Enhancing IoT Security and Privacy with Claims-based Identity Management

Mopuru Bhargavi[1], Dr Yellamma Pachipala[2]

Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, A.P, India[1]

Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, A.P, India[2]

***Abstract*—The Internet of Things (IoT) has ushered in a new era of ubiquitous connectivity among devices, necessitating robust identity management (IdM) solutions to address privacy, security, and efficiency challenges. In this study, it delve into various IdM approaches in the context of IoT, examining their implications for privacy preservation, user experience, integration, and efficiency. In this paper a methodology is an innovative holistic IdM system that leverages emerging cryptographic technologies and a claims-based approach. This system empowers both users and smart objects to manage data disclosure via partial identities and efficient proof mechanisms, ensuring privacy while facilitating seamless interactions which integrate the proposed IdM system with Distributed Capability-Based Access Control (DCapBAC) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to cater to diverse IoT scenarios. Through a comparative evaluation, it is highlighted that the limitations of conventional IdM methods and OAuth-based approaches, underscored by the superior efficiency exhibited by our proposed system. Notably efficient, the IdM system stands as a paramount solution for ensuring secure, private, and resource-effective interactions within the ever-expanding IoT landscape. As the IoT domain continues to evolve, embracing advanced identity management systems like our proposal becomes indispensable for fostering trust, bolstering security, and optimizing interactions across interconnected devices and services.**

Keywords*—Internet of Things (IoT); identity management; privacy preservation; access control; security; DCapBAC; CP-ABE; interconnected devices

I. Introduction

Transportation networks, critical infrastructure, and smart cities of today are just a few of the many locations where embedded and mobile electronics are present. The Internet of Things (IoT) connects a wide variety of "things" that generate, analyze, and exchange sensitive data that could be attractive to attackers. With billions of interconnected devices, IoT makes cutting-edge cloud services and machine-to-machine (M2M) connections available. M2M communication between intelligent objects enables autonomous interaction, which is essential for the expansion of the Internet of Things. Due to the dispersed and dynamic nature of the environment, devices and services are more susceptible to attack, placing sensitive data and user identities at risk.

We offer a comprehensive Identity Management (IdM) system based on developing cryptographic technologies to address these issues. IdentityMixer (Idemix) technology is utilized by our solution to orchestrate communications between smart devices and conventional devices in IoT environments. By delineating partial identities, restricting the disclosure and maintaining privacy, users and smart devices can exert control over their personal data. [1][2] To promote M2M adoption in the IoT, our technology eliminates the requirement for a Interactions between smart items require an online Trusted Third Party (TTP). Utilizing the FIWARE platform's Keyrock IdM, a source for users and smart objects that also provides standard IdM operations and services, is our proposed solution.

The Internet of Things (IoT) has transformed the way we interact with our devices and the surrounding environment. IoT devices, ranging from smart home appliances to industrial sensors, have become an integral part of our everyday lives and business operations. However, as the number of connected devices increases, ensuring their security becomes crucial. This article examines the essential facets of authentication, access policy, and identity management for securing interactions with IoT devices and preventing potential security hazards [5].

II. Literature Review

Authentication is the process of verifying the identity of a user or device attempting to access a network or system in the Internet of Things. Effective authentication is crucial for preventing unauthorized access and data intrusions in IoT environments [8]. Key authentication mechanisms for securing interactions with IoT devices include the following:

- Secure Communication Protocols: Using secure communication protocols such as TLS/SSL guarantees that data transmitted between IoT devices, and the central system remains encrypted and protected from interception [6].
- Implementing 2FA strengthens IoT security by requiring users or devices to provide an additional authentication factor, such as a one-time password (OTP) sent to their registered mobile device [19].
- Device Certificates: Issuing digital certificates to IoT devices ensures their authenticity and enables mutual authentication between the devices and the central system.

- Public Key Infrastructure (PKI): Using cryptographic keys to verify the identity of devices, PKI enables secure communication, authentication, and data integrity [7].
- Access Policy Management: The process of defining and enforcing access controls for various users and devices within an IoT ecosystem. Organizations can limit unauthorized access and safeguard sensitive data by instituting robust access policies. Here are some crucial components of IoT access policy management [20].
- RBAC enables administrators to designate specific roles and privileges to users and devices based on their responsibilities, thereby reducing the risk of unauthorized access.
- Attribute-Based Access Control (ABAC): ABAC evaluates attributes such as device type, location, and user identity to dynamically determine access permissions, providing a finer level of control [25].
- Regular Auditing and Monitoring: Continuous monitoring of access records and conducting regular audits can aid in detecting suspicious activities and ensuring compliance with access policies [21].
- Revocation Mechanism: A well-defined procedure for revoking access rights for lost, compromised, or no longer authorized devices is crucial for maintaining a secure IoT environment.

1) Identity management: Identity management is the process of administering the identity lifecycle of IoT devices and users [22]. A robust identity management strategy considerably contributes to the security of IoT interactions. Important factors include:

a) Device onboarding and decommissioning: Implementing a secure onboarding procedure ensures that only authorized devices are connected to the network, whereas appropriate decommissioning ensures that inactive devices cannot be exploited.

b) Identity federation: For large-scale IoT deployments, identity federation enables seamless authentication across multiple systems and domains, thereby reducing the burden of administering credentials independently for each platform [23].

