Digital Wallets and Identity Management: Pioneering Advances for Cloud Service Evolution

Fatemeh Stodt and Christoph Reich
Institute for Data Science, Cloud Computing, and IT Security; Furtwangen University,
Robert-Gerwig-Platz 1, 78120 Furtwangen, Germany
{Fatemeh.Stodt, Christoph.Reich}@hs-furtwangen.de

***Abstract*—In today's technology-driven world, the management of digital identities has become a crucial concern. This is mainly because of the widespread use of online services and digital devices. The widespread use of digital platforms has created a complex web of online identities, placing the responsibility of juggling numerous usernames, passwords, and authentication methods on individuals. Digital wallets have emerged as a promising solution to tackle this complex challenge. This text highlights the versatility of these tools, which allow users to securely store, efficiently manage, and effectively utilize their digital assets, including personal data, payment information, and various credentials. In addition, the field of digital identity management has seen the rise of federated services, which provide users with the convenience of accessing multiple services using just one digital identity. An exceptional example in this field is Gaia-X, an innovative initiative focused on creating a reliable and secure data infrastructure. Gaia-X showcases the immense potential of federated services in bolstering digital identity management. This paper delves into a comprehensive examination of digital identity management, specifically examining the use of digital wallets and federated services. Our investigation delves into the categorization of identities needed to access various cloud services, taking into account their distinct requirements and characteristics. In addition, we explore the ever-changing world of digital wallets and federated identity management in the cloud. This sheds light on the upcoming requirements, challenges, and advantages. In addition, we present a thorough categorization scheme for cloud services, distinguishing them based on their security and privacy requirements. In this framework, we demonstrate the strategic mapping of different identity types to each category, providing a practical approach to aligning identity measures with the specific services being accessed.**

Keywords-Digital wallet; Identity management; Federated service; Cloud.

I. Introduction

The management of digital identities has become a crucial issue in our modern digital era [1]. In today's digital landscape, the constant use of online services and the integration of digital devices into our daily routines have led to a situation where individuals are constantly sharing personal information to access a wide range of digital platforms, services, and applications [2]. The constant demand for digital identities has created a complex and fragmented landscape, where users are left with the task of managing multiple usernames, passwords, and authentication methods [3]. This situation, although aimed at guaranteeing access and security, frequently presents itself as a tangled web of complexity and vulnerability.

In this context, personal identity is spread across various digital domains, each requiring a unique set of keys for access. The fragmentation of identity and the proliferation of digital keys highlight the complex nature and risks of our interconnected digital world [4]. Managing multiple digital personas can be a cognitive challenge for users. Each persona is safeguarded by a unique combination of characters and security measures. This practice, although necessary, can be mentally taxing and increases the chances of security breaches. The more passwords one has to handle, the greater the risk of encountering vulnerabilities in the security system.

Clearly, the digital identity landscape has become a challenging arena where convenience and security often clash. The task at hand is to create creative solutions that not only simplify the management of digital identities but also strengthen their ability to withstand the constantly changing threats of the digital world [5]. This paper delves into the realm of digital identity management, seeking to clarify its complexities, address its challenges, and propose potential solutions in a world that is becoming more interconnected and data-driven.

Amidst these challenges, digital wallets have emerged as a promising solution for efficient digital identity management [6]. These software applications provide users with a convenient way to store, manage, and deploy a wide range of digital assets, including personal data, payment information, and various credentials [7].

In addition, the groundbreaking Gaia-X initiative exemplifies the importance of federated services and the considerable advantages they provide (Braud et al., 2021). Gaia-X has been meticulously designed to provide users with a strong and reliable data infrastructure, giving them unparalleled control over their personal information [8]. With Gaia-X's unified digital wallet, users can effortlessly navigate various platforms and services using just one digital identity. This simplifies the management of their digital presence and enhances security and privacy. This approach prioritizes the needs of users, giving them more control and encouraging innovation and competition in the digital realm. It strengthens the benefits of Gaia-X federated service model.

In today's digital landscape, the significance of efficient digital identity management cannot be emphasized enough. Luckily, there are some promising solutions on the horizon to address this complex challenge. Digital wallets and federated services are emerging as potential avenues to explore [9]. This paper aims to provide a thorough exploration of digital identity management and shed light on its practical uses, specifically in the areas of digital wallets and federated services. In addition,

we will delve into the use of digital wallets for accessing cloud services, offering valuable insights into their advantages and possible obstacles.

Here is the structure of this paper: Section II provides important background information on digital wallets and federated services. In Section III, we explore the requirements for identity management within wallets, specifically in the context of cloud access. In Section IV, we explored the benefits of digital wallets for cloud-based identity management. Section V provides a comprehensive categorization of cloud access based on identity group levels, offering valuable insights into the complex nature of the process. Section VI provides a use case that helps to further understand our approach. In Section VII, we bring together our findings and present a comprehensive conclusion that captures the essence of our exploration.

