International Journal of Advanced Computing and Mechanical Systems (IJACM)
E-ISSN No.: xxxx-xxxx www.ijacm.com
Volume Number: 1 **Issue Number:** 1 **pp:** 8- 15 **Publication Month:** Dec-2025

Entity-Driven Design for Secure Identity Administration

Dinesh K[1,*], Uma Mahesh[2], T Naresh[2]
[1]*Research Scholar, Department of ECE, P.K. University, Shivpuri (M.P), India*
[2]*Assistant Professor, Department of ECE, P.K. University, Shivpuri (M.P), India*
***Corresponding Author*:** dkaranam24@gmail.com

ABSTRACT

Access to digital services requires entities, such as users or software services, to establish their identities before interacting with service providers. Conventional identity management systems typically maintain separate identity records for each application, often resulting in multiple accounts for the same entity within a single service provider. When identical personally identifiable information and attributes are reused across platforms, these fragmented records can be correlated, increasing the risk of identity exposure and privacy breaches. This work presents an entity-centric identity management model tailored for cloud environments, designed to enhance privacy and reduce unnecessary information disclosure. The proposed approach is founded on two core components. The first is anonymous identification, which enables entities to interact with cloud services based on predefined privacy preferences without revealing their true identities. The second component introduces active bundles, which encapsulate personally identifiable information, usage policies, and an embedded execution environment responsible for enforcing privacy constraints. These bundles autonomously apply protection mechanisms to safeguard sensitive data, even when deployed on untrusted platforms. The proposed model offers several advantages, including reduced dependence on external identity providers, controlled disclosure of identity attributes to service providers, and secure utilization of identity data in untrusted cloud environments. By integrating privacy-enhancing technologies such as zero-knowledge proofs, the framework provides a robust and flexible solution for privacy-aware identity management in modern cloud-based systems.

Keywords: Entity-Centric Identity Management, Anonymous Identification, Active Bundles, Privacy Preservation

I. INTRODUCTION

1.1 Managing Individual Identities

An individual's identity is defined by a collection of personal characteristics and attributes that distinguish one entity from another. The act of assigning a name, number, or symbol to uniquely distinguish an entity is referred to as identification [1]. In digital environments, identification plays a crucial role in enabling secure interactions between entities and service providers (SPs). To successfully complete authentication with a service provider, an entity must present a unique identifier that allows the SP to verify the legitimacy of the request. Through this process, the SP determines whether the requesting entity is indeed who it claims to be [2]. In cyberspace, it is common for a single individual or organization to possess multiple identities across different platforms and services. Identity Management (IDM) systems are designed to manage these multiple digital identities efficiently, while also determining how and when personal information should be disclosed to obtain a service [3].

doi: https://doi.org/10.5281/zenodo.18212728

Identity management systems serve several important functions. First, they establish identities by associating identifiers with existing real-world entities. Second, they assign attributes that describe an entity's defining features. Third, IDM systems monitor and log access to sensitive data, enabling accountability and auditability. Finally, IDM solutions support scheduled deletion of identity-related data, ensuring that personal information becomes permanently inaccessible after a defined period [2], [4]. In the authentication scenario illustrated in Fig. 1, personally identifiable information (PII) is used to authenticate a user requesting access to a service. While the service provider requires PII to accurately identify the user, the user may be reluctant to disclose sensitive personal details. The fundamental challenge lies in deciding what information should be disclosed, to whom, and through which mechanism, without compromising privacy [5].

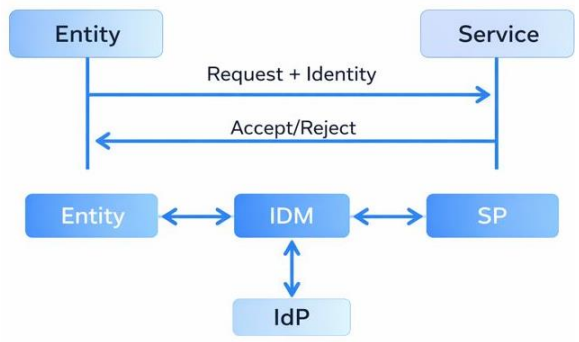

Figure 1: Authentication process using third-party identity management

IDM systems are widely used by collaborative environments to determine the identity of users or services. As outlined in [3], such systems typically involve multiple components, including an Identity Provider (IdP), which issues and manages identities, and service providers that rely on these identities to grant access. Governments, financial institutions, and other trusted organizations often act as IdPs, issuing credentials that enable secure transactions [6]. The real-world entity whether a person or object is represented digitally using identifiers such as names, dates of birth, or national identification numbers [1].