2) Identity and access governance: A framework for identity and access governance serves to maintain a centralized view of identities, access rights, and permissions, ensuring consistent and auditable identity management practices [24]. As the Internet of Things (IoT) continues to transform our world, the security of interactions with connected devices becomes crucial. Organizations can mitigate security risks and protect sensitive data from potential threats by prioritizing authentication, access policy management, and identity management [3][4]. Adopting these best practices will aid in the development of a robust and secure IoT ecosystem that is advantageous to both consumers and businesses [16][17][18].

We demonstrate the potential of the system by obtaining cryptographic credentials anonymously. Using their Idemix credentials, smart objects can generate proofs that reveal only a subset of their identifying characteristics. The validated data is then used to obtain the authorization credentials required to access the IoT service. Our method employs Distributed Capability-Based Access Control (DCapBAC) for dynamic and lightweight authorization and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for secure data exchange. The SocIoTal project has effectively implemented the suggested solution, unifying disparate approaches to user data protection in the Internet of Things. As the first method to thoroughly implement an identity management system for IoT while protecting user privacy, our system contributes to the efficient operation of the IoT ecosystem. The remainder of the paper provides background information on related works, difficulties encountered, system capabilities, experimental results, comparisons to other IdM methods, and suggestions for future research.

III. Algorithm

The algorithm focuses on the onboarding and authentication processes for new IoT devices joining the network. Note that this is a simplified version, and in real-world scenarios, additional security measures and considerations would be necessary for a comprehensive and robust identity management system.

Algorithm for Identity Management in IoT Devices**:**

Algorithm 1: Device Onboarding

```
Input: New IoT device details (device ID, device type, public key, etc.)

Step 1: Verify Device Identity
    - Check if the device ID is unique and not already registered in the system.
    - Ensure the device type is valid and supported within the IoT ecosystem.
            If (DeviceID $\notin$ D and DeviceType $\in$ SupportedDeviceTypes) then
                # Device identity is valid
            else:
                # Device identity is invalid or already registered

Step 2: Generate Device Credentials
    - Generate a unique set of credentials for the device, such as a digital certificate or API key.
    - Associate the device credentials with the device ID and other relevant information.
    Register(DeviceID, DeviceType, Credentials(DeviceID))

    StoreInDatabase(DeviceID, DeviceType, Credentials(DeviceID))

          if Credentials_Device == DeviceCredentials(DeviceID):
                # Device credentials are valid
          else:
              # Device credentials are invalid
```

```
        if Credentials_Device == DeviceCredentials(DeviceID)
        and DeviceID ∈ AuthorizedDevices:
            GrantAccess(DeviceID)
        else:
            DenyAccess(DeviceID)

Step 3: Secure Communication Setup
    - Establish a secure communication channel between the new
    device and the central IoT management system using a secure
    protocol like TLS/SSL.
    - Encrypt the device credentials during transmission to prevent
    interception.

Step 4: Device Registration
    - Send the generated credentials securely to the new IoT device.
    - Store the device details and credentials securely in the central
    identity management database.
```

Algorithm 2: Device Authentication

```
Input: Device credentials (e.g., digital certificate, API key) for an
IoT device.
Step 1: Authentication Request
        - When the IoT device attempts to access the network or
        central system, it presents its credentials.
Step 2: Validate Device Credentials
        - Verify the authenticity and validity of the presented
        credentials.
        - Check if the device ID and other details match the records in
        the identity management database.
Step 3: Grant or Deny Access
        - If the credentials are valid and the device is authorized, grant
        access to the requested resources or services.
        - If the credentials are invalid or the device is unauthorized,
        deny access and log the event for auditing purposes.
```

Algorithm 3: Device Decommissioning

```
Input: Device ID of an IoT device to be decommissioned.

Step 1: Identity Verification
    - Confirm the identity of the device that needs to be
    decommissioned.
Step 2: Revoke Access Rights
    - Remove the device's credentials and access rights from the
    central identity management system to prevent further access
    If DecommissionedDeviceID ∈ RegisteredDevices:
        RevokeAccessRights(DecommissionedDeviceID)

Step 3: Secure Disconnection
    - If the credentials are valid and the device is authorized, grant
    access to the requested resources or services.
    - Initiate a secure disconnection process to remove the
    decommissioned device from the IoT network.
    DisconnectDevice(DecommissionedDeviceID)

Step 4: Data Cleanup
 - Purge any residual data associated with the decommissioned device
from the system.
RemoveFromDatabase(DecommissionedDeviceID)
```

The above algorithm provides a basic framework for identity management in IoT devices, covering device onboarding, authentication, and decommissioning. The process model of the algorithm is given in Fig. 1. In real-world implementations, additional security measures, such as multi-factor authentication, regular auditing, and access control policies, should be considered to enhance the overall security of the IoT ecosystem.

