloud-based systems. The critical elements of cloud security are federated identity, third-party authentication services, and end-to-end identity management. The confidentiality and integrity of the cloud applications and confidentiality of the data are achieved through identity security, which ensures that the cloud-based systems are only available to appropriate users [7].

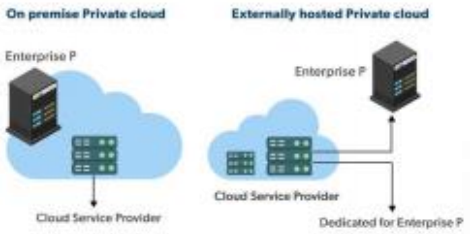

Figure 1. Private Window[6]

2.2. Strategy for Identity Management and Access Control

The current state of the art strategies in addressing the problems associated with privacy in identity management and access control include:

2.2.1. Strong Authentication and Access Control

Strong authentication may also be achieved through multi-factor authentication, two-factor authentication, biometric logins, and one-time passwords, which provide both controlled access and identity privacy for cloud-based systems [8]

2.2.2. Controlled Access to Cloud-based systems

In the mandatory access control, access to technological systems and cloud storage is based on the persons' level of clearance and labels. One study surveyed access control mechanism for cloud computing, noting that uncontrolled access to cloud storage increased the risks of data loss and outing of users [9]. The researchers noted that mandatory controlled access to cloud storage fostered confidentiality, anonymity, and integrity of the system and restricted user actions, unauthorized access, and information changes in the cloud systems.

2.2.3. Blockchain-based Identity Management Systems

Blockchain technology has also enhanced the security of data and individual identity in cloud-based systems. Those who examined a blockchain-based framework for electronic medical records coupled with fine-grained access control reported similar conclusions. The results indicated that fine-grained access control, Ethereum blockchain, and attribute-based encryption resulted in a secure and efficient cloud storage system for medical records [10]. Those who reported that chain code used in intelligent contracts fostered attribute-based access control, ensuring data was accessible to individuals with the right attributes, drew comparable conclusions. Moreover, the K-anonymity and searchable encryption protected the data from leaking.

2.2.4. Steganography

Steganography is a time-honored method that entails the covert embedding of one data set inside a different one, presenting a formidable obstacle for unknown entities to discern the hidden data. Inside data security, steganography is used to conceal sensitive data inside apparently benign files or media clandestinely [11].

2.2.5. Data Splitting

Data splitting entails partitioning confidential information into several shards and dispersing it across various places or systems. Individually, isolated data points lack significant informational value; nevertheless, their integration enables the reconstruction of the original dataset. This approach effectively increases privacy by mitigating the potential risks of just one breakdown point [12]

For example, if an organization wants to perform a Secure Function Evaluation for a function 'F' of their shares while maintaining privacy to hide the shares variables, these can be represented as;

$$F(x_1, x_2, x_3 \ldots x_n) = y \qquad (1)$$

Where by

$x_1, x_2, x_3 \ldots x_n$ represent parties' inputs.

Y represents the result of the Function F

2.2.6. Homomorphic Encryption

Homomorphic encryption is a robust cryptographic methodology that enables the execution of calculations on encrypted information without necessitating the process of decoding. This implies that the data maintains its protected state throughout the processing phase, ensuring the preservation of its secrecy. Homomorphic encryption plays a crucial role when safeguarding the confidentiality of information is of utmost importance, such as in the domains of medical research and financial evaluation [13]. The primary objective of this mechanism is to guarantee that confidential data remains secure and is never disclosed in its original, unencrypted form, even throughout the execution of intricate computational operations.

2.2.7. Signcryption

Signcryption is a cryptographic technique that integrates the functionalities of encrypted digital signatures within a unified process. The technology offers a combination of reliability of information and secrecy, hence streamlining the safe transmission and verification of data. Signcryption is advantageous in safe interaction standards since it enables concurrent authentication and encryption of communications [14]. Signcryption can improve performance and decrease computing expenses by minimizing the cryptographic procedures needed.