II. Background (State of the Art)

This section provides an overview of three key components: Digital Wallets, Federated Services, and Federated Identity Management System, which play pivotal roles in ensuring secure and efficient digital experiences.

A. Digital Wallet

The rapid acceleration of digitization in transactions has been greatly influenced by the global pandemic, leading to an increased dependence on electronic services. Users today are actively involved in a variety of activities, including tax declarations, accessing vaccination and test certificates, and interacting with public administrations. These tasks are primarily carried out through digital platforms [10]. Users must complete an authentication process to access these services, ensuring electronic identification (eID) and protecting personal information. The authentication processes rely on identity management (IdM) systems to serve as gatekeepers, ensuring reliable and secure user authentication [11].

In this ever-changing digital landscape, digital wallets have become crucial elements in the realm of digital identity management. A digital wallet functions as a secure and encrypted repository, allowing users to effectively store and manage their digital identities, credentials, and other relevant information [12]. This serves as a crucial hub, providing a secure haven for users to store a wide range of authentication data, including usernames, passwords, digital certificates, and more [13].

There are a multitude of advantages associated with digital wallets in the field of identity management, which are both extensive and persuasive [14]. One of the standout features is the incredible convenience it provides, allowing users to store all their identities in one place, regardless of the services and platforms they use. In the safe and convenient realm of their digital wallet, users can easily store and organize multiple sets of credentials, eliminating the need to remember separate usernames and passwords for each service provider. This efficient integration of identity management not only streamlines the user experience but also significantly reduces the mental strain associated with managing multiple identities [15].

Throughout the years, a multitude of models for identity management systems have been developed and put into action. The earliest and most common model is the isolated model, which states that each service provider operates its own identity provider (IdP) [16]. Unfortunately, this approach places a heavy burden on users, as they are required to register with each service provider individually. This can be quite overwhelming, as it means having to manage multiple sets of credentials. This challenge prompted the introduction of the central identity model, which revolutionized the way IdP functionality is handled. It involves outsourcing the IdP functionality to a central entity that can be utilized by multiple service providers collectively [17]. Under this model, users only need to register once with the central IdP. After that, they can easily access a wide range of services using the same credentials.

Although the central identity model undeniably improves usability, it also brings up valid concerns about the central IdP being a potential single point of failure and a target for privacy breaches. The federated IdM model was introduced as a visionary approach that forges trust relationships among multiple IdPs, addressing these concerns [18]. Users registered with one IdP can easily authenticate themselves to service providers served by other IdPs within a circle of trust in this model. An excellent example is the European eIDAS interoperability framework, which effectively coordinates cross-border authentication processes by connecting national IdM systems across EU Member States.

The user-centric IdM model takes a different approach, with identity data being stored within the user's domain. This data is typically found on a smartcard or a smartphone equipped with a hardware-based security element [19]. Users maintain a strong sense of control over their identity data in this model, resulting in heightened privacy. Notable instances of this model include national IdM solutions that utilize smartcards effectively, like the Austrian Citizen Card and the German eID. The authentication processes retrieve the necessary identity information from the user's domain and seamlessly relay it to the requesting service provider, which improves control and privacy.

Nevertheless, the ever-changing digital identity landscape has given rise to the concept of Self-Sovereign Identity (SSI). This paradigm empowers users with complete control over their credentials, as recent advancements have demonstrated [20][14]. SSI represents a significant shift away from the conventional dependence on central authorities. Instead, it utilizes distributed ledgers among multiple IdPs operating within a circle of trust to register new credentials. Initiatives like the European Self-Sovereign Identity Framework (ESSIF) and Veramo exemplify this progressive approach. These developments showcase a noticeable transition towards user-controlled identity data, a trend that has garnered the interest of policymakers, as highlighted by the European Commission's proposal for a new European Digital Identity.

The OpenWallet Foundation (OWF) has established itself

as a leading force in the realm of digital wallets, showcasing innovation and creating new opportunities in this dynamic landscape [21]. OWF, under the Linux Foundation Europe, is dedicated to promoting open-source software development that enables interoperability among a wide range of wallet applications [22]. These applications cover a wide range of use cases, including secure payments, identity verification, and the secure storage of validated credentials. The vision of OWF perfectly aligns with the direction of a digital era characterized by user empowerment and the importance of secure, user-centric digital identities.

B. Federated Services

The concept of a federated catalog is crucial in the field of identity management as it enables the seamless discovery and access to a wide range of services through a centralized repository [8]. In this cutting-edge framework, various catalog systems work together to share important information about the services they offer. This collaborative effort results in a comprehensive and user-friendly resource center, simplifying the sometimes complex process of finding services [23].

The inter-catalog synchronization is a crucial element at the core of this federated catalog model. This crucial aspect guarantees that information regarding services, including their availability, descriptions, and detailed attributes, is consistently kept up-to-date and aligned across various catalog systems [24]. The updates and modifications made within one catalog seamlessly reverberate across others, thanks to the intricate mechanisms of inter-catalog synchronization. This carefully executed coordination not only maintains the integrity of the data but also ensures that users receive precise and up-to-date information. The result is a smooth user experience where people can trust the federated catalog to provide consistent and unified information about the services available [25].