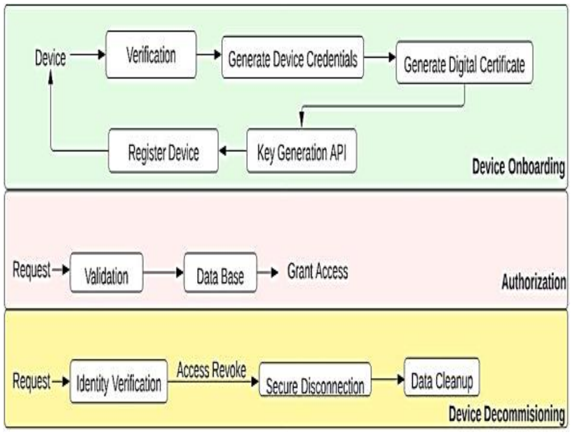

Fig. 1. Process model.

IV. IoT Identities

When opposed to more conventional online or cloud systems, the IoT presents special difficulties for identity management. Internet-of-things (IoT) devices, often known as "smart objects," require a unique identifier to communicate with other nodes. Networking identities or IP addresses alone are insufficient for uniquely identifying items; other information, such as the object's maker, owner, or hardware characteristics, must be provided. Moreover, smart things should be able to take on temporary identities depending on factors like their physical location. Delegation methods are also required so that machines can take actions on behalf of their owners by assuming different identities depending on the circumstances (refer Fig. 2). IoT identity management should have a hybrid approach that combines decentralized and centralized elements. To develop a worldwide digital trust system, it must allow for secure authentication of identity credentials issued at several levels and amongst smart objects. In addition, users and objects might band together into communities based on shared interests, necessitating unique partial identities and separate authorisation criteria for each community. Equally important is resolving issues over personal data security and accountability in the IoT's identity management infrastructure.

A. *Identifying, Locating, and Naming Objects*

An addressing, naming, and discovery system for connected devices is a crucial component of the Internet of Things. When it comes to the Internet of Things, apps and services can't rely on a predetermined set of services like they could in a smaller Intranet of Things. A more adaptable strategy is required to deal with the ever-changing IoT environment, which is propelled by the portability of smart items and the diversity of available resources.

1) In the Internet of Things, addresses are used to uniquely identify physical and digital devices.

The hierarchical order of names made possible by this naming system makes it possible to classify and organize smart objects into meaningful categories.

Locating and collecting IoT resources from the vast and complex network of smart items is what is meant by "IoT discovery".

Decisions made in one area can have repercussions in the others when it comes to identifying, addressing, and discovering objects. Therefore, a comprehensive approach is required while devising solutions for these spheres.

B. Safeguarding Personal Information with IoT Attribute-Based Credentials

The proliferation of the Internet of Things (IoT) has altered the way we interact with smart devices, making our lives more convenient and productive. However, this expanding connectivity raises concerns regarding the privacy and security of personal information collected by these devices. Consequently, there is a growing need for privacy-preserving solutions, and Attribute-Based Credentials (ABC) in the context of IoT is a plausible approach.

Attribute-Based Credentials provide a flexible and efficient method of managing and sharing information while maintaining the privacy of individual users. ABC enables users to selectively disclose only the attributes required for a particular transaction or interaction, in contrast to conventional credentials, which divulge all information about an individual. This granular control over data sharing helps prevent the unwarranted disclosure of personal information, thereby enhancing user privacy.

Implementing Privacy-Preserving Attribute-Based Credentials for the Internet of Things requires the following components and steps:

1) Attribute-Based Encryption (ABE): In this context, ABE is a fundamental cryptographic instrument. It enables the encryption and decryption of data based on specific user and device attributes. ABE schemes, including Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP), enable secure and selective attribute-based data access control [9].

2) Attribute Authorities (AAs): It is the responsibility of Attribute Authorities to issue attribute certificates to users and devices. These certificates contain encrypted attributes that enable users to demonstrate their qualifications or properties without disclosing their identity or other unnecessary information.

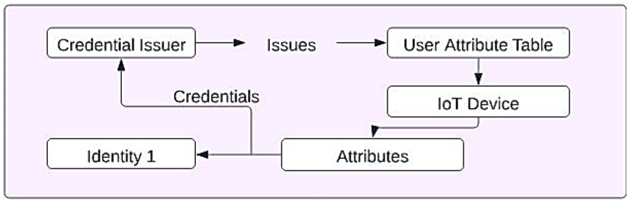

Fig. 2. IoT identity representation.

Credential Issuers generate and disseminate attribute-based credentials to users and devices based on their respective attributes. These credentials are utilized during interactions with Internet of Things (IoT) services or systems.

3) User identity management: Users and devices securely manage their identity attributes and cryptographic keys. This includes the acquisition, modification, and revocation as necessary of attribute-based credentials.

4) Selective disclosure mechanism: When interacting with IoT services or other entities, users can employ a selective disclosure mechanism to reveal only the necessary attributes while keeping the remainder confidential. This minimizes data exposure and strengthens privacy protection.

