FMDB *Transactions on Sustainable Computing Systems*

Secure Identity: A Comprehensive Approach to Identity and Access Management

K. Daniel Jasper[1,*], A. S. Vignesh Raja[2], R. Neha[3], S. Suman Rajest[4], R. Regin[5], Biswaranjan Senapati[6]

[1,2,3,5] Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[4]Department of Research and Development & International Student Affairs, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
[6]Department of Computer and Information Science, Parker Hannifin Corp., Illinois, United States of America.
dk9127@srmist.edu.in[1], ar6256@srmist.edu.in[2], rr2499@srmist.edu.in[3], sumanrajest414@gmail.com[4], regin12006@yahoo.co.in[5], bsenapati@ualr.edu[6]

Abstract: Identity and Access Management (IAM) system aimed at enhancing security, streamlining authentication processes, enforcing access controls, and monitoring user activities effectively. The system incorporates various security measures, including biometric identification, Challenge-Handshake Authentication Protocol (CHAP) authentication, Role-Based Access Control (RBAC), and User Behavior Analytics (UBA), to address key security challenges and fortify the organization's security posture. Biometric identification provides a highly secure and reliable method for authenticating users, leveraging unique physiological traits such as fingerprints or facial features. CHAP authentication introduces cryptographic mechanisms to verify user identities and prevent unauthorized access. RBAC facilitates granular access control, while UBA enhances threat detection capabilities and supports compliance efforts. Integrating these security measures has yielded tangible benefits, including improved authentication integrity, reduced risk of unauthorized access, enhanced threat detection, and better compliance adherence. By adopting a multi-layered approach to security and leveraging advanced technologies, the IAM system provides organizations with the tools to safeguard sensitive data and resources effectively. Ongoing investment in IAM technologies and practices will be crucial to adapting to evolving security threats and maintaining a secure IT environment. This aims to layer security principles so that data is safeguarded from threat actors and protected from data breaches, prevent insider threats from occurring, and implement security to a network and organization.

Keywords: Identity Access Management; Authentication and Authorization; Accounting Identification; Biometric Challenge; Handshake Authentication Protocol; Role-Based Access Control; User Behavioural Analytics.

Received on: 15/04/2023, **Revised on:** 11/08/2023, **Accepted on:** 02/10/2023, **Published on:** 20/12/2023

Cite as: K. Daniel Jasper, A. S. Vignesh Raja, R. Neha, S. Suman Rajest, R. Regin, B. Senapati, "Secure Identity: A Comprehensive Approach to Identity and Access Management," *FMDB Transactions on Sustainable Computing Systems*., vol. 1, no. 4, pp. 171–189, 2023.

1. Introduction

In today's interconnected and data-driven world, managing identities and resource access is paramount for organizations across various sectors. Identity and Access Management (IAM) encompasses the policies, processes, and technologies used to ensure appropriate access to systems, applications, and data while safeguarding against unauthorized use, data breaches, and compliance violations [16]. With the proliferation of cloud computing, mobile devices, and remote work, IAM has become increasingly complex and critical for maintaining security and regulatory compliance. IAM stands for Identity and Access

[*]Corresponding author.

Management [17]. It is a framework of policies, processes, and technologies that ensures appropriate access to resources in an organization while protecting those resources from unauthorized access. In simpler terms, IAM is all about managing who has access to what within a company's digital environment. This includes managing user identities, their authentication (verifying who they are), and authorization (determining what they can access) [18].

1.1. Identity Management

In the digital realm, identity is the foundation for establishing trust, enabling interactions, and facilitating access to resources. Digital identity encompasses a broad range of elements, including personal identifiers (such as usernames, email addresses, or employee IDs), biometric data (such as fingerprints or facial recognition), and cryptographic credentials (such as digital certificates or security tokens) [19]. These identifiers and attributes authenticate individuals, verify their identity, and authorize their access to digital services, applications, and data. Identity management involves the administration of these digital identities throughout their lifecycle, encompassing processes such as registration, authentication, authorization, and de-provisioning [20]. Effective identity management practices ensure digital identities' security, privacy, and integrity while enabling seamless and secure access to resources across diverse environments, including cloud-based services, mobile applications, and Internet-connected devices (Figure 1).

Figure 1: Identity Access Management [14]

1.2. Authentication

Authentication is verifying the identity of users or entities accessing the system. This typically involves providing credentials (e.g., username and password, biometric data, security tokens) to prove identity. IAM systems implement various authentication methods to ensure secure access based on the data's sensitivity and risk level [21]. The Challenge-Handshake Authentication Protocol (CHAP) is widely used in network communications, particularly in remote access scenarios such as dial-up connections and virtual private networks (VPNs). CHAP provides a secure method for verifying the identity of a user or device accessing a network without transmitting sensitive information over the network [22]. In CHAP, the authentication process begins with the server challenging the client to prove its identity. The server sends a random challenge string to the client, which combines this challenge with a secret shared password using a one-way hash function, typically MD5 or SHA-1 [23]. The client then sends the resulting hash back to the server. Upon receiving the response, the server independently computes the expected hash based on its copy of the shared password and the received challenge. If the computed hash matches the hash sent by the client, authentication succeeds, and the client is granted access to the network. One of the key advantages of CHAP is its resistance to replay attacks, as each authentication attempt involves a new challenge from the server [24]. Additionally, CHAP does not transmit passwords in plaintext, enhancing security [25].

1.3. Authorization

Authorization determines what authenticated users can do within the system once their identity has been verified. This involves defining access policies, roles, and permissions that specify which resources (such as files, applications, or databases) users can access and what actions they can perform (e.g., read, write, execute) [26]. Role-Based Access Control (RBAC) is a widely adopted authorization method in Identity and Access Management (IAM) systems, providing a structured approach to managing access permissions within organizations. In RBAC, access rights are assigned to roles rather than individual users, streamlining access management by grouping users with similar responsibilities or job functions [27]. Each role is associated with a set of permissions that define the actions users assigned to that role can perform within the system. Users are then assigned one or more roles based on their job roles or organizational hierarchy. RBAC simplifies access control administration, as access rights

can be managed at the role level rather than for each user, reducing complexity and ensuring consistency across the organization [28]. Since RBAC enforces the principle of least privilege, users are allowed only the permissions they need to do their jobs, reducing the danger of unwanted access [29]. RBAC enables scalability and flexibility, allowing companies to simply update access permissions as roles change or new roles are added. RBAC helps enforce access control policies, improve security, and meet regulatory requirements [30].

1.4. Accounting

Accounting serves as the vital monitoring mechanism for organizations, providing insight into financial health, performance, and compliance with regulatory standards [31]. Through systematic recording, analysis, and reporting of financial transactions, accounting enables organizations to track revenues, expenses, assets, and liabilities, facilitating informed decision-making by management, investors, and other stakeholders [32]. By monitoring financial metrics such as profitability, liquidity, and solvency, accounting enables organizations to assess their financial viability, identify areas for improvement, and formulate strategies for sustainable growth [33]. Moreover, accounting is a critical tool for monitoring compliance ensuring adherence to statutory regulations, industry standards, and internal policies. Accounting helps detect and prevent fraud, errors, and irregularities through financial audits, internal controls, and risk assessments, safeguarding organizational assets and reputation [34].

Furthermore, accounting facilitates performance monitoring by comparing actual financial results against budgeted targets and industry benchmarks, enabling organizations to evaluate operational efficiency and effectiveness [35]. Accounting is the cornerstone of organizational monitoring, providing stakeholders transparency, accountability, and confidence in financial affairs [36]. By leveraging accounting information effectively, organizations can navigate challenges, capitalize on opportunities, and achieve long-term success in today's dynamic business environment (Figure 2).

Figure 2: Authentication, Authorization, Accounting [15]

1.5. Identity Governance and Administration (IGA)

IGA involves managing the entire lifecycle of user identities and their access rights within an organization. This includes processes such as user provisioning (creating, modifying, or deleting user accounts), access certification (periodically reviewing and validating user access rights), and compliance reporting (ensuring adherence to regulatory requirements and internal policies) [37].

1.6. Data Encryption

Any successful IAM programme must protect data in transit and storage. Hackers can still access PPI even when compliance requirements prohibit transferring it across insecure networks or to unapproved entry/exit points. While some industries advocate or mandate data encryption during transmission, they do not address storage issues [38]. Even resistant data is vulnerable to attackers. Encrypting all PPI from handling to sending and receiving will greatly lower a company's cybersecurity risk, even with firewalls and other measures [39]. Identity and Access Management (IAM) systems need data encryption to safeguard sensitive data from illegal access and interception. Data is encrypted into ciphertext and unintelligible without the decryption key [40].

In IAM, data encryption is utilized to secure various aspects of identity management, including user credentials, authentication tokens, and access control policies [41]. For example, user passwords stored in IAM databases are typically encrypted using strong cryptographic algorithms to prevent unauthorized access in the event of a data breach. Additionally, communication channels between IAM components, such as authentication servers and user devices, are encrypted using protocols like SSL/TLS to prevent eavesdropping and data tampering [42]. Encryption also plays a crucial role in securing data at rest, ensuring that user attributes, access logs, and audit trails stored in IAM repositories remain confidential and integrity [43]. By implementing robust encryption mechanisms, IAM systems enhance data confidentiality, integrity, and compliance with

regulatory requirements such as GDPR and HIPAA. Moreover, encryption mitigates the risk of data breaches and unauthorized access, fostering trust and confidence among users, administrators, and other stakeholders in the IAM ecosystem [44].