The incorporation of digital wallets into the structure of federated catalogs brings an extra level of functionality and convenience to the field of identity management [25]. The seamless integration of digital wallets and federated catalogs enhances the efficiency of service discovery and access, as they securely store and manage users' digital identities and associated credentials. When a user interacts with the federated catalog using their digital wallet, the wallet plays a vital role in verifying the user's identity and sharing relevant identity information with the catalog. The symbiotic interaction allows the catalog to provide personalized service recommendations, curate search results to meet individual needs, and smoothly manage authentication and authorization processes [26]. The end outcome is an enhanced user experience, carefully adjusted for both user convenience and security.

It's worth mentioning that federated services and federated catalogs are closely connected concepts in the field of identity management. Federated services rely heavily on federated catalogs as crucial resources, necessary for providing users with a centralized and comprehensive view of the services available. Thanks to this collaboration, users now have the convenience of exploring and accessing services with just one digital identity. This powerful collaboration between service providers and catalogs, operating under the federated model, efficiently simplifies identity management processes. The catalog serves as a reliable intermediary, managing authentication, user authorization, and facilitating smooth information exchange between users and service providers [27]. The smooth functioning of the federated ecosystem relies heavily on the crucial role played by federated catalogs, which serve as linchpins in the complex task of managing identity.

C. Federated Identity Management System

The Federated Identity Management System (IdMS) marks a notable departure from the conventional centralized IdMS concept. The federated IdMS system connects user identity information across multiple organizations, as shown in Figure 1. This approach avoids relying on a single central identity provider. In this dynamic model, the service providers and identity providers are entities that represent trusted organizations within the federation.

At the heart of this framework lies the importance of fostering a collaborative agreement among the different service providers. This agreement guarantees that a user's identity is not just acknowledged but also universally accepted by all participating service providers within the federation. The seamless access to services from multiple providers within the federation allows users to avoid the hassle of repeated authentication or the need to create separate accounts for each service [28]. This collaborative approach improves user convenience and promotes a greater sense of trust within the federation.

The federated IdMS is a powerful and versatile solution that allows users to effortlessly access a wide variety of services, all while ensuring their identity remains secure and consistent across trusted organizations. This represents a notable departure from the conventional centralized identity model, providing improved adaptability, scalability, and user-focused identity management.

The federated IdMS model introduces the concept of a user needing to authenticate themselves only once to access multiple services, making it more convenient for users. This efficient process is known as Single Sign-On (SSO), and it relies on the established trust between service providers and the identity provider [28]. SSO operates by utilizing security tokens to enable secure and efficient access to a range of services.

III. Requirements for Identity Wallets for Future Clouds

In today's rapidly evolving digital landscape, the importance of robust identity management cannot be overstated. With the increasing prevalence of cloud computing, it is crucial to establish secure and seamless access to cloud services. This section explores the categorization of identities needed for various cloud services, examines their specific requirements and characteristics, investigates the future needs for digital wallets and federated identity management in the cloud, identifies possible challenges in implementing identity wallets for future

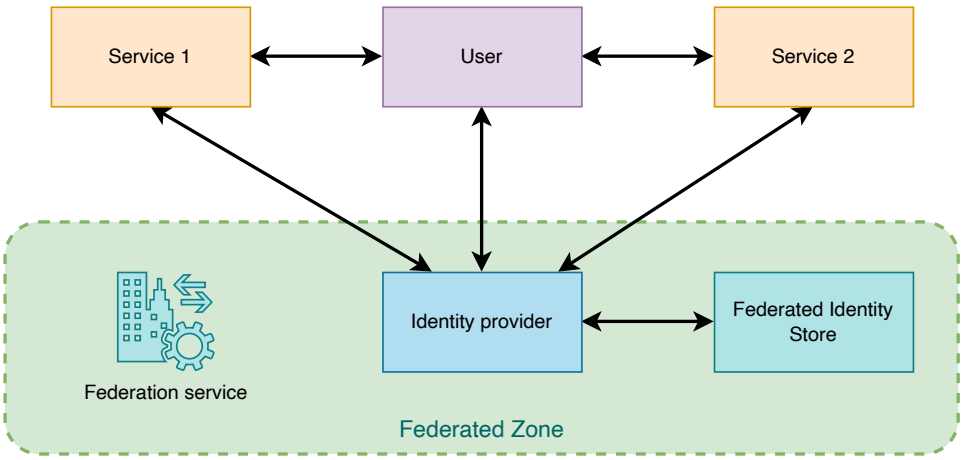

Figure 1. Dataflow Representation of a Federated Identity Management System

clouds, and emphasizes the potential advantages of using digital wallets for identity management in the cloud.