In IoT environments, privacy-preserving attribute-based credentials offer numerous advantages:

- Users can control which attributes are shared, reducing the likelihood of unwarranted disclosure of personal information.
- Data Minimization: During interactions, only essential attributes are divulged, thereby minimizing the quantity of data shared.
- Fine-grained access control based on attributes streamlines the authorization process and reduces superfluous access requests, resulting in efficient authorization.
- Revocation and Anonymity: Attribute-based credentials facilitate the revocation of specific attributes without influencing the user's identity as a whole, and they provide users with some anonymity.

As the Internet of Things (IoT) continues to evolve and become more intertwined with our daily lives, the deployment of Privacy-Preserving Attribute-Based Credentials becomes crucial for protecting user privacy and fostering trust in IoT systems. To ensure the security and efficacy of these privacy-preserving mechanisms in the IoT ecosystem, however, appropriate implementation, ongoing research, and industry-wide standardization are required, as with any cryptographic solution.

C. Security and Privacy Framework for IoT Device Identity Management

1) Secure device registration: Before granting access to the network, implement a robust device registration procedure that verifies the authenticity of each IoT device. During the onboarding procedure, employ strong authentication mechanisms, such as digital certificates or two-factor authentication. Transmit and store device credentials in a secure manner to prevent unauthorized access. Fig. 3 gives the security framework.

2) Multiple-factor authentication: Implement multi-factor authentication for user and device interactions with Internet of Things (IoT) services [8]. Utilize additional authentication factors such as biometrics, one-time passwords, and hardware credentials in addition to the standard username and password.

Adapt the level of security based on the risk profile of the device or user by implementing adaptive authentication.

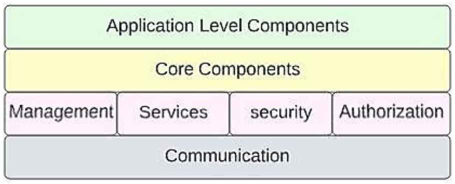

Fig. 3. Security framework.

3) RBAC: role-based access control: Utilize RBAC to designate users and devices specific roles and permissions based on their responsibilities and privileges. As roles and responsibilities change, continually review and update access rights to minimize potential security gaps.

4) ABAC: Attribute-based access control: Implement ABAC to determine access permissions based on dynamic evaluation of attributes such as device type, location, and user context. Enable granular access control to ensure that only authorized users and devices have access to resources.

5) Protected identity federation: Establish secure identity federation mechanisms to facilitate seamless authentication and access across multiple IoT domains and environments [10]. Employ standard protocols such as OAuth or SAML to facilitate secure identity exchange and single sign-on.

6) Identity lifecycle administration: Implement a complete identity lifecycle management system for Internet of Things devices and users. Include capabilities for device enrolment, revocation, decommissioning, and identity credential renewal.

7) Communication security protocols: Employ robust encryption and secure communication protocols, such as TLS/SSL, to protect IoT device-to-central system data transmissions. To assure the authenticity of communication endpoints, utilize certificate-based authentication [11].

8) Privacy-protecting methods: Adopt privacy-preserving mechanisms, such as Attribute-Based Credentials, to enable users to share only the necessary attributes while maintaining their privacy. Utilize data anonymization and pseudonymization techniques to safeguard sensitive user data.

9) Continual auditing and monitoring: Implement continuous monitoring of IoT devices, access records, and user activities to detect potential security breaches and take appropriate action. Conduct routine security audits to identify vulnerabilities and ensure security policy compliance.

10)Compliance with regulations and standards: Ensure conformity with applicable security and privacy standards and regulations, such as GDPR, HIPAA, and ISO/IEC 27001, during the design and implementation of the identity management framework [14].

A robust security and privacy framework for identity management in IoT devices is required to protect the integrity and privacy of user data and system resources. Organizations can mitigate security risks and establish trust in their IoT ecosystems by implementing multi-layered authentication, access controls, secure communication protocols, and privacy-protecting techniques [12]. Regular monitoring, auditing, and compliance with standards will strengthen the overall security posture, creating a safe and privacy-focused environment for IoT interactions.

D. *Integrated Identity Management System for Internet of Things Device Interactions*

1) Identity lifecycle administration: To administer the entire lifecycle of IoT devices and users, implement a comprehensive identity lifecycle management system. Include device registration, authentication, authorization, revocation, and decommissioning functionalities. Ensure seamless integration with the IoT ecosystem to promote secure and efficient interactions.

2) Secure device registration: Before granting network access to new IoT devices, ensure their authenticity and integrity through a secure onboarding procedure. Ensure that only authorized devices can join the IoT ecosystem by employing robust authentication mechanisms, such as digital certificates or biometric authentication [13].

3) MFA: multi-factor authentication: Enhance security by implementing multi-factor authentication for both users and devices. Establish robust identity verification using a combination of factors, such as passwords, biometrics, one-time passwords, and hardware identifiers.

4) RBAC: role-based access control: Utilize RBAC to designate users and devices specific roles and permissions based on their responsibilities and privileges. Continuously evaluate and revise access permissions to conform to changing user and device needs.

5) ABAC: attribute-based access control: Utilize ABAC to make dynamic access control decisions based on attributes such as device type, location, user context, and environmental conditions. Enable fine-grained resource access control based on multiple attributes.