To ensure uniqueness, service providers may request identifiers to validate specific claims about an entity. Authentication may rely on information known to both the entity and the SP, information verified by an IdP, or biometric attributes such as fingerprints or facial features [7]. These mechanisms help strengthen trust but also raise privacy concerns, particularly in cloud-based systems. In cloud computing, privacy refers to the ability of users or organizations to control how their data is stored, accessed, and shared. Cloud service providers are expected to follow strict policies governing the collection, storage, and dissemination of user data [4], [8]. However, ensuring the confidentiality of sensitive information in the cloud remains a significant challenge at both individual and organizational levels. Users often have limited visibility into how their data is managed or who can access it [9].

Cloud service providers store data on behalf of individuals, enterprises, and governments, introducing privacy and security risks due to outsourcing. Trusting external providers involves inherent risk, as providers may not always act in the best interest of data owners [4]. Risks include high potential damage from single data breaches and exposure arising from multi-tenant environments where multiple users share the same infrastructure [10]. Key concerns include reliance on SPs for data access, the difficulty of establishing trust without auditing mechanisms, and conflicts arising from shared resources.

doi: https://doi.org/10.5281/zenodo.18212728

Traditional cloud-based identity management follows an application-centric model [5], where each application maintains its own user database. As a result, organizations often maintain multiple accounts across different SPs or even within the same provider offering multiple services. During service registration, users are required to disclose PII such as names, email addresses, and contact numbers, creating digital footprints that can be correlated across platforms [5], [11]. If not adequately protected, this information can be exploited for unauthorized tracking or identity theft [4].

In cloud environments, responsibility for data privacy ultimately lies with the data owner. However, enforcing privacy without technological safeguards is impractical. Cloud service requests must include identity and authorization information [6], increasing the risk of over-disclosure. To address these challenges, we propose an entity-centric identity management model, where the data owner controls all disclosure decisions rather than the service provider. The conceptual difference between application-centric and entity-centric IDM models is illustrated in Fig. 2. In this work, we present a structured approach for designing and implementing an entity-centric IDM system that enables privacy-preserving identity usage in cloud environments.

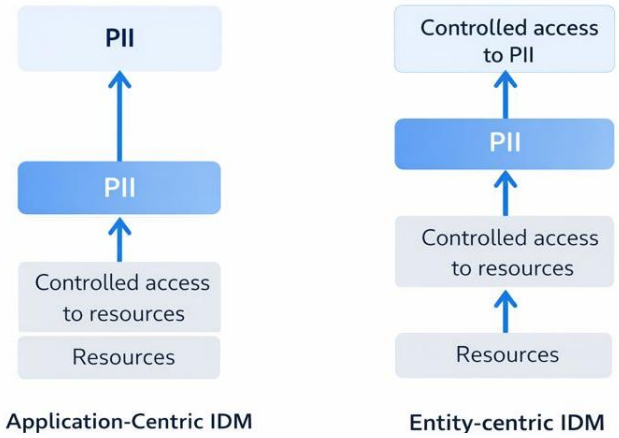

Figure 2: Comparison between application-centric and entity-centric identity management models

II. LITERATURE REVIEW

This section reviews representative approaches and technologies related to Identity Management (IDM), with a focus on privacy preservation, user control, and secure identity usage in distributed and cloud environments. Three prominent identity management solutions are discussed, followed by an overview of the Active Bundle scheme and its mobile-agent-based implementation.

2.1 PRIME: Privacy and Identity Management for Europe

PRIME (Privacy and Identity Management for Europe) is a privacy-oriented IDM framework that enables users to obtain and use anonymous credentials while maintaining control over their personal information [7]. The system allows users to acquire claims endorsed by Identity Providers (IdPs) through a user agent interface that manages interactions with Relying Parties (RPs). PRIME employs an identity mixing mechanism based on selective disclosure protocols, allowing users to reveal only specific attributes required for a transaction while keeping other identity details hidden. The credentials issued within PRIME are digitally signed using public key infrastructure, ensuring authenticity and integrity. While PRIME offers strong privacy guarantees, it introduces deployment

doi: https://doi.org/10.5281/zenodo.18212728

challenges, as both service providers and user agents must adopt PRIME-specific middleware. This requirement limits interoperability and poses obstacles to widespread standardization [7].