Understanding the diverse identity landscape becomes more comprehensive when identities are categorized based on their usage in various cloud services. The identities mentioned can be categorized into user identities, service identities, and device identities [29]. The different types of identities in the cloud ecosystem include user identities, service identities, and device identities. User identities are used by individuals to access cloud services, while service identities are specifically associated with cloud services or applications. Device identities, on the other hand, are used to authenticate and authorize devices that interact with cloud resources. Effective identity management requires careful consideration of the unique requirements and characteristics of each identity category.

R1: Secure storage of identity-related data: In the ever-changing landscape of cloud services, the protection of identity and identity-related data becomes a top priority. This essential requirement is based on the importance of maintaining the confidentiality, integrity, and availability of sensitive data associated with user identities, service identities, and device identities [13].

When it comes to cloud services and the movement of data across virtual boundaries, the importance of secure storage cannot be emphasized enough. It forms the foundation for establishing trust and ensuring data protection. This requirement is crucial in protecting the digital identities that are essential for accessing cloud resources.

Secure storage goes beyond just keeping data. It encompasses much more than that. It demonstrates a strong dedication to implementing thorough security measures that protect identity-related information. The implementation involves the use of strong cryptographic measures, strict access controls, and robust data encryption methods. The implementation requires the use of intrusion detection systems and ongoing monitoring to protect user identities, service credentials, and device authentication data from unauthorized access and potential harm. Through this approach, secure storage effectively minimizes the potential dangers linked to data breaches, identity theft, and unauthorized access.

R1 exemplifies the fundamental principle of trust in cloud-based identity management. This serves as a crucial safeguard, preserving the integrity of identity-related data and strengthening the foundation of cloud security and user trust.

R2: Effective management of identity-related data: Managing identity-related data within the cloud is a complex task that involves a range of important functionalities. The functionalities cover a wide range of tasks, from carefully curating data to thoroughly reviewing it, all done within the cloud environment. In addition, it is crucial to have the ability to determine which aspects of identity data should be shared beyond the cloud's boundaries [30]. R2 aims to give users a greater sense of control over their stored information, promoting privacy and enabling more nuanced data management.

R2 goes beyond basic data management and instead encourages a feeling of digital self-determination within the expansive realm of the cloud. This requires the ability to carefully select, modify, or delete portions of identity data stored in cloud repositories. Users have the power to shape their digital personas within the cloud ecosystem, making thoughtful decisions about which aspects of their identity should be accessible. This falls under the purview of R2.

The concept of selective data sharing is crucial to R2's mandate. This allows users to determine which aspects of their identity data should be shared with external entities or services, extending beyond the boundaries of the cloud. The careful management of data sharing provides a strong privacy mechanism, which enhances user trust in the cloud's identity management processes.

R2 serves as a protector of user autonomy, creating an environment where individuals have precise control over their digital identities. R2 prioritizes privacy and data sovereignty by incorporating these capabilities into the cloud environment. It highlights the idea that users play an active role in managing their identity-related information, rather than being passive recipients. By doing so, it strengthens the core principles of

trust and user-centricity in cloud-based identity management. This ushers in a new era where users are not just data subjects, but rather thoughtful guardians of their digital identities.

R3: Secure sharing of identity-related data: The importance of R3 becomes evident in the complex realm of cloud-based identity management. This involves the facilitation of secure sharing of identity-related data beyond the boundaries of the cloud environment, which is of utmost significance. This undertaking relies on the creation of robust and secure communication channels and protocols, coordinating the distribution of identity data to trusted entities [31]. It is crucial to maintain unwavering commitment to upholding data integrity and confidentiality throughout the data-sharing process.

R3 encapsulates a fundamental dichotomy. It acknowledges the importance of sharing identity-related data for the smooth operation of digital services, applications, and interactions. However, it emphasizes the absolute need for strong protections to surround this data as it moves beyond the confines of the cloud.

This task involves the development of strong communication channels that can withstand potential adversarial forces. These channels serve as pathways for identity data to travel to its intended recipients. At the same time, strong protocols are implemented to regulate the journey of this data. The protocols serve as digital guardians, ensuring the integrity and confidentiality of every packet of information.

In addition, R3 highlights the intricate relationship between trust and technology. The cloud environment must foster a sense of trust, allowing users to securely entrust their identity data to the digital realm. The trust in our system is reinforced by a comprehensive set of technical measures that effectively protect against data breaches, eavesdropping, and tampering.

R3 effectively resolves the dilemma of sharing data while ensuring its protection. This statement highlights the importance of protecting identity-related data as a means to safeguard individual privacy and security in the digital realm. R3's commitment to secure sharing harnesses the power of the cloud to effectively balance the need for seamless service delivery and robust data protection. In the realm of cloud-based identity management, it serves as a strong foundation where trust and security work together to create a thriving digital ecosystem that is safe and reliable.