2.2.8. Machine Learning Algorithms in Cloud-based Systems

Machine learning algorithms have also improved privacy in identity management and access control within cloud-based systems. A survey of machine learning and non-machine learning techniques used to achieve cloud security was conducted [15]. Controlled access to systems in the cloud and effective detection of cyberattacks have been achieved via machine learning methods such as SVM (Support Vector Machines), choice trees, randomized forests, naive Bayes, AI-integrated neural networks, and algorithmic genetics. .

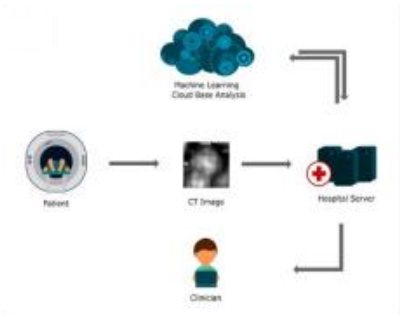

Figure 2. Illustration of machine learning cloud-based system [16]

The sophistication and advanced cyberattacks on cloud-based systems have influenced research on how machine-learning algorithms have been adopted to enhance privacy in access control and identity management in cloud-based systems, as seen in Figure 2.

2.2. Gaps in Literature

Several obstacles and restrictions accompany the integration of PETs into IAM systems. A notable constraint arises from the possible trade-off between safety and convenience. Numerous extant user-centric privacy-enhancing technologies exhibit intricacies that possess the potential to perplex end-users and impede widespread acceptance. Further investigation is required to further the development of user-centric privacy-enhancing technologies that include easy-to-use interfaces. Many existing methodologies need to improve in providing full resolutions for achieving interoperability. Incorporating different user-centric Privacy Enhancing Technologies into a range of Identity and Access Management contexts, such as cloud-based platforms and legacy applications, continues to provide a multifaceted and intricate obstacle. There is a significant need for improvement in the education provided to users and IAM administrators on the advantages and appropriate use of user-centric PETs.

In cloud-based IAM systems, scalability is a critical challenge for user-centered privacy management. The number of users and information items may increase rapidly as businesses develop. A system's agility and security might be jeopardized by delays in performance caused by unaddressed scaling difficulties. Confirming that the suggested approach can effectively handle many users and data items is crucial. Scalability is essential for addressing growth and changing user privacy demands in contemporary businesses. It not only ensures uninterrupted operation but also considers the dynamic character of these entities. Scalability issues must be addressed for user-centric privacy restrictions in cloud-based IAM systems to be successful and relevant in the long run.

Most of the current strategies did not consider users having a role to play in the management of their privacy and identity access control in a cloud environment.

According to GDPR, users have the ability to determine how their data is shared by individuals or services that collect their data. Therefore, there will be a need to implement a robust user-centric privacy control mechanisms in cloud-based IAM systems, which can help to mitigate unauthorized access and data breaches. This will involve development of an algorithm and system that allows users to have fine-grained control over their data, specifying who can access it and under what conditions. It will be considered in the aspect of scalability to accept many users and solve complexity issues

3. METHODOLOGY

This section gives an overview of the methodology in this research. It involves series of steps at different stages of its implementation.

3.1. Data Collection

The assessment of scalability in user-centered privacy controls in a cloud-based IAM system relies heavily on gathering data as a core feature. This multi-step procedure will use many methods to guarantee accurate data collection. Users will willingly provide their identifying information via a User Registration Form in the first registration stage. Secure enrollment of users and data gathering will be easier with the help of AWS Cognito. Users will be instructed on how to set up their privacy settings in Azure Active Directory, including defining who has access to what kinds of data. As the foundation of the system's user-centric security procedures, thorough audit logs will be created for each event of access to data objects. The audit logs will use ELK Stack to efficiently record and examine access activity. The study will need to gather

data such as user IDs, policy settings, and audit logs to gauge the system's scalability in the face of rising numbers of users, regulations, and login events. With this data-driven strategy, the IAM system will be able to effectively meet the changing privacy requirements of its users without compromising on security or responsiveness.

As illustrated in Figure 3, survey and interview are two major ways of collecting user data. The user consent must be sought before the data can be used while extracted data is securely stored for future use. Data analysis will be performed on the collected data to identify trends and patterns.