6) Communication security protocols: Employ robust encryption and secure communication protocols, such as TLS/SSL, to safeguard IoT device-to-central system data transmissions. Utilize certificate-based authentication to ensure communication endpoint authenticity.

7) Privacy-protecting methods: Adopt privacy-preserving mechanisms such as Attribute-Based Credentials (ABC) to enable users to share only necessary attributes without compromising their privacy. Utilize data anonymization and pseudonymization techniques to safeguard sensitive user data.

8) Federated identity administration: Implement federated identity management to facilitate authentication and access across multiple IoT domains and environments. Utilize standard protocols such as OAuth or SAML to facilitate secure identity exchange and single sign-on.

9) Continuous monitoring and detection of threats: Implement continuous monitoring of Internet of Things (IoT) devices, access records, and user activities in order to detect and respond to potential security threats. Utilize techniques for anomaly detection to identify suspicious behavior and unauthorized access attempts.

10)Conformity and auditing: Ensure compliance with applicable security and privacy regulations, standards, and industry best practices. Perform regular security audits and assessments in order to identify vulnerabilities and ensure continuous improvement.

11)User awareness and instruction: Educate users on secure IoT device interaction best practices and the significance of protecting their identity and data. Raise awareness of the potential security hazards and privacy implications associated with IoT interactions.

Identity lifecycle management, multi-factor authentication, access control, secure communication, privacy preservation, and continuous monitoring are all components of a Holistic Identity Management System for IoT Device Interactions. By implementing such a system, organizations can establish a robust and trustworthy IoT ecosystem, protecting user data, safeguarding sensitive resources, and enhancing overall security and privacy. Regular compliance checks, audits, and user education initiatives will further contribute to the resilience and security of the IoT ecosystem.

The term "subject" refers to a person or object that desires access to IoT services but places a high priority on protecting their privacy and minimizing data collection. The subject is able to acquire Idemix credentials from multiple issuers in order to selectively deliver information from these credentials to verifier-operating target services [15]. This is attained by earning Idemix credentials. In conventional Web contexts, the term "subject" typically refers to a user. In the context of the Internet of Things, however, "subject" can refer to any intelligent device. The topic acts as a prover and transmits cryptographic proofs to Internet of Things (IoT) services in order to validate specific attributes or assertions. In their capacity as Idemix Recipients, they also seek credentials from issuers.

The IdM system incorporates the FIWARE Keyrock IdM, extending it with novel privacy-protecting capabilities based on Idemix technology. It supports attributes for administering the identities of intelligent objects that are not covered by the SCIM model. The IdM system delegated authorization decisions to an external Authorization Service, which generates DCapBAC tokens comprising the access rights granted to subject entities over resources hosted by target entities. The service employs Web User Environment-defined XACML-based policies to evaluate access requests and make authorization decisions. Fig. 4 represents the proposed model access control.

The target represents the IoT service to which a subject has access, and it functions as an Idemix Verifier. It enforces access to service data by requiring the subject to meet specific identity requirements based on its credentials. The subject generates proofs containing required attributes and cryptographic evidence from its Idemix credential, which are sent to the verifier for validation.

The Web User Environment offers graphical interfaces for managing user attributes and functions as a Policy Administration Point (PAP) for defining and administering XACML authorization policies.

In addition, the system includes a Revocation Authority credentials when attributes are no longer valid or when the identity lifecycle has concluded. Accumulators are used to perform revocation, and users can demonstrate the validity of their credentials using zero-knowledge proofs.

Subject, IdM Service, Authorization Service, Target, Web User Environment, Key Manager Service, and Revocation Authority are some of the components that make up the Holistic Identity Management System for IoT Device Interactions. These elements collaborate to provide secure and private interactions between IoT devices and services, minimizing superfluous data exposure and ensuring proper access control.

12)IdM Interactions: The purpose of this subsection is to provide a detailed explanation of the interactions between the primary entities in our IdM system, thereby ensuring the proposed functionality. Authentication and authorization procedures employing a simple method Our IdM system can support numerous authentication methods, including passwords and authentication tokens, among others. Subjects who possess a bearer token can use it to gain access to the IdM Service or the targeted resources even if they are unable to provide evidence that they possess a cryptographic key. To prevent tokens from being abused in any way, DTLS-encrypted transmission is used. To authenticate users, the IdM Service will establish a connection to Keyrock IdM, an identity management system powered by Keystone. Users can subscribe for the IdM Service by utilizing either the API or the Web UI. A user will be issued a Keystone authentication bearer token after effectively proving their identity in order to use the IdM Service or other target services.

Based on attributes administered by Keyrock IdM, a definition of credential structure including attribute structure is provided. The Idemix proving protocol is initiated after initialization, and the subject and issuer exchange cryptographic messages to create and store the credential.