R4: Secure storage of cryptographic material: R4 is a crucial necessity in the constantly changing world of cloud-based identity management. This mandate emphasizes the importance of creating a secure vault to protect the cryptographic components of digital identities within the cloud ecosystem [32]. This requirement emphasizes the importance of protecting cryptographic elements, such as keys and certificates, from unauthorized access, ensuring their confidentiality and security.

R4 emphasizes the importance of cryptographic material as the foundation of trust in the digital world. The cryptographic artifacts, which include cryptographic keys and digital certificates, play a crucial role in verifying users, validating services, and ensuring the security of data exchanges. R4 has a dual purpose. It emphasizes the need for strong cryptographic storage mechanisms that can effectively protect against intrusion, manipulation, and compromise. These repositories ensure that cryptographic material is kept securely protected, safeguarded from any potential harm caused by malicious individuals.

Furthermore, R4 emphasizes the importance of maintaining confidentiality. The text emphasizes the importance of robust cryptographic measures to safeguard sensitive information. It highlights the need for multiple layers of protection to ensure the confidentiality of cryptographic secrets, even in the event of a breach. The maintenance of confidentiality relies heavily on cryptographic mechanisms like encryption, digital signatures, and access controls.

In addition, the imperative embedded within R4 goes beyond simple storage. The entire lifecycle of cryptographic material is covered, including generation, distribution, rotation, and retirement. Every aspect of this lifecycle requires careful planning, strict security measures, and ongoing supervision to ensure the material remains resilient against emerging threats.

R4 plays a crucial role in maintaining trust in the cloud's identity management infrastructure. This serves as a guardian, guaranteeing that the cryptographic keys and certificates, which are crucial for secure digital identities, remain completely secure and cannot be compromised. The cloud demonstrates its dedication to upholding the importance of digital interactions, protecting user identities, and supporting the fundamental principles of security and trust in the digital world by adhering to R4's mandate.

R5: Combining identity data before sharing: The complex world of cloud-based identity management is enriched by the presence of R5, which seamlessly aligns with the profound concept of selective disclosure. The core concept of R5 emphasizes the importance of users having the ability to carefully merge and curate their identity data, aligning it with their specific sharing needs [33]. This skillful capacity to combine and distribute pertinent aspects of identity is crucial for maintaining privacy and managing the sharing of identity-related data.

The mandate outlined in R5 is rooted in the fundamental principle of selective disclosure. In the complex world of cloud computing, it is important for users to have control over how they disclose their identity. This allows them to customize their disclosures to suit their specific needs and preferences. This thoughtful approach to data sharing allows individuals to take control of their digital identities, sharing only the necessary information for each interaction. This not only protects their privacy but also gives them greater control over their identity-related data.

Practically speaking, R5 acts as a protector of personal privacy, giving users the ability to have precise control over their identity data. The necessity for extensive data sharing is eliminated, as it enables a more precise and refined approach to identity facets. The users have the ability to carefully construct their identity by selecting the relevant attributes, credentials, or personal details to include, customizing their disclosure for each unique situation.

R5 aims to promote a more sophisticated approach to data

sharing, moving away from a simplistic binary perspective. Users have the ability to find a delicate equilibrium between sharing the right amount of information to foster meaningful interactions, while also protecting their privacy. This approach not only improves personal data protection, but also fosters a sense of trust in cloud-based identity management.

R5 acts as a diligent sentinel, safeguarding the delicate equilibrium between privacy and data exchange in the expansive domain of the cloud. It highlights that in the era of digital technology, the act of sharing data is not necessarily a binary choice. The cloud ecosystem promotes a robust sense of privacy, enabling individuals to retain mastery of their digital identities with proficiency.

Using digital wallets for identity management in the cloud provides a variety of advantages. Digital wallets improve user convenience by offering a centralized platform for managing identities across various cloud services. The security measures are enhanced by implementing secure authentication mechanisms, employing strong encryption for identity data, and implementing efficient access control. In addition, digital wallets provide users with the power to have control over their personal information and the option to selectively share it with trusted entities. The integration of digital wallets with federated identity management enhances the efficiency of identity management processes, facilitating easy access to cloud resources and promoting compatibility.

Table I provides a comparison of various digital wallets, with a specific focus on their Identity Management (IdM) capabilities and wallet requirements. This table is an excellent resource, offering a concise summary of the strengths and functionalities of different digital wallet solutions in terms of identity management.

The table examines the authentication methods used by each digital wallet. These mechanisms play a crucial role in maintaining secure identity validation within the cloud environment. By familiarizing themselves with these approaches, users can make well-informed decisions regarding which wallet is most suitable for their individual security requirements.

Encryption Techniques: Security is of utmost importance in IdM, and the table reveals the encryption techniques used by each digital wallet. The techniques serve as a strong defense for identity data, ensuring its protection against potential threats. Users are empowered with the knowledge to effectively prioritize the protection of their identity data.

Controlling access to identity attributes is crucial for maintaining privacy and security. The table provides a comprehensive explanation of the access control features found in each digital wallet, detailing how they effectively handle the distribution of user identity information. Users can adjust their privacy settings to match their personal preferences and needs.