2.2 Microsoft CardSpace

Microsoft CardSpace is an identity management solution integrated into the Windows platform, designed to manage users' digital identities through virtual identity cards known as InfoCards [8]. Each InfoCard represents a set of claims, which may include identifiers such as usernames, addresses, or other personal attributes. These claims are packaged into security tokens that can be verified by service providers. When accessing a CardSpace-enabled application or website, the user selects an InfoCard, and CardSpace communicates with an IdP to obtain a digitally signed XML-based security token. This token is then forwarded to the requesting service for authentication. Although CardSpace simplifies identity handling, it has been criticized for placing excessive trust responsibility on users. Many users do not adequately verify service provider certificates, potentially exposing themselves to security risks. Furthermore, CardSpace relies heavily on the security of the IdP. If a user's credentials are compromised or an authentication session is hijacked, all participating relying parties within that session become vulnerable. This single point of failure presents a significant security concern [8].

2.3 OpenID

OpenID is a decentralized authentication protocol that enables users to maintain a single digital identity that can be reused across multiple online services [9]. By using an OpenID, users can reduce the number of credentials they must manage, thereby improving usability and convenience. OpenID providers authenticate users and request user consent before sharing identity information with relying parties. During authentication, the OpenID provider verifies the user often using a password and confirms whether the relying party should be granted access to the requested identity attributes. Once verified, the relying party accepts the authentication and grants access accordingly. Despite its advantages, OpenID has been widely criticized for its susceptibility to phishing and social engineering attacks. Malicious websites can impersonate legitimate OpenID providers, tricking users into revealing their credentials [10], [18]. This vulnerability has earned OpenID the reputation of being highly attractive to attackers.

2.4 Review of the Active Bundle Scheme

The Active Bundle (AB) paradigm was introduced as a mechanism for securely transporting sensitive data, associated metadata, and executable code in the form of a virtual machine [11]. The primary objective of Active Bundles is to protect sensitive information against unauthorized access, misuse, and improper dissemination, even when deployed on untrusted hosts. An Active Bundle contains metadata that defines its security properties, including data origin, integrity requirements, access permissions, dissemination constraints, encryption algorithms, trust server identifiers, and lifetime parameters [11], [12]. The embedded virtual machine enforces these policies autonomously. Core functions of the AB virtual machine include enforcing access control through mechanisms such as apoptosis, evaporation, and decoy generation; regulating dissemination policies; and verifying the integrity of the bundle. Although Active Bundles are designed to mitigate data leakage on malicious hosts, their effectiveness depends on the host's ability to correctly execute the virtual machine. This assumption defines the threat model and represents a critical limitation of the approach.

doi: https://doi.org/10.5281/zenodo.18212728

2.5 Mobile Agent–Based Active Bundle Prototype

A prototype implementation of the Active Bundle framework has been developed using the mobile agent paradigm and the Java Agent Development Framework (JADE) [14]. The prototype incorporates multiple specialized agents, including the Security Services Agent (SSA), Trust Evaluation Agent (TEA), and Audit Services Agent (ASA), as defined in the AB-TTP architecture. The system consists of four main components organized into separate bundles: the Active Bundle Coordinator (ABC), Active Bundle Destination (ABD), Directory Facilitator (DF), and the Active Bundle itself. The ABC manages service registration and discovery using the JADE Directory Facilitator, allowing agents to dynamically locate and communicate with one another. The ABC acts as the primary interface between users and the system. Users provide data, metadata, and movement instructions, which are used to construct Active Bundles containing both content and policy-enforcing virtual machines. The ABD functions as a host environment responsible for receiving and executing Active Bundles. The SSA maintains security-related information, including encryption keys and minimum trust requirements. The TEA evaluates host trustworthiness in response to SSA queries [15], while the ASA records audit information generated during bundle execution for later inspection by authorized parties.