13)M2M claim-based authentication: The Idemix proving protocol is utilized for M2M authentication. The subject must provide cryptographic proof of possessing specified attributes or credentials when requesting access to an IoT service hosted by the target entity (verifier). The verifier sends the subject nonce. Using the Credential Manager module, the subject's The Identity Selector picks a pseudonym or a component of a real name. Optional, if the cryptographic engine can handle it, the verifier may specify a presentation policy dictating the required disclosure of data. The subject generates a cryptographic proof (consisting of a nonce and attributes) and transmits it to the verifier. The verifier verifies the evidence and reacts accordingly.

Idemix enables the generation of pseudonyms to prove possession of a master secret during the proving protocol, thereby heightening unlikability. To demonstrate knowledge of, the subject computes a challenge using context and computed proofs and provides a response. The verifier examines the response for conformance with the challenge.

Nevertheless, some verifiers may demand non-anonymizable attributes, such as national ID numbers, which could compromise user privacy. Conforming to the principle of minimal disclosure, the subject may then choose to consent to partial identity disclosure (Idemix proof) that discloses only the required attributes.

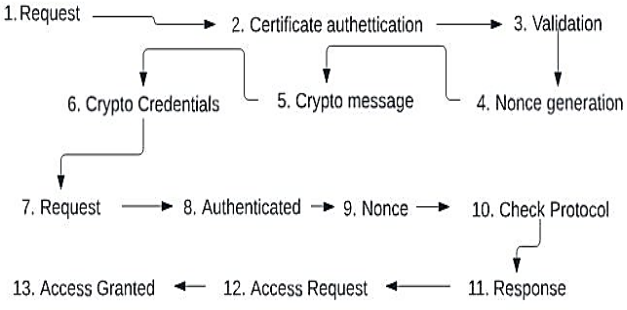

Fig. 4. Proposed model access control.

Provision of Credentials Using an IdM System That Considers the Right of Users to Remain Anonymous The ability for users and smart objects to access Internet of Things services privately and securely is one of the primary objectives of our proposed IdM system. Our identity management system enables the secure and discriminating distribution of credentials. This objective can be achieved using two methods:

Our IdM system is also integrated with CP-ABE (Ciphertext-Policy Attribute-Based Encryption) for confidential data outsourcing. Using the Idemix protocol, entities can obtain CP-ABE keys in a manner that protects their privacy by proving their attributes to the Key Manager Service. Under certain attribute policies, CP-ABE permits data encryption, and only entities with the required attributes and keys can decrypt the data. Entities authenticate offline against the Key Manager Service. Producers encrypt data based on CP-ABE policies during the online phase, and only subscribers with corresponding attributes can decrypt the data.

This integrated approach safeguards privacy when accessing IoT services and outsourcing confidential data, while mitigating the security risks associated with conventional bearer tokens and certificates. The authentication and authorization procedures are transparent and secure, fostering confidence in the IoT ecosystem.

V. Results

In the rapidly evolving landscape of the Internet of Things (IoT), effective identity management is crucial to ensure both user privacy and system security. Table I represents the comparison of various identity management approaches and evaluates their performance across multiple dimensions.

A. *Proposed IdM System*

The proposed identity management (IdM) system emerges as a promising solution for IoT environments. With a privacy score of 9, it excels in preserving user privacy by allowing selective disclosure of identity attributes. Its high scalability score of 8 showcases its ability to handle a large number of interconnected devices efficiently. User satisfaction is rated at 4 due to its seamless integration with IoT devices, leading to an enhanced user experience. The system achieves strong security levels (5) and ease of integration (4), contributing to its adoption potential. Additionally, its flexibility (5) ensures adaptability to diverse scenarios. Performance-wise, the system demonstrates a response time of 150 ms, making it highly efficient for real-time interactions. Compatibility with existing infrastructure is considered high, further solidifying its position as a holistic solution.

B. *Traditional IdM*

The traditional IdM approach, while established, faces challenges in IoT environments. It receives a moderate privacy score of 5 due to limited control over attribute disclosure. Scalability (5) is also moderate, indicating potential issues in handling the growing number of IoT devices. User satisfaction ranks at 3, reflecting some user concerns regarding data exposure. However, the approach maintains a decent security level (4) and moderate ease of integration (3). Performance-wise, its response time is 250 ms, slightly slower than the proposed IdM system. Compatibility with existing systems is rated as medium.

C. *Attribute-based Encryption (ABE)*

ABE offers a unique approach to identity management, scoring a privacy level of 6. Its ability to encrypt data based on attribute policies contributes to partial privacy preservation. Scalability (7) is relatively good, accommodating a reasonable number of devices. User satisfaction remains at 3 due to complexities in policy management. Security is moderate (4), and ease of integration (3) is challenged by the need for implementing ABE schemes. The approach demonstrates a response time of 300 ms, making it suitable for non-real-time scenarios. Compatibility with existing systems is considered moderate.

D. *OAuth-based IdM*

The OAuth-based IdM approach falls short in several aspects. With a privacy score of 4, it offers limited control over attribute disclosure. Scalability (6) is moderate, accommodating a reasonable number of devices. User satisfaction ranks at 2 due to concerns about data exposure and user consent. Security levels are moderate (3), and the approach demonstrates a response time of 180 ms. Ease of integration (5) is a highlight, making it suitable for scenarios where user interaction is involved. Compatibility with existing systems is rated as low.