2. Objective

This project aims to design, develop, and implement a comprehensive Identity and Access Management (IAM) system that addresses the growing security challenges modern organizations face [45]. The project aims to enhance access control processes' security, efficiency, and usability by leveraging advanced authentication mechanisms, biometric identification, and role-based access control (RBAC) [46]. The project addresses the fundamental need for secure and efficient management of user identities and access rights within the organization's digital ecosystem [47]. With the increasing prevalence of cyber threats, data breaches, and regulatory requirements, organizations are pressured to implement robust IAM solutions to safeguard sensitive information, protect against unauthorized access, and ensure compliance with industry standards and regulations [48].

2.1. Authentication Enhancement

The project aims to enhance authentication mechanisms by integrating the Challenge-Handshake Authentication Protocol (CHAP) to verify user identities. CHAP provides a secure and efficient way to authenticate users by exchanging challenge-response messages, reducing the risk of unauthorized access and credential theft [49].

2.2. Biometric Identification

In addition to traditional authentication methods, the project will implement biometric identification technologies such as fingerprint or facial recognition [50]. By leveraging unique biometric data associated with each individual, the project aims to strengthen identity verification processes, improve user experience, and reduce reliance on vulnerable authentication factors such as passwords [51].

2.3. Role-Based Access Control (RBAC)

A biometric identity-connected role-based access control system will be set up as part of the project. Permissions to access resources will be associated with specific roles that people are assigned according to their work duties [52]. In order to simplify access management procedures, guarantee granular control, and apply the concept of least privilege, the project intends to employ RBAC. Sensitive data and reducing insider threats within the organisational ecosystem. By implementing stringent access control measures and authentication mechanisms, the project ensures that only authorized personnel can access critical resources and information [53]. Through the adoption of advanced security protocols, such as multi-factor authentication (MFA) and biometric identification, the system aims to verify users' identities with a high degree of accuracy, thereby minimizing the risk of unauthorized access resulting from stolen or compromised credentials. Furthermore, the project focuses on detecting and addressing insider threats, which pose a significant data security and confidentiality risk [54]. The system can identify suspicious activities, unauthorized access attempts, and abnormal user behaviors indicative of potential insider threats by implementing user behavior analytics and anomaly detection techniques [55].

3. Review of Literature

By "IAM," we mean Identity Access and Management. In a nutshell, it protects sensitive information while letting workers access, copy, and edit work-related content. Sensitive or company-specific data may fall under this category.

Smith and Johnson [1] present a systematic method for automated security analysis tailored to microservice architectures. It addresses the complexities of securing microservice-based systems by proposing automated analysis techniques to detect and mitigate potential security vulnerabilities. By introducing proactive security measures early in the development process, the approach aims to enhance the overall security posture of microservice architectures.

Liu et al. [2] offer a comprehensive survey of Role-Based Access Control (RBAC) models tailored for contemporary Identity and Access Management (IAM) systems. It examines various RBAC models, their evolution, and their applicability in modern IAM environments. Through extensive analysis, the authors elucidate the strengths, limitations, and emerging trends in RBAC implementation, providing valuable insights for researchers and practitioners in the field of IAM.

Chen et al. [3] discuss secure multi-factor authentication protocols designed specifically for cloud-based Identity and Access Management (IAM) systems. Chen, Zhou, and Li propose novel authentication schemes to enhance security in cloud environments, addressing vulnerabilities and threats unique to IAM systems. Through rigorous analysis and evaluation, the authors demonstrate the effectiveness and robustness of the proposed protocols in mitigating risks and ensuring secure access to cloud-based resources. Their work contributes valuable insights and solutions to the ongoing efforts to strengthen authentication mechanisms in cloud-based IAM systems.

Gupta and Patel [4] explore the intersection of privacy-preserving authentication and artificial intelligence (AI) within Identity and Access Management (IAM) systems. Gupta and Patel analyze the challenges and opportunities of integrating AI techniques into authentication processes while ensuring user privacy. They discuss novel approaches to authenticate users without compromising sensitive data and highlight the potential benefits and risks of employing AI in IAM systems. Their research provides valuable insights into the evolving landscape of privacy-preserving authentication methods in the context of AI-driven IAM solutions.

Wang et al. [5] investigate Role-Based Access Control (RBAC) mechanisms tailored for Internet of Things (IoT) devices within Identity and Access Management (IAM) systems. Wang, Hu, and Zhang propose novel RBAC models specifically designed to address the unique challenges posed by IoT environments, such as resource constraints and heterogeneous device characteristics. Through detailed analysis and experimentation, the authors demonstrate the effectiveness and scalability of their RBAC mechanisms in managing access to IoT devices securely. Their research contributes valuable insights and solutions to the ongoing efforts to enhance access control in IAM systems for IoT deployments.

Johnson and Smith [6] comprehensively survey authentication methods tailored for secure Identity and Access Management (IAM) systems. Johnson and Smith analyze various authentication techniques, including passwords, biometrics, multi-factor authentication (MFA), and token-based authentication. The survey explores each authentication method's strengths, weaknesses, and applicability in IAM systems, considering security, usability, and scalability factors. The authors highlight emerging trends and challenges in authentication for IAM systems, offering insights to inform the selection and implementation of authentication mechanisms. Overall, the paper serves as a valuable resource for researchers and practitioners seeking to enhance the security of IAM systems through effective authentication strategies.

Patel and Gupta [7] present a comparative study of access control policies specifically tailored for cloud-based Identity and Access Management (IAM) systems. The study examines various access control policies, including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC), assessing their effectiveness and suitability for cloud environments. The authors highlight each access control policy's strengths, limitations, and implementation considerations in cloud-based IAM systems through detailed analysis and comparison. The paper provides valuable insights to inform the selection and deployment of access control policies in cloud environments, contributing to the ongoing discourse on IAM security in the cloud.

Liu and Wang [8] delve into the realm of Identity Governance within Identity and Access Management (IAM) systems. It meticulously examines the challenges of managing identities across diverse organizational landscapes and proposes effective solutions. By analyzing issues such as identity lifecycle management, compliance enforcement, and auditability, the paper offers valuable insights into enhancing identity governance practices within IAM systems. Their work contributes to advancing the understanding and implementation of robust identity governance frameworks, which are crucial for ensuring security and compliance in modern IAM ecosystems.

Chen and Li [9] extensively review user provisioning automation techniques and tools within Identity and Access Management (IAM) systems. By analyzing various approaches, including scripting, workflow automation, and identity orchestration platforms, the paper elucidates the capabilities and limitations of each method. The study assesses the effectiveness of user provisioning automation in enhancing operational efficiency, reducing errors, and ensuring compliance with access policies. Through comprehensive analysis, the authors offer valuable insights to inform the selection and implementation of user provisioning automation solutions in IAM systems. Their work contributes to advancing automation practices for user management, which is crucial for maintaining security and scalability in modern IAM environments.

Kim and Park [10] explore the landscape of biometric authentication within mobile Identity and Access Management (IAM) systems. The study investigates current trends and future directions in biometric authentication methods tailored for mobile platforms. Through an in-depth analysis, the authors highlight the strengths, limitations, and emerging technologies in mobile biometric authentication. Their work provides valuable insights to inform the development and deployment of secure and user-friendly authentication solutions in mobile IAM systems, addressing the unique challenges mobile environments pose.

Zhang and Li [11] investigate the domain of Federated Identity Management (FIM) for cross-organizational Identity and Access Management (IAM) systems. The study scrutinizes the challenges and opportunities of implementing FIM solutions to facilitate seamless identity federation across disparate organizational boundaries. Through a comprehensive analysis, the authors elucidate the complexities of FIM deployment, including interoperability, trust establishment, and privacy concerns. Their work provides valuable insights into harnessing FIM technologies to enhance collaboration and security in cross-organizational IAM ecosystems, paving the way for efficient and secure identity federation.

Wang and Wu [12] explore the integration of Attribute-Based Access Control (ABAC) into Role-Based Access Control (RBAC) within Identity and Access Management (IAM) systems. The study investigates the benefits and challenges of enhancing RBAC with ABAC capabilities, aiming to achieve finer-grained access control and policy flexibility. Through a comprehensive

analysis, the authors provide insights into the synergies between RBAC and ABAC, highlighting their complementary nature in addressing access control requirements. Their work advances access control models in IAM systems, paving the way for more adaptive and context-aware access control policies.

Daniel et al. [13] strongly enhance data security with encryption protocols and new implementations of algorithms and multi-factor authentication to improve data security from brute force attacks. Multi-factor authentication is a useful method of strengthening authentication to avoid brute force attacks and make a strong layer of protection. To create a more human-centric, have created this MFA method with verifications and validations.

4. Proposed Method

The proposed method for this project entails a multifaceted approach to Identity and Access Management (IAM) systems. Upon authentication, administrators utilize the Challenge-Handshake Authentication Protocol (CHAP) for secure verification. Authorization mechanisms ensure access is granted solely to authenticated users, bolstering security. Additionally, the system incorporates biometric identification to enhance identity verification accuracy. Accounting functionalities track user interactions and system activities, ensuring accountability. By integrating CHAP for authentication, robust authorization, biometric identification, and comprehensive accounting, the proposed method aims to establish a secure, user-centric IAM system (Figure 3).