The table emphasizes the level of user control offered by each digital wallet in terms of personal information, which is crucial in today's data-driven world where ownership and autonomy are highly valued. This text offers valuable insights into how users can carefully choose which identity data to share with trusted entities, allowing them to maintain their privacy and control over their data.

Table I provides readers with a comprehensive understanding of the intricate features and capabilities of each digital wallet. With this knowledge at hand, stakeholders can confidently make decisions and choose a digital wallet solution that perfectly matches their specific identity management requirements. This table is a valuable tool that provides insights into effective, secure, and user-centric identity management in the constantly changing world of cloud services.

IV. Unlocking the Advantages of Digital Wallets for Cloud-Based Identity Management

Digital wallets have a significant impact on identity management in the cloud, offering a wide range of benefits that transform the way we engage in digital interactions. The virtual guardians play a crucial role in strengthening the foundation of cloud-based identity management. This section explores the numerous benefits that users gain from cloud services and the complex nature of cloud security.

Enhanced User Convenience: Digital wallets have become exemplars of user-centricity, creating a haven of convenience within the vast realm of the cloud. They appear as centralized repositories, giving users the ability to seamlessly manage their digital identities across a variety of cloud services. Gone are the days of managing a collection of credentials, each resembling a digital puzzle piece, as they slowly fade into obscurity. Users are introduced to a realm where a streamlined interface enhances their experience with the digital world. This transformation not only simplifies the user experience but also reduces the mental effort required to handle multiple digital identities.

Fortified Security Infrastructure: Digital wallets serve as strong protectors of security in the cloud. The authentication mechanisms they implement set a high standard, providing strong protection against unauthorized access. Within these virtual strongholds, identity data is securely protected by layers of robust encryption. This strong armor guarantees that even when faced with possible breaches, the identity data remains a mystery, protecting its integrity and confidentiality. The diligent guardians of access control oversee the allocation of identity attributes, granting access only to those who possess the necessary permissions to unlock the wallet.

Empowerment and Data Sovereignty: The concept of empowerment lies at the core of digital wallets. Users have the power to become guardians of their personal information, choosing who they share it with and maintaining control over it. This shift in power represents a new era, where individuals are at the forefront of their digital identities. Users are no longer passive participants, but rather discerning custodians of their identity data. This transformation represents a significant milestone in the age of digital interactions, where the control of data is placed in the hands of those who are most affected by it.

Seamless Integration with Federated Identity Management: The integration of digital wallets with federated identity

TABLE I. COMPARISON BETWEEN DIFFERENT DIGITAL WALLET BASED ON IDM AND WALLET REQUIREMENTS

Reference	IdM	Environment	R1	R2	R3	R4	R5
[20]	SSI	Local	✓	✓	✓	✓	✓
[25]	Federated	Local	✓	✓	✓	✓	✓
[13]	Centralized	Local	✓	✓	✓	✓	✗
[34]	as a Service	Remote	✓	✓	✓	✗	✓
[19]	User-centric	Local	✓	✓	✓	✓	✗
[17]	Centralized	Remote or Local	✓	✓	✓	✓	✗
[14]	SSI	Remote or Local	✓	✓	✓	✓	✓
kudra2022self , [21]	SSI	Remote or Local	✓	✓	✓	✓	✓

management is like a harmonious collaboration within the expansive realm of cloud computing. This seamless blending of two elements results in a beautifully orchestrated identity management system. The integration acts as a crucial component that simplifies identity management processes, bringing about a time of effortless access to cloud resources. Users navigate the digital realm with a unified digital identity, surpassing the obstacles posed by various service providers. In this realm of collaborative synergy, creativity blossoms, and healthy competition thrives, highlighting the significant benefits of a federated service model.

Overall, digital wallets play a crucial role in ensuring user-centricity, security, and interoperability in the vast realm of the cloud. They have a unique perspective on the user experience, prioritize security, give individuals control over their data, and promote the effectiveness of federated identity management. In this era of rapid technological advancements, digital wallets serve as essential tools that help users navigate the complex realm of cloud-based identity management. They play a crucial role in maintaining trust, security, and user empowerment as unwavering principles.

V. ACCESS MANAGEMENT AND CATEGORISING IDENTITIES FOR CLOUD SERVICES

The significance of security and privacy in the dynamic field of cloud computing cannot be emphasized enough. We present a rigorous categorization approach that groups cloud services according to their distinct security and privacy needs in order to efficiently traverse this difficult terrain. This scheme offers practical insights into choosing the most suitable identity type for each service, in addition to providing a framework for comprehending the heterogeneous environment of cloud services.

As Figure 2 illustrates, our classification approach distinguishes between three categories of cloud services: low-security services, moderate-security services, and high-security services. Every layer is carefully crafted to conform to the differing levels of privacy and security requirements that are specific to certain service kinds.