2.6 Active Bundle Operation and Activation

Active Bundle behavior follows a defined execution lifecycle, beginning with construction and ending with activation, as illustrated in Figure 3. During construction, the ABC encrypts sensitive data and metadata using keys provided by the SSA. Separate keys are used for encryption and digital signatures to prevent unauthorized modification and re-signing of data. Upon arrival at a host, the Active Bundle initiates activation by querying the SSA to retrieve security parameters and assess host trustworthiness. If the host satisfies the minimum trust threshold, the bundle proceeds with data decryption. Otherwise, protective actions such as apoptosis are triggered. Integrity verification is performed by comparing computed hash values with signed hashes to ensure data authenticity. Finally, the Active Bundle reports its activities to the ASA, including details of host interaction and execution outcomes. Throughout its lifecycle, the Active Bundle strictly enforces privacy and dissemination policies defined by its owner.

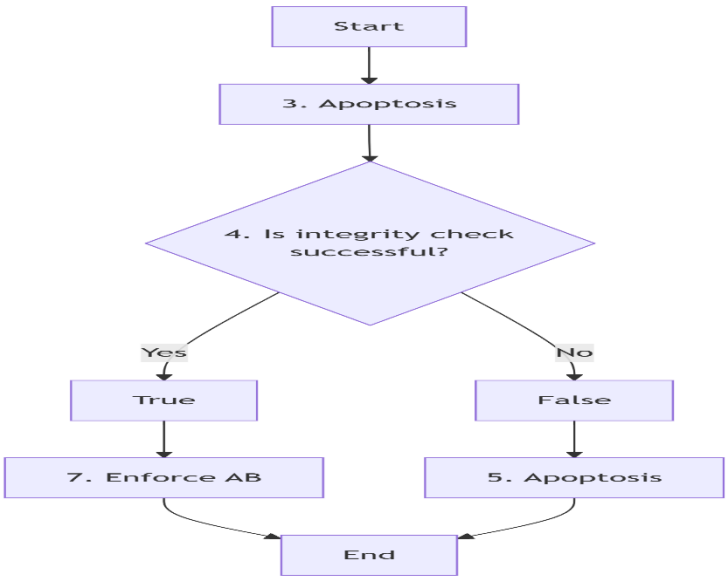

Figure 3: UML activity diagram illustrating the lifecycle and activation process of an active bundle

doi: https://doi.org/10.5281/zenodo.18212728

III. PROPOSED METHOD FOR SECURE STORAGE

This section presents an entity-centric identity management (IDM) approach designed to securely manage personal data stored in cloud environments. The proposed method integrates the Active Bundle (AB) paradigm with anonymous identification techniques to ensure privacy preservation, even when interacting with untrusted service providers.

3.1 Limitations of Existing IDM Approaches

Most existing IDM solutions rely on a trusted third party (TTP) to mediate authentication between users and service providers. In cloud environments, this assumption is problematic because the service provider and the TTP may belong to the same organization, resulting in centralized control and potential privacy violations. If the TTP is compromised, sensitive personal data may be exposed. Another limitation is that current IDM solutions assume that identity data is processed only on trusted hosts. This restricts the use of identity services on untrusted or public platforms, which is incompatible with modern cloud computing practices. Additionally, secure communication between users and service providers is essential to prevent side-channel and correlation attacks, particularly when sensitive data is forwarded between multiple providers.

3.2 Entity-Centric IDM and IDM Wallet

To address these challenges, we propose an entity-centric IDM model called the IDM Wallet, where identity disclosure decisions are fully controlled by the data owner. The IDM Wallet uses Active Bundles to encapsulate personally identifiable information (PII), privacy policies, and an embedded virtual machine that enforces access control rules. This ensures that sensitive data remains protected even on untrusted hosts. The system employs anonymous identification, supported by zero-knowledge proofs, to verify identity claims without revealing actual identity details. The architecture and operation of the IDM Wallet are illustrated in Fig. 4.