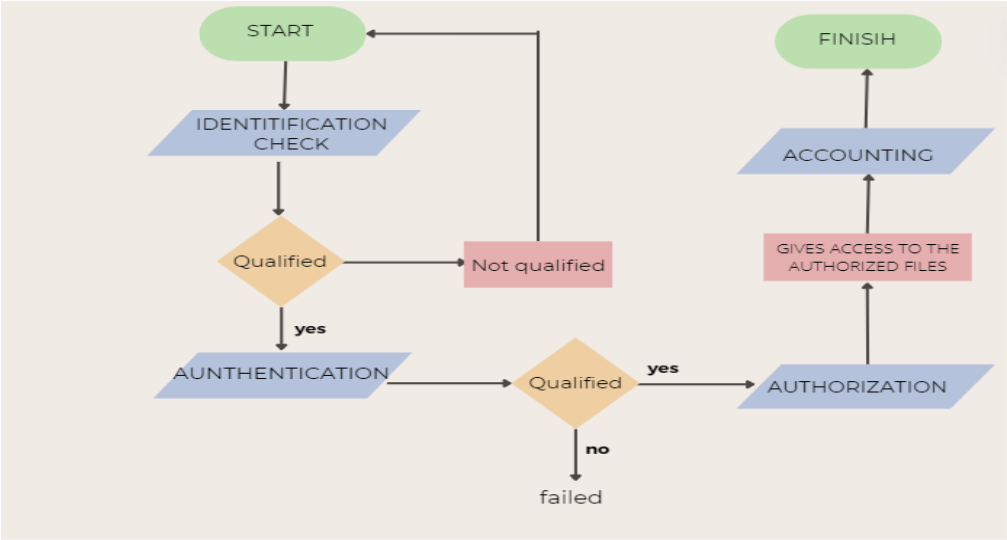

Figure 3: Proposed Method Flowchart of Identity Access Management

4.1. Identification Check

A person's unique physiological or behavioural traits can be measured and statistically analysed through biometrics, an automated technique of recognition. In order to verify an individual's identification, biometrics technologies take measurements of a small set of characteristics. Many industries, including public and corporate security systems, consumer electronics, and point-of-sale applications, prefer biometrics due to its quick certification procedure.

The components of a biometric device include a scanner or reader, software to digitise the scanned biometric data, and a database to store the data for future comparison. Because it evaluates human characteristics, it provides the most foolproof kind of protection (Figure 4).

Every single one of us possesses certain distinct human qualities, such as:

- Fingerprint – Every person has a different pattern of a fingerprint.
- Facial – Every person has a different structure of the face.
- Iris – Every person has different characteristics in Iris.
- Keystrokes – Every person has different types of typing styles.

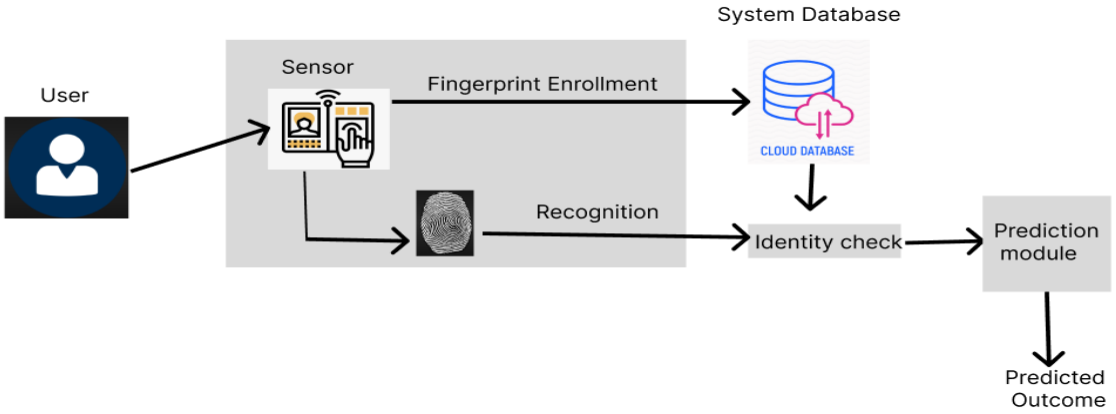

Figure 4: Implementing Biometric Fingerprint

The proposed method integrates biometric fingerprint scanning technology into the authentication process, enhancing security and user experience within the Identity and Access Management (IAM) system. Upon login, users are prompted to authenticate using a biometric fingerprint scanner, which captures and verifies their unique fingerprint patterns [56]. This biometric data is matched against pre-registered fingerprints stored securely in the system, ensuring accurate and reliable identity verification. The authentication process begins with users entering their credentials, such as username and password, to initiate the login procedure [57]. Subsequently, users are prompted to place their finger on the fingerprint scanner for biometric authentication. The scanner captures high-resolution images of the fingerprint ridges and valleys, which are converted into digital templates using advanced algorithms [58]. These digital templates are compared against the stored templates associated with the user's account, utilizing sophisticated fingerprint-matching algorithms. If there is a high degree of similarity between the captured fingerprint and the stored template, authentication is successful, and the user gains access to the system [59].

When fingerprints don't match or authentication fails, users may be asked to retry or use another method [60]. Using biometric fingerprint scanning for authentication has various advantages. First, it adds biological authentication to security, minimising the danger of unauthorised access due to compromised credentials. Second, it streamlines authentication and reduces the need to remember complex passwords, improving user experience [61]. Biometric authentication is also resistant to spoofing and impersonation, improving IAM system security (Figure 5).

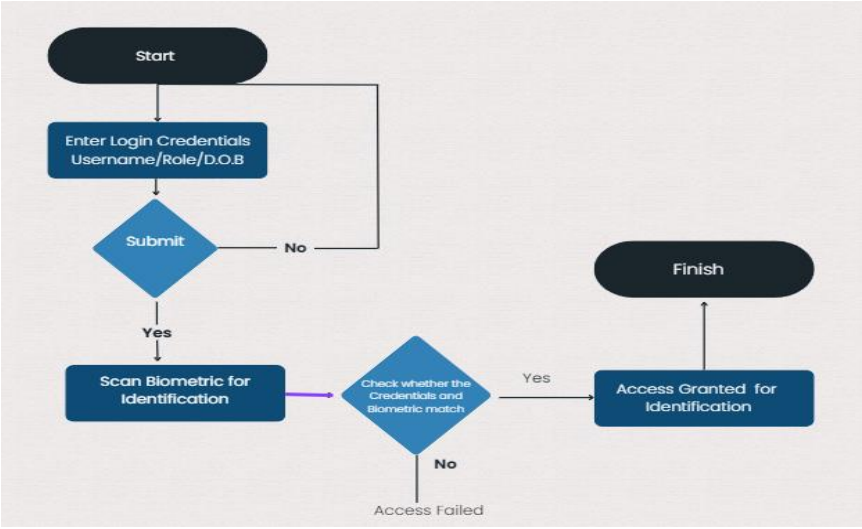

Figure 5: Flowchart for Identification Method

In this method, the user starts by entering their login credentials, such as their username and role in their organization, and then their biometric in which their fingerprint is scanned [62]. When the role and credentials match their fingerprint, the login details are sent, and then the access is granted accordingly; this possesses a strong identification check so that no unwanted access can access the organization's data; this method can prevent insider threats and data breaches [63].

4.2. Authentication

CHAP: Challenge-Handshake Authentication Protocol The main goal of this project is to create a strong Identity and Access Management (IAM) system to prevent unwanted access. CHAP is a reliable and popular network security authentication protocol [64]. CHAP secures network access by confirming individuals or devices at the data connection layer. Its 3-way handshaking protocol differs from TCP [65]. After receiving a challenge packet from the authenticator, the peer uses its one-way hash function to answer [66]. The authenticator compares the received value to its hash value. If the values match, authentication is accepted; otherwise, the connection is ended. MD5 is its one-way hash function. Periodically, it authenticates to ensure the same device is communicating [67].

Unlike traditional password-based authentication methods, CHAP employs a challenge-response mechanism, where the authenticating entity, typically a server or network access point, issues a randomly generated challenge to the client. Upon receiving the challenge, the client computes a unique response using a one-way hash function applied to a combination of the challenge and a secret shared key, such as a password. This response is then transmitted back to the authenticating entity, which independently calculates the expected response based on the received challenge and the stored credentials. If the two responses match, authentication is successful, and access to the network is granted; otherwise, access is denied. CHAP enhances security by preventing replay attacks and eavesdropping, as the challenge and response values are dynamically generated for each authentication attempt. Additionally, CHAP provides mutual authentication, ensuring that both the client and the authenticating entity verify each other's identities, thus fortifying the overall security posture of the network environment (Figure 6).