A. Low-Security Services

Cloud offerings classified as low-security services are typically used for non-sensitive data and require only minimal protection measures. These services generally consist of information that is readily available to the public and poses little risk if it becomes exposed. There are various sources where you can find information, such as websites, public repositories, and blogs.

1) Identity Needs: Within the domain of low-security cloud services, the authentication and access control techniques depend on simple user identities, usually consisting of usernames and passwords. Due to their widespread presence, these user identities provide convenient management. Within this particular scenario, the main objective is to develop a solid foundation for safeguarding data rather than implementing strict safeguards to ensure privacy. Although privacy is still a worry, the focus is on adopting fundamental security measures, such as ensuring data protection during transmission through protocols like HTTPS. Nevertheless, the implementation of strong encryption and multifactor authentication is sometimes considered superfluous in these situations. The main goal is to prioritize simplicity and user-friendliness, making it easier for a wide range of users to access and use this specific category of cloud services.

2) Mapping Identities to Categories: For services in this category, basic user identities like usernames and passwords may be enough for authentication and access control. These credentials offer sufficient security for services with low privacy concerns.

B. Moderate-Security Services

Moderate-security services are positioned in the middle of the range, dealing with fairly sensitive data that necessitates stronger protective measures compared to low-security services. These services handle data of moderate sensitivity, such as personal information, internal organizational papers, or consumer data with a certain degree of secrecy.

1) Identity Needs: When dealing with the needs of cloud services that have moderate security requirements, there are various factors linked to identification that need to be taken into account. Improving security is of utmost importance, requiring the implementation of more robust authentication methods like two-factor authentication (2FA), biometrics, or the integration of extra security measures. At the same time, there is increased focus on privacy concerns due to the fact that the data being managed may have legal or compliance ramifications. In order to address these concerns, implementing data anonymization and controlled access mechanisms are considered appropriate safeguards. In addition, security precautions in this context include encrypting data both when it is stored and when it is

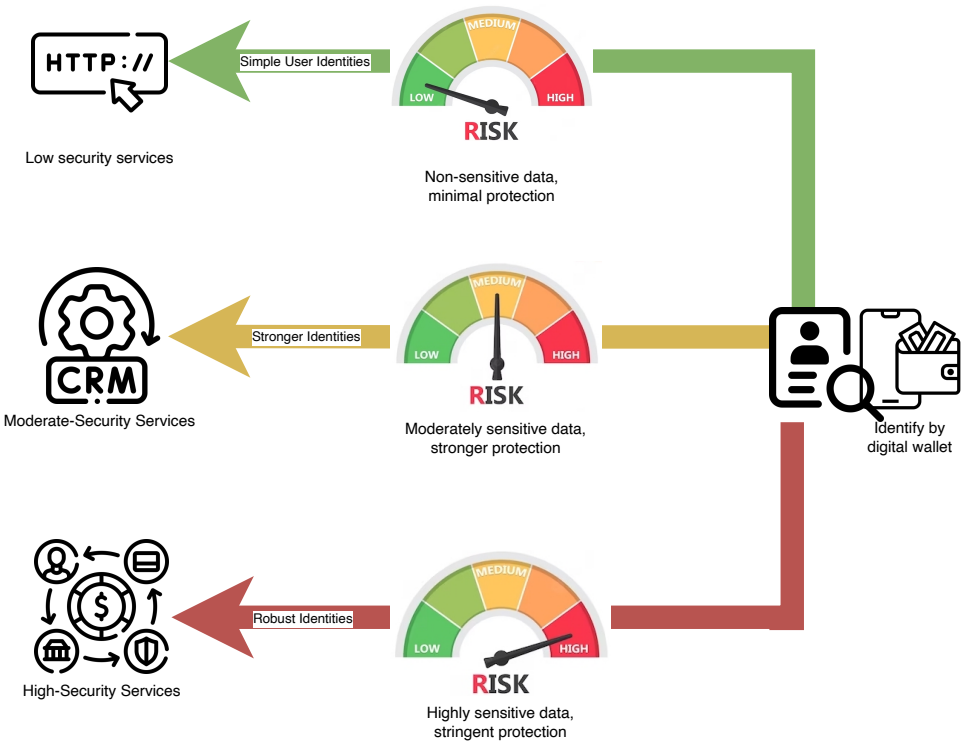

Figure 2. Categorisation of Cloud Services and Identity Types

being transferred. These steps are supported by regular security audits and checks to ensure compliance. In the middle of these efforts focused on security, there is a deliberate attempt to find a careful balance between improving security measures and maintaining a great user experience. This recognizes the significance of user convenience, especially in the context of cloud services with moderate levels of protection.

2) Mapping Identities to Categories: The moderate-security category requires more robust authentication procedures to enhance security. Implementing two-factor authentication or biometrics may be essential in order to ensure strong protection for personal information or organizational documents.

C. High-Security Services

High-security services are responsible for safeguarding extremely sensitive data and so must implement the most rigorous and demanding protective measures. These services manage highly confidential data, including bank records, health information, trade secrets, and classified information. Unauthorized access or breaches may result in significant repercussions.