3.2. Data Processing

The suggested approach relies heavily on data cleaning and modification to guarantee the quality and applicability of the information gathered. The research will utilize the pandas package in Python to clean up the data and fix faults like missing values, anomalies, and inconsistent data. This application provides a versatile and powerful setting for data cleansing tasks. The scikit-learn module in Python will be used to do feature design and data standardization. To ensure that data is adequately prepared for analysis, Scikit-learn offers various tools for doing so. The data processing step will be simplified using these technologies, yielding higher-quality information suitable for additional evaluation.

Figure 4 illustrates all stages involved for the preprocessing of the data. This will include Data Cleansing, and Extraction among others. At this stage, you collect raw IAM system logs from the data repository where they are stored.

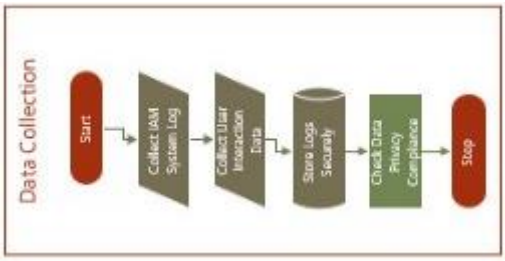

Figure 3. Flowchart diagram for data collection

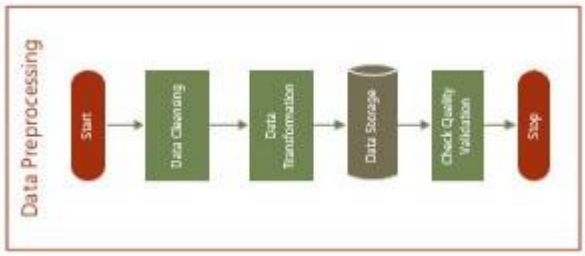

Figure 4. Flowchart of data preprocessing

By following these steps, we must have prepared the IAM system logs for analysis, ensuring that the data is clean, structured, and ready for use in the User-Centered Privacy Control Algorithm (UCPCA) and other components of your cloud-based IAM system.

There would be need to conduct data quality validation checks after preprocessing to confirm that the dataset is ready for analysis and verify that the dataset meets the requirements of the UCPCA algorithm and IAM system.

3.3. Data Classification

Data categorization is essential in closing the scalability gap, as it involves carefully sorting collected data across numerous identification levels. Segmentation and methodical classification will effectively classify user identities concerning established roles and traits. These algorithms will be executed in Python's sci-kit-learn module and are coupled with Apache Nutch to analyze user identities, structured data, and access control rules. At the same time, Apache NiFi will be used to classify data according to how sensitive or essential each piece is after thoroughly examining the access control policies, who is allowed access to what kind of data, and when it is determined. Following user-centric privacy requirements, this granular categorization will pave the way for implementing exact access controls.

3.4. Data Utilization

Data utilization is crucial in Evaluating the scalability of a user-centered cloud-based IA system. Users can create granular access control restrictions, improving the security of sensitive information.

Access Control Lists (ACLs) in the HashiCorp Vault will be constructed using these rules as their basis. Access control lists (ACLs) determine who may see what in a database. Further, Microsoft Azure Active Directory will establish Role-Based Access Control (RBAC), allowing users to be placed into preset roles with specific permissions. Axiomatics enables Attribute-Based Access Control (ABAC), which automatically assigns permissions to data items based on attributes such as users' roles, departments, and geographical locations. These access controls will be easily implemented and enforced using Python and the PyCryptodome package.

3.5. Algorithm Development

This is the development of the User-Centered Privacy Control Algorithm (UCPCA) as shown in Figure 5. It also emphasizes the four subcategories under the algorithm design as further illustrated by Figure 5. Its implementation would include the following steps. It starts with Policy Specification and User Interface. This is with regard to the Domain-Specific Language (DSL) Design. You design a user-friendly DSL that allows users to express access policies in a natural and intuitive way. The DSL should support specifying who can access data, under what conditions, and for what purposes. Create an intuitive user interface within the IAM system's dashboard for users to define and manage their access policies. This will include features like policy templates, rule builders, and policy versioning for ease of use.