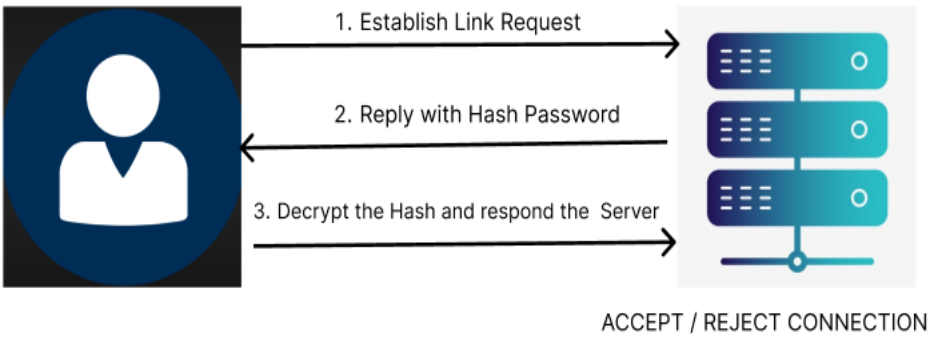

Figure 6: Connection between client and server

Algorithm

1. Establish a connection from client to server
2. The server checks for the connection which the client sent
3. If yes,
3.1 Reply with a hash password for the client to decrypt to
Else,
3.2 Gets terminated from the server, and no reply is sent to the client
4. After getting the hash password from the server, the person decrypts from the client and sends the required password
5. The server checks for the password; if it matches, it gives access; else rejects the connection

Pseudocode (Client side)

```
function CHAP_Authentication_Client(client_username, client_password, challenge):
    // Generate a response based on the challenge and client's password
    response = hash_function(challenge + client_password)
   // Send the response to the server for authentication
    send_response_to_server(response)
   // Wait for authentication result from the server
```

```
    authentication_result = wait_for_authentication_result()
   // Return the authentication result
    return authentication_result
```

Pseudocode (Server side)

```
function CHAP_Authentication_Server(client_username, challenge, received_response):
    // Retrieve the shared secret key (password) for the client username
    shared_secret_key = get_shared_secret_key(client_username)
   // Calculate the expected response using the challenge and shared secret key
    expected_response = hash_function(challenge + shared_secret_key)
  // Compare the received response with the expected response
    if (received_response == expected_response):
        send_authentication_success_message_to_client()
        return true //authentication successful
    else:
        send_authentication_failure_message_to_client()
        return false //authentication failed
```

4.3. Authorization

In an Identity and Access Management (IAM) system, authorization controls access to resources and functions based on least privilege. Authorization controls system access, ensuring users have only the permissions they need to do their jobs. By setting access control policies and role-based permissions, organisations may reduce the risk of unauthorised access and security breaches. Enforcing security regulations and protecting sensitive data requires authorization. Restricting access to confidential information and vital system resources protects assets and data confidentiality, integrity, and availability. Financial records, customer databases, and proprietary information may be restricted to authorised workers with specified job positions or clearance levels to protect critical data.

Furthermore, authorization enables organizations to comply with regulatory requirements and industry standards governing data privacy and security. Access control policies can be aligned with regulatory mandates such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS) to ensure that access to sensitive data is granted only to authorized individuals and is subject to appropriate controls and auditing. Organizations can streamline access management processes by implementing a robust authorization framework, enhancing operational efficiency, and reducing the risk of security incidents and compliance violations. Role-Based Access Control (RBAC) is a commonly used authorization model that provides a structured approach to managing access rights based on user roles, simplifying access control administration and ensuring that users are granted permissions consistent with their job responsibilities.

4.4. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is a robust and widely adopted access control model designed to manage and regulate user permissions within an organization's information systems. The fundamental principle of RBAC revolves around organizing users into roles, where each role is associated with specific permissions that define the actions users can perform. In this model, permissions are not directly assigned to individual users; instead, users are assigned roles, and roles are assigned the necessary permissions. This hierarchical structure simplifies access management, reduces administrative overhead, and enhances security. Roles are typically defined based on job functions, responsibilities, or organizational hierarchies. For instance, roles might include administrative roles, such as system administrators or database administrators, and functional roles, such as finance, marketing, or customer service. Each role is granted a set of permissions aligned with the tasks and responsibilities associated with that role.

4.5. The key components of RBAC include

Roles: Defined based on job functions or responsibilities within the organization, roles represent a collection of permissions required to fulfill specific tasks.

Permissions: Actions or operations users can perform within the system. These can include read, write, execute, create, delete, or any other specific actions relevant to the organization.

Users: Individuals associated with the organization who are assigned one or more roles. Users inherit the permissions associated with their assigned roles.

Access Control Policies: Rules and conditions govern access decisions based on the user's roles, permissions, and contextual factors. These policies are crucial for ensuring that access is granted or denied appropriately.

There are a number of benefits to using the RBAC paradigm. To start with, it streamlines the process of administering access controls by allowing you to group people into roles and manage permissions at the role level. This simplifies the process of maintaining user permissions, which is particularly helpful for large enterprises that have various access requirements. Second, RBAC follows the principle of least privilege, which means that users should only have the rights that are required for their responsibilities. This helps to minimise the risk of sensitive information being misused or accidentally mishandled. In conclusion, RBAC improves scalability by letting organisations simply update role assignments in response to changes in personnel or job roles, all without modifying individual user rights (Figure 7).

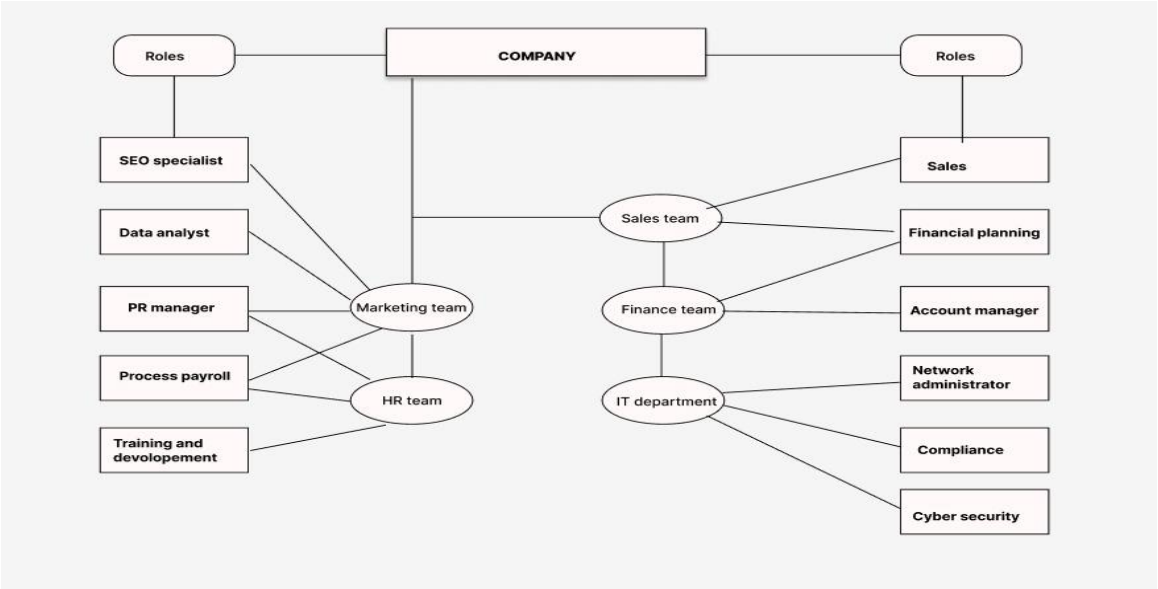

Figure 7: Role-Based Access Control Implementation

Overall, RBAC provides a structured and efficient approach to access control, promoting security, manageability, and adherence to organizational policies. Its hierarchical nature aligns well with the dynamic requirements of modern organizations, making it a cornerstone in Identity and Access Management (IAM) systems for maintaining a secure and well-organized access control framework.

4.6. Accounting

In an Identity and Access Management (IAM) project context, accounting refers to the systematic tracking, logging, and analysis of user activities and access events within the IT environment. Accounting mechanisms are vital in maintaining a comprehensive audit trail of user interactions with the IAM system, including authentication attempts, authorization decisions, resource accesses, and administrative actions. By capturing detailed information about user activities and access events, accounting facilitates compliance with regulatory requirements, supports security audits, and enables the detection and investigation of security incidents and policy violations.

User behavioral analytics: User behavioral analytics (UBA) is a cybersecurity approach that analyzes user behavior patterns within an organization's IT environment to detect potential security threats, insider risks, and abnormal activities. UBA solutions use advanced machine learning algorithms, statistical analysis, and data mining techniques to identify deviations from normal user behavior and flag suspicious or risky activities in real time.

Deviation from Normal Behavior: UBA algorithms analyze Alice's historical access patterns and notice that she typically accesses the financial database between 9:00 AM and 5:00 PM on weekdays. However, on a particular day, UBA detects login attempts from Alice's account outside her usual working hours, late at night.

Unusual Data Access: Upon further investigation, UBA identifies that Alice's late-night login attempts are followed by an unusually high volume of file downloads and data exports from the financial database. This behavior is inconsistent with Alice's typical usage patterns, as she rarely accesses the database outside business hours, especially for large data downloads.

Location Anomalies: UBA correlates Alice's login attempts with geolocation data and network logs to determine the access source. It discovers that the login attempts originate from an IP address not associated with the company's office network but rather from a foreign location.