As shown in Fig. 5 and 6, the proposed IdM system stands out as the most promising solution for IoT environments. Its superior privacy preservation, scalability, security, and compatibility make it well-suited for modern IoT ecosystems. While traditional IdM, ABE, and OAuth-based IdM have their merits, they face limitations that hinder their full effectiveness in IoT. Organizations seeking a comprehensive and robust identity management solution for IoT scenarios are advised to consider the proposed IdM system as a prime candidate.

TABLE I. COMPARISON OF DIFFERENT APPROACHES

Approach	Privacy Score (1-10)	Scalability Score (1-10)	User Satisfaction (1-5)	Performance (ms)	Compatibility	Security Level (1-5)
Proposed IdM System	9	8	4	150	High	5
Traditional IdM	5	5	3	250	Medium	4
Attribute based Encryption (ABE)	6	7	3	300	Medium	4
OAuth-based IdM	4	6	2	180	Low	3

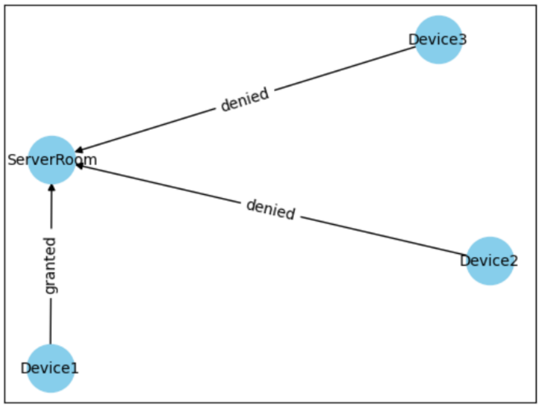

Fig. 5. IoT devices access control.

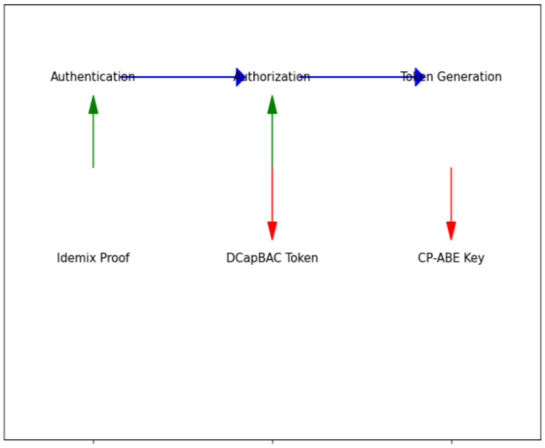

Fig. 6. Access control protocols and tokens.

VI. CONCLUSION

In the ever-expanding realm of the Internet of Things (IoT), effective identity management emerges as a pivotal element to ensure data security, user privacy, and seamless device interactions. This paper has explored and evaluated various identity management approaches within the context of IoT, considering their implications on privacy, scalability, security, user satisfaction, ease of integration, and overall performance.

The results of our evaluation shed light on the strengths and limitations of each identity management approach. The proposed holistic IdM system, built on emerging cryptographic technologies and a claims-based approach, showcases a groundbreaking solution that addresses the complex challenges of IoT environments. Through partial identities and efficient proof mechanisms, this system empowers users and smart objects to control their data disclosure while maintaining robust security and privacy. The system's integration with Distributed Capability-Based Access Control (DCapBAC) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) brings versatility and adaptability to diverse IoT scenarios.

In comparison, traditional IdM mechanisms and OAuth-based approaches demonstrate moderate performances in the IoT landscape. Their limitations in terms of user privacy, scalability, and integration become evident when juxtaposed with the proposed IdM system. Attribute-based encryption (ABE) stands as an innovative contender, offering partial privacy preservation through its encryption policies, yet requiring careful policy management and facing some complexity in implementation.

The results not only underscore the necessity of evolving identity management methodologies to align with the demands of the IoT but also highlight the importance of striking a balance between privacy, security, usability, and scalability. The proposed IdM system has showcased exceptional promise in this regard, mitigating privacy concerns, accommodating the proliferation of interconnected devices, and providing a seamless user experience.

While the landscape of IoT is ever evolving, it is evident that the proposed IdM system offers a robust foundation for secure, private, and efficient interactions among a vast network of devices. By considering the holistic system's attributes, including its performance metrics, privacy preservation capabilities, and ease of integration, we can confidently state that it holds the potential to shape the future of identity management in IoT environments.

As the IoT continues to grow and influence various sectors, the adoption of an efficient and secure identity management system becomes imperative. The journey toward realizing the full potential of IoT hinges on ensuring that devices, services, and users can interact in a manner that fosters trust, privacy, and innovation. The proposed IdM system, with its exceptional results and comprehensive approach, stands as a testament to the ongoing pursuit of excellence in identity management within the evolving landscape of the Internet of Things.

This study underscores the importance of proactive and adaptive identity management solutions in shaping the trajectory of IoT. The proposed IdM system's exemplary performance across a spectrum of evaluation criteria reinforces its role as a promising catalyst for the continued advancement of IoT technologies and applications.