Regarding Access Request Processing, it will involve developing a module within the IAM system responsible for processing access requests and enforcing access policies. Ensure that access requests are authenticated and authorization decisions are made based on the defined policies. Implement a rule-based evaluation engine that can interpret policies expressed in the DSL. Evaluate access requests against these policies to determine if access should be granted or denied.

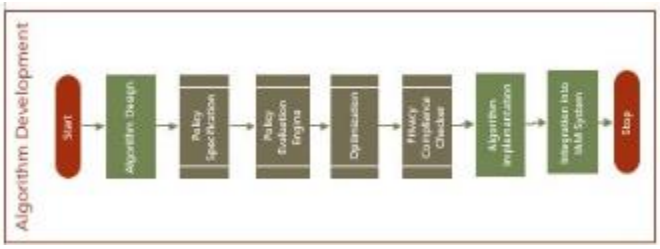

Figure 5. Algorithm development

In term of Logging and Auditing, there will be need to Implement comprehensive logging and auditing capabilities within the policy evaluation engine. This will include Log access requests, policy decisions, and any relevant events for compliance and auditing purposes.

For Optimization and Resource Management, we need to implement optimizations to address scalability issues that may arise when evaluating policies for a large number of users and data objects. Techniques such as caching, parallel processing, and load balancing can be used to improve performance. Monitor system resource utilization and allocate resources efficiently to ensure optimal policy evaluation. Implement resource management strategies to prevent resource bottlenecks.

Choose the appropriate technology stack for the IAM system, considering the cloud platform (e.g., AWS, Azure, Google Cloud) and programming languages (e.g., Python, Java, Node.js.

3.6. UCPCA Algorithm Integration

After developing the UCPCA algorithm, there will be need to incorporate fine-grained user-centric privacy controls. Ensure that the algorithm can handle policy specification, evaluation, and optimization. Integrate the UCPCA algorithm into the IAM system architecture, specifically into the policy management and access control components. For the User Dashboard and Administrator Console, design a user-friendly dashboard where users can manage their access policies and privacy settings. Implement a clear and intuitive interface for users to specify who can access their data and under what conditions. Create an administrator console for system administrators to manage user accounts, roles, and system-wide policies.

There would be need to Implement secure user authentication mechanisms, such as multi-factor authentication (MFA) and single sign-on (SSO), to ensure user identity verification. Then develop an authorization module that evaluates access requests against user-defined policies and UCPCA algorithm rules. For Data Encryption and Access Controls, implement data encryption at rest and in transit to protect sensitive user data and policies. Apply strict access controls to the IAM system components to prevent unauthorized access.

At this stage there would be need for Compliance Checks and Audit Logging: Therefore, implement automated compliance checks to ensure that user-defined policies comply with relevant privacy regulations and standards (e.g., GDPR, HIPAA). Create detailed audit logs of system activities, including policy changes, access requests, and user interactions, for compliance and security audits.

3.7. Integration with Microsoft Azure

Everything needed for a smooth integration with Microsoft Azure is outlined as shown in Figure 7. Set Up a Microsoft Azure Account and create a new Azure subscription or use an existing one

for your IAM system project. Define the Azure resources you'll need for your IAM system, including virtual machines, databases, and storage accounts. Set up a Virtual Network (VNet) to isolate and secure your IAM system resources. Implement Azure Active Directory (Azure AD) for user authentication and identity management.

Set Up a Microsoft Azure Account and create a new Azure subscription or use an existing one for your IAM system project. Define the Azure resources you'll need for your IAM system, including virtual machines, databases, and storage accounts. Set up a Virtual Network (VNet) to isolate and secure your IAM system resources. Implement Azure Active Directory (Azure AD) for user authentication and identity management.This can be followed by Testing and Quality Assurance which could be unit testing, integration testing, and user acceptance testing, to validate the integration of UCPCA into the IAM system on Azure. Address any issues or bugs that arise during testing.

Then Deploy the integrated IAM system with UCPCA on Azure, considering scalability and high availability. There would be a need for documentation and training to Provide user documentation and training materials for your IAM system, explaining how to use the UCPCA features within the Azure environment. Train administrators on how to manage the IAM system effectively on Azure.