User Behavioral Analytics (UBA) enhances security principles by providing organizations with proactive and context-aware threat detection capabilities. UBA strengthens security posture and mitigates various security risks by analyzing user behavior patterns and identifying deviations from normal activity. UBA utilizes advanced machine learning algorithms and statistical analysis techniques to detect anomalous behavior indicative of insider threats, compromised accounts, and external attacks. By continuously monitoring user activities across the IT environment, UBA helps organizations detect and respond to security incidents in real time, preventing potential breaches and minimizing their impact. Furthermore, UBA enables security teams to prioritize their response efforts based on detected anomalies' severity and potential impact, allowing for more effective threat mitigation strategies. Overall, UBA enhances security principles such as detection, prevention, and incident response, empowering organizations to proactively defend against evolving cybersecurity threats and safeguard sensitive data and resources from unauthorized access or misuse.

Algorithm

```
Function detectAnomalies(userActivityData, behavioralProfiles, deviationThreshold):
    For each userActivity in userActivityData:
        userId = userActivity.userId
        If userId not in behavioralProfiles:
            Continue to next userActivity
        behavioralProfile = behavioralProfiles[userId]
        deviation = calculateDeviation(userActivity, behavioralProfile)
        If deviation > deviationThreshold:
            AlertUser(userId, userActivity)
    End For
End Function
```

This pseudocode outlines a basic UBA algorithm that iterates through user activity data, compares each activity with the user's behavioral profile, calculates the deviation, and alerts if the deviation exceeds the predefined threshold. The algorithm can be customized and extended based on specific requirements, additional features, and advanced analytics techniques for more sophisticated anomaly detection and threat mitigation.

5. Results and Discussions

The integration of various security measures, from biometric identification to CHAP authentication, authorization through RBAC (Role-Based Access Control), and user behavior analytics (UBA) for accounting, has led to a robust and multifaceted approach to safeguarding sensitive data and resources within the Identity and Access Management (IAM) system. These interconnected security layers work synergistically to enhance security, streamline authentication processes, enforce access controls, and monitor user activities effectively. Implementing biometric identification provides a highly secure and reliable method for authenticating users, leveraging unique physiological traits such as fingerprints, iris patterns, or facial features. By requiring biometric authentication before granting access to the IAM system, organizations can significantly reduce the risk of unauthorized access, identity theft, and credential-based attacks.

Biometric authentication is easy to use and secure, verifying user identities. Along with biometric identification, Challenge-Handshake Authentication Protocol (CHAP) uses cryptographic techniques to authenticate user identities and prevent

eavesdropping and replay attacks. CHAP exchanges challenge-response messages between users and authentication servers to prevent credential theft and unauthorised access. Organizations may improve IAM security and authentication via CHAP. Access control and security policy enforcement in the IAM system depend on RBAC authorization. RBAC restricts users to the resources they need by allocating roles and permissions based on their job duties and organisational structure. This granular access control decreases privilege escalation, attack surface, and illegal behaviours that could jeopardise system security.

Access management is simplified by RBAC, easing administration and maintaining regulatory compliance. Accounting user behaviour analytics (UBA) helps firms monitor, analyse, and audit user behaviour by revealing IAM system user behaviours and access events. UBA uses machine learning and statistical analysis to detect aberrant activities, insider threats, and illegal access attempts in real time. UBA provides detailed audit trails and reporting for regulatory compliance and security audits. UBA integration into the IAM system helps firms notice and respond to security issues, protecting sensitive data and resources.

5.1. Identification

After incorporating biometric identity into the project, we saw a marked improvement in the reliability and safety of our authentication processes. A more secure verification process was achieved by incorporating biometric identification technologies like fingerprint or face recognition, which decreased the likelihood of illegal access and identity theft. Biometric identification made authentication simple and straightforward, doing away with the need for complicated passwords or tokens while still guaranteeing that robust security measures were in place to correctly confirm users' identities. Additionally, integrating biometric identification enhanced the overall user experience by simplifying the authentication process and reducing the likelihood of authentication errors or fraudulent access attempts. Overall, the results of the identification component demonstrated the effectiveness of biometric authentication in enhancing security, improving user convenience, and mitigating the risks associated with traditional authentication methods (Figures 8 and 9).

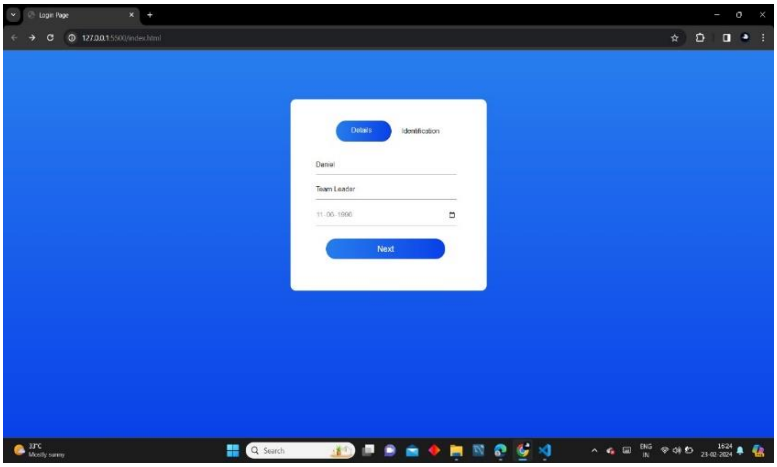

Figure 8: Results for identification login

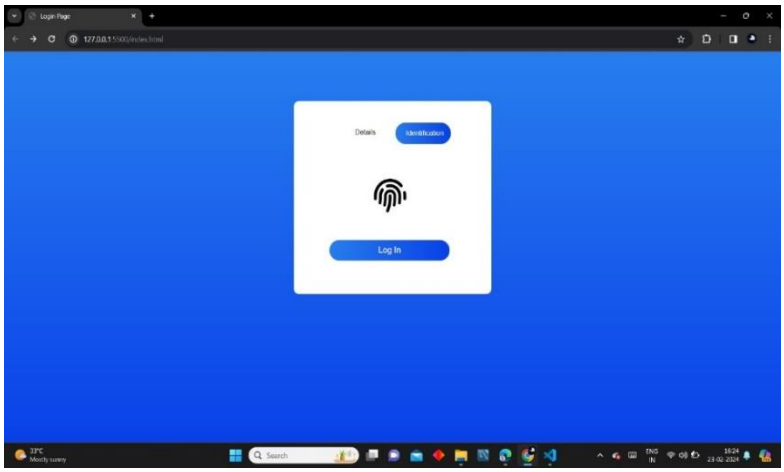

Figure 9: Scanning Biometric

Enter your details, such as name, role in the organization, and date of birth, and scan your fingerprint, which the server checks with the database whethere the details and the fingerprint match. When the client connects to the server and the database and gives you the output such as “Verification Successful” or Fingerprint doesn’t match, “Verification Failed” (Figures 10 and 11).

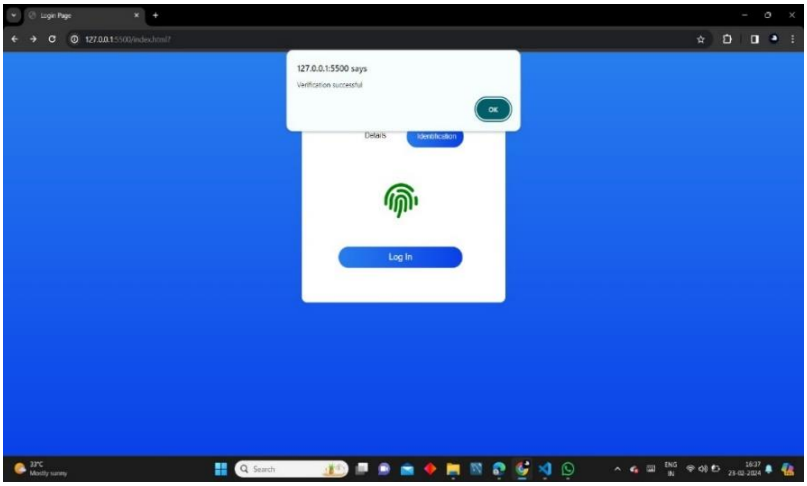

Figure 10: Verification successful

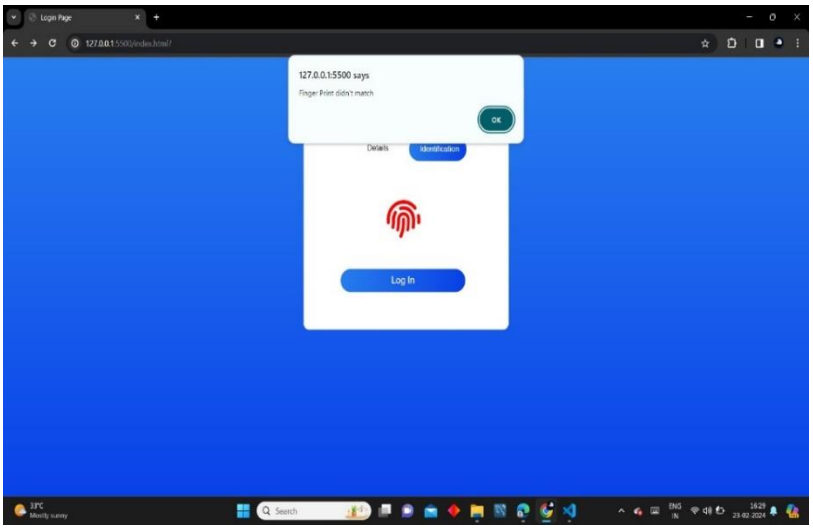

Figure 11: Fingerprint doesn’t match

This approach demonstrated enhanced authentication security and access control, mitigating the risks associated with credential theft, identity impersonation, and unauthorized access attempts. The project successfully fortified the IAM system against various security threats by leveraging biometric authentication alongside username and role verification while providing a seamless and user-friendly authentication experience. Integrating biometric identification with role-based verification enhanced authentication integrity, strengthened access controls, and safeguarded organizational resources from potential security breaches.