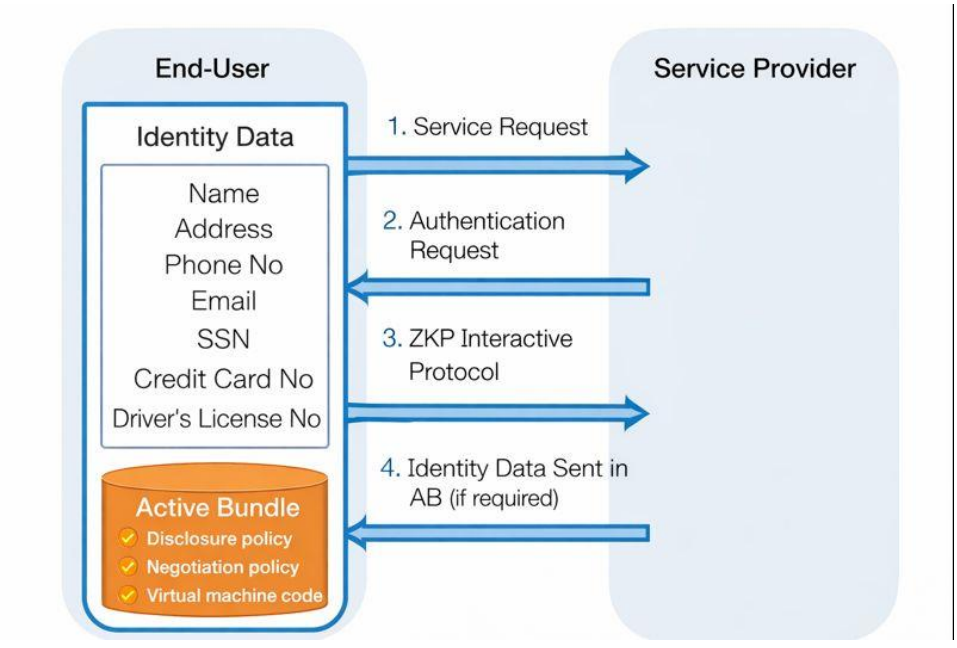

Figure 4: Architecture of the proposed IDM Wallet.

doi: https://doi.org/10.5281/zenodo.18212728

3.3 Anonymous Identification Using Fiat–Shamir Scheme

The proposed approach adapts the Fiat–Shamir identification scheme [16] to support anonymous authentication. In this scheme, an Identity Provider (IdP) issues identity credentials, while service providers verify identity claims through an interactive protocol. The verification process allows a service provider to confirm that an entity possesses a valid identity without accessing the underlying PII. To enhance privacy, the verification protocol is modified so that identity information is never directly disclosed. Instead, the entity proves possession of valid attributes within a predefined set, ensuring anonymity while maintaining authentication correctness.

3.4 Advantages of the Proposed Approach

The proposed entity-centric IDM model provides several important benefits for secure cloud-based identity management. It enables the safe use of identity data even on untrusted hosts by incorporating built-in protection mechanisms that prevent unauthorized access and misuse of sensitive information. The model ensures minimal disclosure of personal data by allowing service providers to access only the information strictly required to deliver a service. It operates independently of external trusted third parties, thereby eliminating centralized points of failure and reducing privacy risks. Additionally, the IDM Wallet is portable and can be carried across multiple devices, allowing users to maintain consistent control over their identities. Overall, the proposed approach offers a practical, flexible, and privacy-preserving solution for managing digital identities in cloud environments.

IV. PROTECTING PRIVACY OF VISUALLY IMPAIRED USERS

Individuals with visual impairments value security and privacy to the same extent as other members of society. However, the use of assistive navigation tools such as white canes often draws unwanted attention, making visually impaired users more vulnerable to physical threats and exploitation. Consequently, protecting their privacy—especially location privacy is of critical importance. Recent navigation systems for visually impaired users leverage mobile and cloud computing technologies to provide contextual assistance [17]. Such systems typically consist of a mobile device equipped with location-sensing capabilities for local navigation, obstacle detection, and user interaction, alongside cloud-based web services that support outdoor navigation, indoor routing, and object recognition. Since context-aware services heavily depend on real-time location information, location-based services play a central role in these systems. However, continuously uploading location data to the cloud introduces serious privacy risks. If compromised, such information could allow an attacker to track or physically harm a user. To mitigate this threat, the proposed entity-centric IDM framework ensures that users' locations are not permanently linked to cloud services. The system follows the principle of minimal data disclosure and employs Active Bundles to protect sensitive information. In the proposed model, a visually impaired user's digital identity including personal and subscription details is encapsulated within an Active Bundle. When interacting with a pedestrian route planning service, only the necessary subscription identifier and current location are selectively disclosed. Before transmitting any sensitive data, the Active Bundle verifies the service provider's trust level via a trust server. If the trust level is insufficient, the bundle activates its apoptosis mechanism to destroy sensitive data. For authentication, zero-knowledge proof techniques are used instead of revealing personally identifiable information. This allows the service provider to verify user eligibility without learning the user's identity or location history. As a result, user privacy is preserved, and long-term behavioral tracking becomes significantly more difficult.