There would be need for oongoing Maintenance and updates. Therefore, establish a maintenance plan for regular updates, security patches, and bug fixes. Continuously monitor the IAM system's performance, security, and compliance with Azure-specific requirements. Also, conduct regular compliance audits to ensure that the IAM system, including UCPCA, complies with Azure-specific privacy regulations and security standards.

3.8. Evaluation for Scalability

The scalability testing to assess system performance will include the following steps:
Test Data Generation: Create test scenarios with varying numbers of users, data objects, and access requests to simulate real-world usage. Performance Metrics: Define key performance metrics, such as response time, throughput, and resource utilization. Load Testing: Use load testing tools to subject the system to increasing loads and monitor its performance under stress. Scalability Analysis: Analyze the system's performance metrics as the load increases to identify bottlenecks or performance degradation. Load Balancing: Implement load balancing techniques to distribute traffic evenly among system components, improving responsiveness and scalability. Distributed Computing: Utilize distributed computing techniques such as parallel processing, microservices, or serverless computing to handle increased loads efficiently. Auto-Scaling: Configure auto-scaling mechanisms to automatically adjust resources based on demand, ensuring optimal performance during traffic spikes.

One of the ways to ascertain the effectiveness of the solution is through usability testing as shown in Figure 6. This involves the User Acceptance Testing (UAT) with the following steps:

- Test Scenario Design:
- User Recruitment:
- Usability Testing Sessions:
- Observation and Feedback:
- Task Completion Metrics:
- Analysis of Usability Findings: Analyze the usability test results to identify pain points, challenges, and areas for improvement.

- Iterative Design.
- Usability Testing Cycles

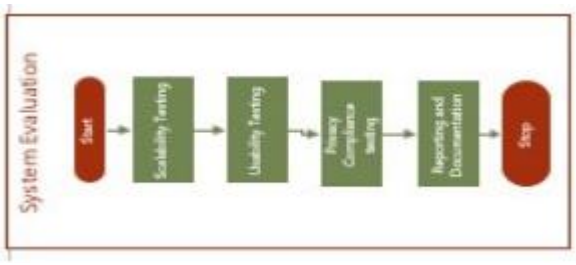

Figure 6. System evaluation

Figure 6 outlines all that is needed for proper evaluation of the solution and its associated components. This involves evaluating the cloud-based IAM system, including the User-Centered Privacy Control Algorithm (UCPCA), which is essential to ensure its effectiveness, usability, and compliance; this will also include scalability testing

By following these steps, we will be able to thoroughly evaluate our cloud-based IAM system, address scalability issues, enhance usability, and ensure compliance with privacy regulations.
The study will generate fake user inquiries or inputs of information that replicate genuine user actions to undertake scaling assessment. Using AWS Cognito, the study will monitor the system's CPU load, storage use, network throughput, and lag times. The study will locate locations where performance could decrease as the workload grows. Loading balancing distributes incoming traffic evenly across numerous servers, which will help avoid bottlenecks and improve speed and fault tolerance. Distributed computing decomposes monolithic elements into smaller, more manageable pieces called microservices, which will be scaled independently to meet fluctuating demand. When using horizontal scaling, more servers from Azure will be added as required to facilitate growth and increase reliability. Cloud vendors often provide solutions that enable dynamic scaling in response to changes in traffic, facilitated by auto-scaling rules that automate capacity modifications based on established limits or events. The study will use sharding, partitioning, and replication for scalable and efficient data storage. This will ensure the system can manage growing user demand and data expansion while maintaining optimum performance and reliability by testing scalability and applying optimization measures like load distribution and distributed computation. Since cloud-based systems' assets may be constantly modified to match fluctuating demands, this is especially crucial in such environments.

The equations are:

1) Access Control Equation:

This equation depicts whether a user has access to a specified data object while considering data object permissions and user identity as the primary variables.
Access = (User Identity and data object permissions) * (All conditions are met)
Where user identity specifies the identity of the user, data object permissions define the permission to access the data.

2) Policy Evaluation Equation:

This equation evaluates the compliance with user policies by assessing the data object permissions and user-identity policies.
Compliant = (user_Identified policies and object permissions met) * (All other conditions met)

These equations are essential to the workability of the algorithm, and Python is used to ensure data access within IAM systems. These equations are central to the Access Control Algorithm and Policy Evaluation Algorithm discussed in the proposed methodology. They are implemented in Python to enable fine-grained user-centric privacy controls and ensure secure data access within the IAM system.