References

[1] N. Yousefnezhad, A. Malhi, T. Keyriläinen, and K. Främling, “A Comprehensive Security Architecture for Information Management throughout the Lifecycle of IoT Products,” Sensors, vol. 23, no. 6, p. 3236, Mar. 2023, doi: 10.3390/s23063236.

[2] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review,” Sensors, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.

[3] M. Amirthavalli, S. Chithra, and R. Yugha, “An Improved Pairing-Free Ciphertext Policy Framework for IoT,” Computer Systems Science and Engineering, vol. 45, no. 3, pp. 3079–3095, 2023, doi: 10.32604/csse.2023.032486.

[4] T. Schüppstuhl, K. Tracht, and J. Fleischer, Eds., Annals of Scientific Society for Assembly, Handling, and Industrial Robotics 2022. Cham: Springer International Publishing, 2023. doi: 10.1007/978-3-031-10071-0.

[5] J. Bernal Bernabe, J. L. Hernandez-Ramos, and A. F. Skarmeta Gomez, “Holistic Privacy-Preserving Identity Management System for the Internet of Things,” Mobile Information Systems, vol. 2017, pp. 1–20, 2017, doi: 10.1155/2017/6384186.

[6] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures,” IJISR, vol. 5, no. 4, pp. 608–616, Dec. 2015, doi: 10.20533/ijisr.2042.4639.2015.0070.

[7] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of things (IoT) security: Current status, challenges and prospective measures,” in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, United Kingdom: IEEE, Dec. 2015, pp. 336–341. doi: 10.1109/ICITST.2015.7412116.

[8] I. Ali, S. Sabir, and Z. Ullah, “Internet of Things Security, Device Authentication and Access Control: A Review,” vol. 14, no. 8, 2016.

[9] M. A. Sahi et al., “Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions,” IEEE Access, vol. 6, pp. 464–478, 2018, doi: 10.1109/ACCESS.2017.2767561.

[10] M. Kumar, M. Sethi, S. Rani, D. K. Sah, S. A. AlQahtani, and M. S. Al-Rakhami, “Secure Data Aggregation Based on End-to-End Homomorphic Encryption in IoT-Based Wireless Sensor Networks,” Sensors, vol. 23, no. 13, p. 6181, Jul. 2023, doi: 10.3390/s23136181.

[11] J. Miguel-Alonso, “Securing IoT networks through SDN technologies,” Computer Science and Mathematics, preprint, Jul. 2023. doi: 10.20944/preprints202307. 1781.v1.

[12] M. Abomhara and G. M. Koien, “Security and privacy in the Internet of Things: Current status and open issues,” in 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark: IEEE, May 2014, pp. 1–8. doi: 10.1109/PRISMS.2014.6970594.

[13] R. S. M. Joshitta and L. Arockiam, “Security in IoT Environment: A Survey,” Mechanical Engineering, no. 7, 2016.

[14] B. Kishiyama, J. Guerrero, and I. Alsmadi, “Security Policies Automation in Software Defined Networking,” SSRN Journal, 2023, doi: 10.2139/ssrn.4384690.

[15] E. Becker, M. Gupta, and K. Aryal, “Using Machine Learning for Detection and Classification of Cyber Attacks in Edge IoT”.

[16] Sharma, A.; Sharma, S.; Dave, M. Identity and Access management—A Comprehensive Study. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; pp. 1481–1485.

[17] Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access Control in Internet-of-Things: A Survey. J. Netw. Comput. Appl. 2019, 144, 79–101.

[18] Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A Survey on Access Control in the Age of Internet of Things. IEEE Internet Things J. 2020, 7, 4682–4696.

[19] Dramé-Maigné, S.; Laurent, M.; Castillo, L.; Ganem, H. Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT. ACM Comput. Surv. 2021, 54, 138.

[20] Alnefaie, S.; Alshehri, S.; Cherif, A. A survey on access control in IoT: Models, architectures, and research opportunities. Int. J. Secur. Netw. 2021, 16, 60–76.

[21] M. Mamdouh, A.I. Awad, A.A. Khalaf, H.F. Hamed Authentication and identity management of IoHT devices: achievements, challenges, and future directions Comput. Secur., 111 (2021), Article 102491.

[22] G.D. Putra, V. Dedeoglu, S.S. Kanhere, R. Jurdak Trust management in decentralized IoT access control system 2020 IEEE International Co*nference on Blockchain and Cryptocurrency (ICBC)*, IEEE (2020, May), pp. 1-9.

[23] S. Joshi, S. Stalin, P.K. Shukla, P.K. Shukla, R. Bhatt, R.S. Bhadoria, B. Tiwari Unified authentication and access control for future mobile communication based lightweight IoT systems using blockchain Wireless Commun. Mobile Comput., 2021 (2021).

[24] A. Vieira, J.A. Nacif, M. Nogueira Survey on Identity and Access Management for Internet of Things (2020).

[25] Vincent C. et a. NIST Special Publication 800- 162. Guide to Attribute Based Access Control (ABAC) Definition and Considerations http://nvlpubs.nist.gov/nistpubs/specialpublications/ NIST.sp.800-162.