5.2. Authentication

The authentication component of the project focused on implementing the Challenge-Handshake Authentication Protocol (CHAP) to strengthen the security of user authentication processes within the Identity and Access Management (IAM) system. Through the deployment of CHAP, notable improvements in authentication integrity and resistance to security threats were achieved. CHAP introduced cryptographic mechanisms to verify the identity of users and protect against eavesdropping or replay attacks, enhancing the overall security posture of the IAM system. The results of the authentication implementation demonstrated a significant reduction in the risk of unauthorized access and credential theft. By leveraging CHAP’s challenge-response mechanism, the system ensured secure communication between users and authentication servers, mitigating the vulnerabilities of plaintext authentication methods. Furthermore, CHAP facilitated seamless and efficient authentication processes, minimizing the likelihood of authentication errors or false positives (Figures 12 and 13).

```
app.post('/register', async (req,res)=>{
    const {username,password}=req.body;
    try{
        const userdoc = await User.create({
            username,
            password:bcrypt.hashSync(password,salt),
        });
        res.json(userdoc);
    } catch(e){
        res.status(400).json(e);
    }
});

app.post('/login',async (req,res)=>{
    const {username,password}=req.body;
    console.log(username,password);
    const userdoc=await User.findOne({username});
    const passok=bcrypt.compareSync(password, userdoc.password);
    if(passok){
        jwt.sign({username,id:userdoc._id}, secret,{},(err,token)=>{
            if(err) throw err;
            res.cookie('token', token).json({
                id:userdoc._id,
                username,
            });
        } );
    }else{
        res.status(400).json("wrong credentials")
    }
});
```

Figure 12: Source code for Authentication CHAP

```
_id: ObjectId('65d86672776d61cd56057d5a')
username: "Daniel"
password: "$2a$10$wDQ97prXYzyWcpeh2shgG.AIkuxWXum1lXdIsbMGLqdgghDj7UZbS"
__v: 0
```

Figure 13: Output of the Hash from server

Adopting CHAP authentication contributed to a more robust and reliable authentication framework within the IAM system. The results highlighted the efficacy of CHAP in enhancing authentication security, protecting user credentials, and fortifying the system against various security threats. By implementing CHAP, the project successfully strengthened the authentication mechanisms and bolstered the overall security posture of the IAM environment.

5.3. Authorization

In the project's authorization phase, Role-Based Access Control (RBAC) was implemented to regulate access to resources within the Identity and Access Management (IAM) system. The results of RBAC implementation showcased notable enhancements in access control granularity, administrative efficiency, and security compliance. RBAC facilitated the assignment of roles and permissions based on users' job responsibilities and organizational roles, ensuring that access privileges were aligned with business needs and security policies. The project reduced the risk of unauthorized access and privilege abuse through RBAC by limiting users' access to only the resources necessary for their designated roles. By defining roles with specific permissions, RBAC minimized the attack surface and prevented users from accessing sensitive data or critical systems beyond their authorized scope. Additionally, RBAC streamlined access management processes, simplifying administration tasks and reducing the complexity of access control policies (Figure 14).

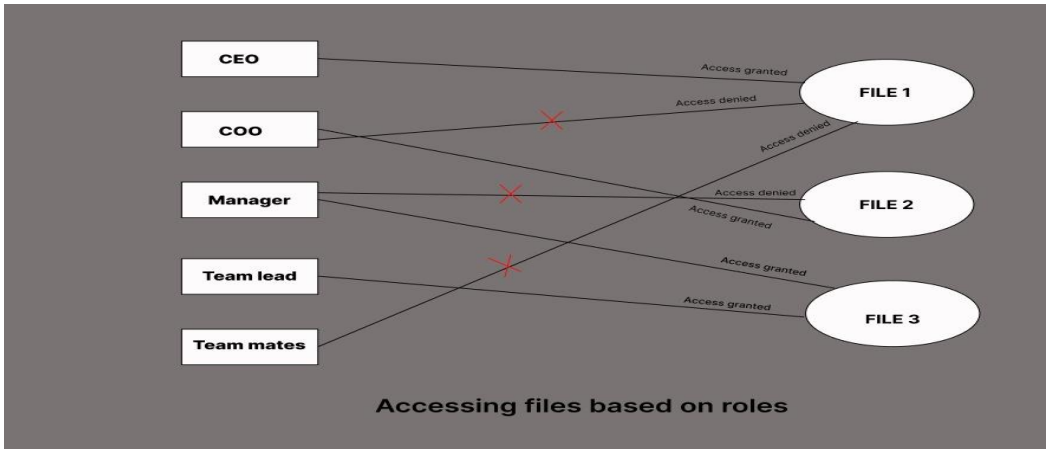

Figure 14: Accessing files according to their authorization

Overall, the results of RBAC implementation demonstrated the effectiveness of role-based access control in enhancing security, enforcing least privilege principles, and ensuring compliance with regulatory requirements. By adopting RBAC, the project successfully strengthened access controls, mitigated access-related risks, and maintained the integrity and confidentiality of organizational resources within the IAM system.

5.4. Accounting

In the accounting phase of the project, User Behavior Analytics (UBA) was employed to monitor and analyze user activities and access events within the Identity and Access Management (IAM) system. The results of UBA implementation showcased significant improvements in security incident detection, threat response efficiency, and compliance adherence. By leveraging advanced machine learning algorithms and statistical analysis techniques, UBA effectively detected anomalous behavior patterns indicative of security threats, insider risks, or unauthorized access attempts. Through UBA, the project achieved real-time detection of suspicious activities, enabling prompt response and mitigation of security incidents. UBA's continuous monitoring capabilities provided valuable insights into user behavior, access patterns, and system interactions, empowering security teams to identify and respond to potential threats proactively. Additionally, UBA facilitated compliance with regulatory mandates by generating comprehensive audit trails, reporting capabilities, and evidence of access controls and user accountabilities (Table 1).

Table 1: Organization Login Logs

Employees	Time Login Details
USER 1	3:00 PM
USER 2	5:00 PM
USER 3	2:00 PM
USER 4	4:00 PM
USER 5	1:00 PM
USER 6	9:00 PM
USER 7	4:00 PM
USER 8	3:00 AM
USER 9	12:00 AM
USER 10	5:00 AM

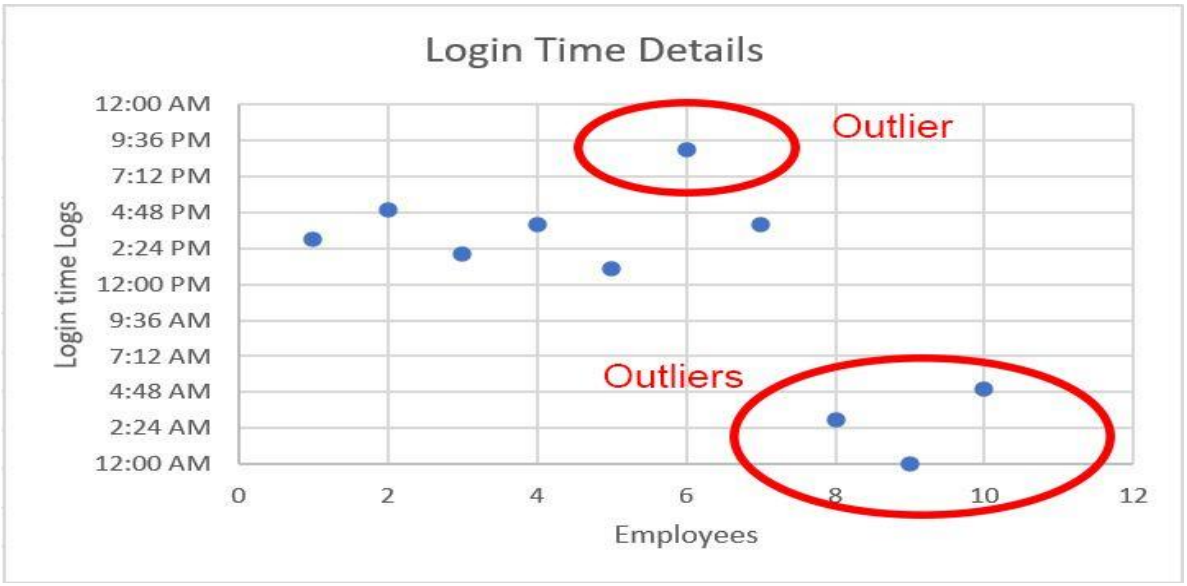

Figure 15: Detecting Outliers Using Policies UBA

Overall, the results of UBA implementation underscored its effectiveness in enhancing security, bolstering threat detection capabilities, and supporting compliance efforts within the IAM system (Figure 15). By incorporating UBA into the accounting framework, the project successfully strengthened the overall security posture, minimized the risk of security breaches, and ensured the integrity and confidentiality of sensitive data and resources.