4. RESULT

Several vital results that align with bridging the scalability gap in cloud-based IAM systems are expected to emerge from the suggested methodology driven by user-centric privacy restrictions. It is anticipated that a significant improvement in user privacy would result from allowing users to establish granular access limitations and privacy rules. Thanks to this autonomy, users' confidence in the IAM system is bolstered as their data is handled in line with their wishes. The strategy employs granular access restrictions and continual tracking of accessibility to data to cut down on unwanted access events. Consequently, the study expects fewer security incidents associated with data breaches and unlawful data access, which will enhance the IAM platform's security in general. The technique is expected to improve compliance by classifying data, classifying users, and strictly enforcing access control restrictions. This involves following laws like the GDPR, HIPAA, and the CCPA (California's Consumer Privacy Act) that protect individuals' personal information.

Adherence to these rules calls for stringent safeguards for user information and openness about how it is used, which is essential to user-centric privacy controls. It is anticipated that the general protection of the IAM framework will be improved by incorporating protection procedures that emphasize user needs, the application of machine learning methods, and the use of Python for regulatory purposes. With these resources, the system will be more flexible in the face of shifting access requirements and more secure overall. One of the main goals of the suggested approach is to reduce the scalability gap. This technique is meant to keep the IAM system performing highly regardless of the number of users, access rules, and information events. The system's scalability will be apparent in its increased capacity to deal with many users and varied access patterns without sacrificing data integrity or individual privacy. The hoped-for outcomes improve user trust in the IAM system and boost faith in the system at the managerial level. Confidence may grow when users are more informed about how their data is used and how to protect it. The IAM platform will be trusted and reliable due to decreased security risks, greater adherence to legal requirements, and superior data protection.

5. FUTURE WORKS

The user-focused privacy control mechanism in cloud-based IAM and future improvements and advancements are described. These upgrades are intended to boost user control and information protection significantly.

5.1. Enabling Fine-Grained Data Accessibility

The system may be improved later to provide even finer control over data access. Clients may be allowed to control access even to specific data items inside the file or dataset. Users may determine precisely who has access to what data using fine-grained restrictions, adding extra security.

5.2. Configuring a user-friendly policy

Future work might develop user-friendly and straightforward platforms for policy setup to improve customer service and promote higher adoption. The process of setting access rules may be made simpler by using optimized administration of policy solutions with assisted interfaces and representations, opening it up to a larger audience of users.

5.3. Integration with Advanced Privacy technology:

The framework may collaborate with innovative security-preserving technology to stay up with changing privacy issues and laws. Improved algorithms for encryption, sophisticated confidentiality procedures, or blockchain-based approaches to improve data openness and provenance may fall under this category.

5.4. Improved Reporting and Monitoring

Enhancing ongoing tracking and auditing of login operations can provide administrators and users with immediate information on data access trends. More advanced monitoring and notification methods may be added to quickly recognize and react to suspicious actions or possible compromises.

5.5. Optimization for Scalability and Performance:

As the system expands, scalability and efficiency must be continuously improved. Performing stress tests is part of this to make sure it can withstand rising user and information quantities without losing effectiveness.

5.6. Compliance with Emerging Legislation:

Given the constantly changing nature of privacy legislation, ongoing measures should be taken to guarantee that the framework complies with growing regulations regarding data protection, including GDPR, CCPA, or equivalent local standards.

6. CONCLUSION

This proposed work outlines a comprehensive methodology to address the absence of user-centric privacy control mechanisms in cloud-based IAM systems. The methodology encompasses data collection, algorithm development, system implementation, and evaluation, with a focus on scalability, complexity, compliance, and usability. By addressing these challenges, the proposed system aims to enhance data privacy and access control in cloud environments, ultimately mitigating unauthorized access and data breaches

REFERENCES

[1] Haleem A, Javaid M, Singh RP, Rab S, Suman R. Hyperautomation for the enhancement of automation in industries. Sens Int 2021;2:100124. https://doi.org/10.1016/j.sintl.2021.100124.