doi: https://doi.org/10.5281/zenodo.18212728

V. CONLUSIONS

The rapid adoption of cloud services by governments and enterprises has made privacy and security critical concerns in modern computing environments. As sensitive data is increasingly outsourced to the cloud, there is a growing need for an entity-centric approach that prioritizes user privacy and enables secure identity management. Such an approach must effectively protect personally identifiable information (PII) while allowing trusted identification of users across organizational and web-based platforms. Identity management plays a central role in ensuring security and privacy in cloud computing. The entity-centric IDM model proposed in this work provides a robust mechanism for maintaining data confidentiality throughout its entire lifecycle. By incorporating the active bundle paradigm, the framework empowers users with direct control over how their identity information is shared and under what conditions it may be accessed. To demonstrate the practicality of the proposed solution, a functional model of the cloud-based system is evaluated under realistic usage scenarios. The results show that the framework operates as intended and successfully balances privacy preservation with service usability. Overall, the proposed identity and privacy management approach offers a promising foundation for establishing secure and privacy-aware standards in cloud computing environments.

VI. REFERENCES

[1] A. Josang and S. Pope. User Centric Identity Management, In Proc. AusCERT, Gold Coast, May 2005.

[2] Wikipedia. Identity Management Systems. July 2010. http://en.wikipedia.org/wiki/Identity_management_systems

[3] Cameron and M.B. Jones. Design Rationale behind the Identity Metasystem Architecture. January 2006.

[4] R. Gellman. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud. World Privacy Forum, 2009.

[5] A. Gopalakrishnan. Cloud Computing Identity Management. SETLabs Briefings, Vol 7, 2009.

[6] Identity Theft Primer, Libery Alliance Whitepaper, http://www.projectliberty.org/, December 05, 2005.

[7] S. Hubner. PRIME, https://www.prime-project.eu/. 2010.

[8] W. Alrodhan and C. Mitchell. Improving the Security of CardSpace, EURASIP Journal on Info Security Vol. 2009.

[9] OPENID, http://openid.net/, 2010.

[10] K. Cameron, Identity Weblog. 2010. http://www.identityblog.com/?p=685

[11] L. Ben-Othmane and L. Lilien. Protecting Privacy in Sensitive Data Dissemination with Active Bundles. Proc. 7th Annual Conference on Privacy, Security & Trust (PST 2009), Saint John, New Brunswick, Canada, August 2009.

[12] L. Lilien and B. Bhargava. A Scheme for Privacypreserving Data Dissemination. IEEE Trans. on Systems, Man and Cybernetics, Part A: Systems and Humans, 2006.

[13] L. Ben-Othmane. “Protecting Sensitive Data During Their Life Cycle,” Ph.D. Thesis, Western Michigan University, 2010 (in preparation).

[14] F. L. Bellifemine, G. Caire and D. Greenwood. Developing Multi-Agent Systems with JADE, John Wiley & Sons Ltd, West Sussex, England, 2007.

[15] Y. Zhong and B. Bhargava. Using Entropy to Tradeoff Privacy and Trust. SKM, Amherst, NY, Sep. 2004.

[16] A. Fiat and A. Shamir. How to prove Yourself: Practical Solutions to Identification and Signature Problems. CRYPTO, 1986.

[17] P. Angin, B. Bhargava and S. Helal. A Mobile Cloud Collaborative Traffic Lights Detector for Blind Navigation. 1st MDM International Workshop on Mobile Cloud. 2010.

[18] C. Sample and D. Kelley. Cloud Computing Security: Routing and DNS Threats. 2009. http://www.securitycurve.com/wordpress/

doi: https://doi.org/10.5281/zenodo.18212728