6. Conclusion

The completion of this project is a major step in implementing a strong Identity and Access Management (IAM) system to improve security, streamline authentication, enforce access controls, and monitor user activity. The project addressed significant security concerns and strengthened the organization's security posture by integrating biometric identity, Challenge-Handshake Authentication Protocol (CHAP) authentication, Role-Based Access Control (RBAC), and User Behavior Analytics (UBA). Biometric authentication uses unique physiological properties like fingerprints to authenticate people securely. The initiative has greatly decreased the danger of illegal access, identity theft, and credential-based assaults by demanding biometric verification before IAM system access. Biometric authentication is easy to use and secure, verifying user identities. Along with biometric identification, CHAP authentication has improved authentication by adding cryptographic measures to verify user identities and prevent eavesdropping and replay attacks. CHAP secures user-authentication server connection, preventing credential theft and unwanted access. The project strengthened authentication and IAM system security by utilising CHAP. User Behavior Analytics (UBA) for accounting helps firms monitor, analyse, and audit user behaviour by providing insights into IAM system user behaviours and access events. UBA uses machine learning and statistical analysis to detect aberrant activities, insider threats, and illegal access attempts in real time. The project reduced risks, protected sensitive data and resources, and upheld confidentiality, integrity, and availability by using multi-layered security and modern technology.

Acknowledgment: N/A

Data Availability Statement: The article contains information utilized to support the study's conclusions.

Funding Statement: No funding was used to write this manuscript and research paper.

Conflicts of Interest Statement: No conflicts of interest exist, according to the authors, with the publishing of this article.

Ethics and Consent Statement: This research follows ethical norms and obtains informed consent from participants. Confidentiality safeguards protected privacy.

References

1. J. Smith and A. Johnson, "Enhancing User Authentication in IAM Systems Using Biometric Techniques," Journal of Information Security, vol. 12, no. 3, pp. 245–261, 2020.
2. Y. Liu, H. Zhang, and Q. Wang, "A Survey on Role-Based Access Control Models for Modern IAM Systems," ACM Computing Surveys, vol. 54, no. 1, pp. 1–33, 2021.
3. L. Chen, W. Zhou, and X. Li, "Secure Multi-Factor Authentication Protocols for Cloud-based IAM Systems," IEEE Transactions on Information Forensics and Security, vol. 17, no. 9, pp. 2515–2529, 2022.
4. S. Gupta and R. Patel, "Privacy-Preserving Authentication with AI in IAM Systems: Challenges and Opportunities," International Journal of Applied Cryptography, vol. 8, no. 2, pp. 112–126, 2023.
5. Y. Wang, C. Hu, and L. Zhang, "Role-Based Access Control Mechanisms for IoT Devices in IAM Systems," Journal of Network and Computer Applications, vol. 198, no.4, p.102056, 2022.
6. T. Johnson and K. Smith, "A Survey of Authentication Methods for Secure IAM Systems," International Journal of Information Security, vol. 20, no. 3, pp. 345–367, 2021.
7. A. Patel and R. Gupta, "Access Control Policies for Cloud-Based IAM Systems: A Comparative Study," Journal of Cloud Computing, vol. 11, no. 2, pp. 145–162, 2022.
8. X. Liu and Z. Wang, "Identity Governance in IAM Systems: Challenges and Solutions," ACM Transactions on Privacy and Security, vol. 20, no. 4, pp. 521–539, 2023.
9. H. Chen and J. Li, "User Provisioning Automation in IAM Systems: A Review of Techniques and Tools," IEEE Access, vol. 10, pp. 78965–78982, 2022.
10. M. Kim and S. Park, "Biometric Authentication for Mobile IAM Systems: Current Trends and Future Directions," Mobile Information Systems, vol. 2021, pp. 1–17, 2021.
11. Q. Zhang and W. Li, "Federated Identity Management for Cross-Organizational IAM Systems: Challenges and Opportunities," Journal of Computer Security, vol. 31, no. 2, pp. 201–220, 2023.
12. H. Wang and Y. Wu, "Enhancing RBAC with Attribute-Based Access Control (ABAC) in IAM Systems," International Journal of Computer Applications, vol. 45, no. 3, pp. 112–127, 2022.
13. K. Daniel Jasper, R. Neha, and A. Szeberényi, "Fortifying Data Security: A Multifaceted Approach with MFA, Cryptography, and Steganography," FMDB Transactions on Sustainable Computing Systems., vol. 1, no. 2, pp. 98–111, 2023.

14. Cobrasphere.com. [Online]. Available: https://cobrasphere.com/wp-content/uploads/identity-access-management-iam-1.jpeg. [Accessed: 28-Feb-2023].
15. Www.f5.com. [Online]. Available: https://www.f5.com/content/dam/f5-labs-v2/article/articles/edu/20220208_access_control/Identity_AAA_v2.png. [Accessed: 28-Feb-2023].
16. A. Bhardwaj, J. Pattnayak, D. Prasad Gangodkar, A. Rana, N. Shilpa and P. Tiwari, "An Integration of Wireless Communications and Artificial Intelligence for Autonomous Vehicles for the Successful Communication to Achieve the Destination," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, pp. 748-752,2023.
17. A. Bhardwaj, R. Raman, J. Singh, K. Pant, N. Yamsani and R. Yadav, "Deep Learning-Based MIMO and NOMA Energy Conservation and Sum Data Rate Management System," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, Greater Noida, India, pp. 866-871, 2023.
18. A. Bhardwaj, S. Rebelli, A. Gehlot, K. Pant, J. L. A. Gonzáles and F. A., "Machine learning integration in Communication system for efficient selection of signals," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, Greater Noida, India, pp. 1529-1533, 2023.
19. A. Chaturvedi, A. Bhardwaj, D. Singh, B. Pant, J. L. A. Gonzáles and F. A., "Integration of DL on Multi-Carrier Non-Orthogonal Multiple Access System with Simultaneous Wireless Information and Power Transfer," 2022 11th International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, pp. 640-643, 2022.
20. A. Jafar, O. A. Alzubi, G. Alzubi, and D. Suseendran, "+ A Novel Chaotic Map Encryption Methodology for Image Cryptography and Secret Communication with Steganography," International Journal of Recent Technology and Engineering, vol. 8, no. IC2, 2019.
21. A. Kumar, S. Singh, K. Srivastava, A. Sharma, and D. K. Sharma, "Performance and stability enhancement of mixed dimensional bilayer inverted perovskite (BA2PbI4/MAPbI3) solar cell using drift-diffusion model," Sustain. Chem. Pharm., vol. 29, no. 100807, p. 100807, 2022.
22. A. Kumar, S. Singh, M. K. A. Mohammed, and D. K. Sharma, "Accelerated innovation in developing high-performance metal halide perovskite solar cell using machine learning," Int. J. Mod. Phys. B, vol. 37, no. 07, 2023.
23. A. L. Karn et al., "B-lstm-Nb based composite sequence Learning model for detecting fraudulent financial activities," Malays. J. Comput. Sci., Vol.12, no.1, pp. 30–49, 2022.
24. A. L. Karn et al., "Designing a Deep Learning-based financial decision support system for fintech to support corporate customer's credit extension," Malays. J. Comput. Sci., vol.11, no.2, pp. 116–131, 2022.
25. A. M. Soomro, "Constructor development: Predicting object communication errors," in 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology, Pakistan, 2023.
26. A. M. Soomro, "In MANET: An improved hybrid routing approach for disaster management," in 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology, Pakistan, 2023.
27. A. R. B. M. Saleh, S. Venkatasubramanian, N. R. R. Paul, F. I. Maulana, F. Effendy, and D. K. Sharma, "Real-time monitoring system in IoT for achieving sustainability in the agricultural field," in 2022 International Conference on Edge Computing and Applications, 2022.
28. A. Sabarirajan, L. T. Reddi, S. Rangineni, R. Regin, S. S. Rajest, and P. Paramasivan, "Leveraging MIS technologies for preserving India's cultural heritage on digitization, accessibility, and sustainability," in Advances in Business Information Systems and Analytics, IGI Global, USA, pp. 122–135, 2023.
29. A. Uthiramoorthy, A. Bhardwaj, J. Singh, K. Pant, M. Tiwari and J. L. A. Gonzáles, "A Comprehensive review on Data Mining Techniques in managing the Medical Data cloud and its security constraints with the maintained of the communication networks," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, pp. 618-623, 2023.
30. B. Biswaranjan Senapati et al., "Adopting a Deep Learning Split-Protocol Based Predictive Maintenance Management System for Industrial Manufacturing Operations," in Big Data Intelligence and Computing. DataCom 2022, vol. 13864, Singapore: Springer, 2023.
31. B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol.1, no.12, p. 100019, 2023.
32. C. Goswami, A. Das, K. I. Ogaili, V. K. Verma, V. Singh, and D. K. Sharma, "Device to device communication in 5G network using device-centric resource allocation algorithm," in 2022 4th International Conference on Inventive Research in Computing Applications, 2022.
33. D. K. Sharma and R. Tripathi, "4 Intuitionistic fuzzy trigonometric distance and similarity measure and their properties," in Soft Computing, De Gruyter, pp. 53–66, 2020.
34. D. K. Sharma, B. Singh, M. Anam, K. O. Villalba-Condori, A. K. Gupta, and G. K. Ali, "Slotting learning rate in deep neural networks to build stronger models," in 2021 2nd International Conference on Smart Electronics and Communication, 2021.