[2] Hassan J, Shehzad D, Habib U, Aftab MU, Ahmad M, Kuleev R, et al. The rise of cloud computing: data protection, privacy, and open research challenges—a systematic literature review (SLR). Comput Intell Neurosci 2022;2022. https://doi.org/10.1155/2022/8303504.

[3] Kumar R, Singh K, Jain SK. An empirical investigation of the relationship among agile manufacturing practices and business performance: A pilot study. J Sci Technol Policy Manag 2022;13:428–55. https://doi.org/10.1108/jstpm-01-2020-0009.

[4] Abdulsalam YS, Hedabou M. Security and privacy in cloud computing: technical review. Future Internet 2021;14:11. https://doi.org/10.3390/fi14010011.

[5] Rak J, Girao-Silva R, Gomes T, Ellinas G, Kantarci B, Tornatore M. Disaster resilience of optical networks: State of the art, challenges, and opportunities. Opt Switch Netw 2021;42:100619. https://doi.org/10.1016/j.osn.2021.100619.

[6] SarthakGarg. Types of Cloud. GeeksforGeeks 2018. https://www.geeksforgeeks.org/types-of-cloud/ (accessed September 15, 2023).

[7] Achar S. Cloud-based System Design. Int J Res Educ Sci Methods IJARESM 2019;7:23–30.

[8] Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digital technologies: tensions in privacy and data. J Acad Mark Sci 2022;50:1299–323. https://doi.org/10.1007/s11747-022-00845-y.

[9] Takabi H, GhasemiGol M. Introduction to the cloud and fundamental security and privacy issues of the cloud. Secur Priv Digit Forensics Cloud 2019:1–22. https://doi.org/10.1002/9781119053385.ch1.

[10] Acharya UR, Meiburger KM, Koh JEW, Vicnesh J, Ciaccio EJ, Lih OS, et al. Automated plaque classification using computed tomography angiography and Gabor transformations. Artif Intell Med 2019;100:101724. https://doi.org/10.1016/j.artmed.2019.101724.

[11] Istiaque Ahmed K, Tahir M, Hadi Habaebi M, Lun Lau S, Ahad A. Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction. Sensors 2021;21:5122. https://doi.org/10.3390/s21155122.

[12] Li H, Yang Y, Dai Y, Yu S, Xiang Y. Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data. IEEE Trans Cloud Comput 2017;8:484–94. https://doi.org/10.1109/tcc.2017.2769645.

[13] Sohrabi N, Yi X, Tari Z, Khalil I. BACC: Blockchain-based access control for cloud data. Proc. Australas. Comput. Sci. Week Multiconference, 2020, p. 1–10. https://doi.org/10.1145/3373017.3373027.

[14] Rana A, Reddy A, Shrivastava A, Verma D, Ansari MS, Singh D. Secure and Smart Healthcare System using IoT and Deep Learning Models. 2022 2nd Int. Conf. Technol. Adv. Comput. Sci. ICTACS, IEEE; 2022, p. 915–22. https://doi.org/10.1109/ictacs56270.2022.9988676.

[15] AlBadi A, Hajamohideen F, AlSaqri D. A Review on Blockchain Techniques Used for Identity Management System: Privacy and Access Control. Int. Conf. Syst. Eng., Springer; 2023, p. 361–75. https://doi.org/10.1007/978-3-031-40579-2_35.

[16] Mamdouh M, Awad AI, Khalaf AA, Hamed HF. Authentication and identity management of IoHT devices: achievements, challenges, and future directions. Comput Secur 2021;111:102491. https://doi.org/10.1016/j.cose.2021.102491.

AUTHORS

Kelvin Ovabor is a PhD candidate at the University of Alabama, USA and is advised by Travis Atkison, an Associate Professor of Computer Science, the Computer Science Cyber Security Program Director, and director of the Digital Forensics and Control Systems Security Lab (DCSL). Kelvin's research focuses on use of novel nature-inspired algorithms in solving security issues. Kelvin is also interested in health informatics in order to apply his expertise in information technology to address real life health issues, thereby appreciating how health and IT complement each other. He enjoys walking around cities, driving around the US, and watching movies.