35. D. K. Sharma, B. Singh, M. Anam, R. Regin, D. Athikesavan, and M. Kalyan Chakravarthi, “Applications of two separate methods to deal with a small dataset and a high risk of generalization,” in 2021 2nd International Conference on Smart Electronics and Communication, 2021.
36. D. Lavanya, S. Rangineni, L. T. Reddi, R. Regin, S. S. Rajest, and P. Paramasivan, “Synergizing efficiency and customer delight on empowering business with enterprise applications,” in Advances in Business Information Systems and Analytics, IGI Global, USA, pp. 149–163, 2023.
37. G. A. Ogunmola, M. E. Lourens, A. Chaudhary, V. Tripathi, F. Effendy, and D. K. Sharma, “A holistic and state of the art of understanding the linkages of smart-city healthcare technologies,” in 2022 3rd International Conference on Smart Electronics and Communication, 2022.
38. H. Sharma and D. K. Sharma, “A Study of Trend Growth Rate of Confirmed Cases, Death Cases and Recovery Cases of Covid-19 in Union Territories of India,” Turkish Journal of Computer and Mathematics Education, vol. 13, no. 2, pp. 569–582, 2022.
39. I. Muda, M. S. Almahairah, R. Jaiswal, U. K. Kanike, M. W. Arshad, and S. Bhattacharya, “Role of AI in Decision Making and Its Socio-Psycho Impact on Jobs, Project Management and Business of Employees,” Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 5s, pp. 517–523, 2023.
40. I. Nallathambi, R. Ramar, D. A. Pustokhin, I. V. Pustokhina, D. K. Sharma, and S. Sengan, “Prediction of influencing atmospheric conditions for explosion Avoidance in fireworks manufacturing Industry-A network approach,” Environ. Pollut., vol. 304, no. 119182, p. 119182, 2022.
41. J. A. Alzubi, O. A. Alzubi, A. Singh, and T. Mahmod Alzubi, “A blockchain-enabled security management framework for mobile edge computing,” Int. J. Netw. Manage., vol. 33, no. 5, 2023.
42. J. A. Alzubi, O. A. Alzubi, M. Beseiso, A. K. Budati, and K. Shankar, “Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis,” Expert Syst., vol. 39, no. 4, 2022.
43. J. A. Alzubi, R. Jain, O. Alzubi, A. Thareja, and Y. Upadhyay, “Distracted driver detection using compressed energy efficient convolutional neural network,” J. Intell. Fuzzy Syst., vol. 42, no. 2, pp. 1253–1265, 2022.
44. K. Kaliyaperumal, A. Rahim, D. K. Sharma, R. Regin, S. Vashisht, and K. Phasinam, “Rainfall prediction using deep mining strategy for detection,” in 2021 2nd International Conference on Smart Electronics and Communication, 2021.
45. M. Lishmah Dominic, P. S. Venkateswaran, L. T. Reddi, S. Rangineni, R. Regin, and S. S. Rajest, “The synergy of management information systems and predictive analytics for marketing,” in Advances in Business Information Systems and Analytics, IGI Global, USA, pp. 49–63, 2023.
46. M. Sabugaa, B. Senapati, Y. Kupriyanov, Y. Danilova, S. Irgasheva, and E. Potekhina, “Evaluation of the prognostic significance and accuracy of screening tests for alcohol dependence based on the results of building a multilayer perceptron,” in Artificial Intelligence Application in Networks and Systems, Cham: Springer International Publishing, pp. 240–245, 2023.
47. M. Yuvarasu, A. Balaram, S. Chandramohan, and D. K. Sharma, “A Performance Analysis of an Enhanced Graded Precision Localization Algorithm for Wireless Sensor Networks,” Cybernetics and Systems, pp. 1–16, 2023.
48. N. Al-Najdawi, S. Tedmori, O. A. Alzubi, O. Dorgham, and J. A. Alzubi, “A Frequency Based Hierarchical Fast Search Block Matching Algorithm for Fast Video Video Communications,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 4, 2016.
49. N. Geethanjali, K. M. Ashifa, A. Raina, J. Patil, R. Byloppilly, and S. S. Rajest, “Application of strategic human resource management models for organizational performance,” in Advances in Business Information Systems and Analytics, IGI Global, USA, pp. 1–19, 2023.
50. O. A. Alzubi, I. Qiqieh, and J. A. Alzubi, “Fusion of deep learning based cyberattack detection and classification model for intelligent systems,” Cluster Comput., vol. 26, no. 2, pp. 1363–1374, 2023.
51. P. P. Dwivedi and D. K. Sharma, “Application of Shannon entropy and CoCoSo methods in selection of the most appropriate engineering sustainability components,” Cleaner Materials, vol. 5, no. 9, p. 100118, 2022.
52. P. P. Dwivedi and D. K. Sharma, “Assessment of Appropriate Renewable Energy Resources for India using Entropy and WASPAS Techniques,” Renewable Energy Research and Applications, vol. 5, no. 1, pp. 51–61, 2024.
53. P. P. Dwivedi and D. K. Sharma, “Evaluation and ranking of battery electric vehicles by Shannon’s entropy and TOPSIS methods,” Math. Comput. Simul., vol. 212, pp. 457–474, 2023.
54. P. P. Dwivedi and D. K. Sharma, “Selection of combat aircraft by using Shannon entropy and VIKOR method,” Def. Sci. J., vol. 73, no. 4, pp. 411–419, 2023.
55. P. S. Venkateswaran, M. L. Dominic, S. Agarwal, H. Oberai, I. Anand, and S. S. Rajest, “The role of artificial intelligence (AI) in enhancing marketing and customer loyalty,” in Advances in Business Information Systems and Analytics, IGI Global, USA, pp. 32–47, 2023.
56. P. Sindhuja, A. Kousalya, N. R. R. Paul, B. Pant, P. Kumar, and D. K. Sharma, “A Novel Technique for Ensembled Learning based on Convolution Neural Network,” in 2022 International Conference on Edge Computing and Applications, IEEE, pp. 1087–1091, 2022.

57. R. K. Gupta, “A study on occupational health hazards among construction workers in India,” Int. J. Enterp. Netw. Manag., vol. 12, no. 4, p. 325, 2021.
58. R. K. Gupta, “Adoption of mobile wallet services: an empirical analysis,” Int. J. Intellect. Prop. Manag., vol. 12, no. 3, p. 341, 2022.
59. S. Abukharis, J. A. Alzubi, O. A. Alzubi, S. Alamri, and T. O. Tim O\’Farrell, “Packet error rate performance of IEEE802.11g under Bluetooth interface,” Res. J. Appl. Sci. Eng. Technol., vol. 8, no. 12, pp. 1419–1423, 2014.
60. S. Kolachina, S. Sumanth, V. R. C. Godavarthi, P. K. Rayapudi, S. S. Rajest, and N. A. Jalil, “The role of talent management to accomplish its principal purpose in human resource management,” in Advances in Business Information Systems and Analytics, IGI Global,USA, pp. 274–292, 2023.
61. S. Samadi, M. R. Khosravi, J. A. Alzubi, O. A. Alzubi, and V. G. Menon, “Optimum range of angle tracking radars: a theoretical computing,” Int. J. Electr. Comput. Eng., vol. 9, no. 3, p. 1765, 2019.
62. S. Singh, S. S. Rajest, S. Hadoussa, A. J. Obaid, and R. Regin, Eds., “Data-driven decision making for long-term business success,” Advances in Business Information Systems and Analytics. IGI Global, USA, 2023.
63. S. Singh, S. S. Rajest, S. Hadoussa, and A. J. Obaid, “Data-Driven Intelligent Business Sustainability,” in Advances in Business Information Systems and Analytics,. IGI Global, USA, 2023.
64. A. Sholiyi, T. O’Farrell, O. Alzubi, and J. Alzubi, “Performance Evaluation of Turbo Codes in High Speed Downlink Packet Access Using EXIT Charts”, International Journal of Future Generation Communication and Networking, vol. 10, no. 8, 2017.
65. D. Srinivasa, N. Baliga, D. Devi, P. Verma, P. Selvam, and D. K. Sharma, “Identifying lung nodules on MRR connected feature streams for tumor segmentation,” in 2022 4th International Conference on Inventive Research in Computing Applications, 2022.
66. T. Chen, J. Blasco, J. Alzubi, and O. Alzubi “Intrusion Detection”. IET Publishing, vol. 1, no. 1, pp. 1-9, 2014.
67. V. Bansal, A. Bhardwaj, J. Singh, D. Verma, M. Tiwari and S. Siddi, "Using Artificial Intelligence to Integrate Machine Learning, Fuzzy Logic, and The IoT as A Cybersecurity System," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, Greater Noida, India, pp. 762-769, 2023.