1) Identity Needs: High-security services necessitate the implementation of the most rigorous protective measures. They employ multifactor authentication, which integrates various authentication techniques such as smart cards, biometrics, and one-time passwords to enhance identity verification. In addition, digital certificates are provided to enhance security by providing identification for both users and services. Hardware Security Modules (HSMs) are essential in safeguarding against advanced cyber threats since they offer tamper-resistant encryption and secure storage of cryptographic keys in hardware. Continuous surveillance and thorough examination of user behaviors also assist in the prompt identification of potential security breaches. In addition, the implementation of stringent access controls, such as role-based access control (RBAC) and the principle of least privilege, ensures that only authorized persons are granted access to sensitive information.

2) Mapping Identities to Categories: High-security services require the use of multifactor authentication, digital certificates, or physical tokens for the most sensitive data. By integrating these safeguards with rigorous surveillance and access restrictions, the utmost level of safeguarding and confidentiality is achieved, guaranteeing secure entry to vital information.

VI. Practical Application of the Categorization Scheme

Here, we demonstrate a tangible implementation of our classification system to showcase its practical use in real-life scenarios. In this case study, we illustrate how the scheme helps in identifying suitable security solutions for various cloud applications.

Case Study: Categorizing the Security of Cloud Services

Let's examine a company called CloudTech Inc. that provides a variety of cloud services. In order to gain a deeper understanding of the advantages of our categorization scheme, we will analyze three specific services it offers: a publicly accessible website, a Customer Relationship Management (CRM) system, and a Secure Financial Transactions (SFT) platform.

Service with minimal security measures - Website accessible to the general public:

CloudTech Inc. manages a website that is accessible to the public. The website offers comprehensive details about the company, its products, and valuable knowledge about the industry. This website solely functions as a promotional and informative tool and does not include the processing of sensitive data. As a result, it is classified as a low-security category in our system.

Identity Type: This service requires a basic user identity, which includes a username and password. Users necessitate fundamental authentication in order to have access to general information and resources on the website.

CloudTech Inc. employs industry-standard security measures, such as data encryption for transmission and safeguards against common online vulnerabilities, to guarantee the security of user interactions on the website.

CRM System with Moderate-Security Service:

CloudTech Inc. provides a cloud-based client Relationship Management (CRM) solution that effectively handles client data, such as contact information, purchase records, and conversation logs. This service entails the management of confidential client data and is therefore classified as having a moderate level of security.

The CRM system utilizes two-factor authentication (2FA) to efficiently protect the security and privacy of customer data. In addition, biometric authentication is used to increase security.

The CRM system employs strong encryption methods to protect data both while it is stored and when it is being transmitted. Access controls are used to guarantee that only authorized individuals have the ability to view or alter client records. The service is brought into alignment with industry standards and laws through regular security audits and compliance inspections.

Advanced Security Service - Secure Financial Transactions (SFT) Platform:

CloudTech Inc. provides a safe Financial Transactions (SFT) platform that enables safe monetary transactions, such as payment processing and cash transfers. This service handles extremely confidential financial information and consequently belongs to the high-security classification.

The SFT platform employs multifactor authentication (MFA), which includes biometrics, smart cards, and one-time passwords (OTP), to guarantee the utmost level of identity verification.

The security measures implemented for the SFT platform encompass various aspects. These include the utilization of end-to-end encryption to protect transaction data, conducting thorough penetration testing to identify vulnerabilities, continuous real-time monitoring of transactions, and adherence to strict financial sector rules.

Analysis of the Case Study:

This case study demonstrates the efficacy and flexibility of our categorization approach in real-life situations:

Customized Security: Our categorization method enables CloudTech Inc. to customize security measures according to the unique requirements of each service. Less secure services benefit from less complex authentication, whereas more secure services require the most rigorous identity verification methods.

CloudTech Inc. optimizes resource allocation by aligning security with service categories, resulting in efficient resource allocation. High-security protocols are specifically implemented for services that deal with confidential information, guaranteeing optimal utilization of security resources.

Data Protection and Privacy: The categorization scheme emphasizes the significance of safeguarding confidential information, advocating for compliance with legislation around data protection and privacy.

To summarize, our hierarchical classification system improves the decision-making process for adding security measures in cloud services. It guarantees that the level of security matches the level of sensitivity of data, enabling organizations such as CloudTech Inc. to offer strong protection for important information without introducing extra complications in less secure situations. This framework is a useful tool in the constantly changing field of cloud computing security.

VII. Conclusion

To summarize, digital wallets and federated services provide substantial benefits in the administration of digital identities. Digital wallets offer a secure and convenient method for users to store and oversee their digital assets, streamlining the management of digital identities while improving security and privacy. The development of various identity management methods, such as federated and user-centric approaches, alongside innovations like Self-Sovereign Identity (SSI), provide users more authority over their credentials. Initiatives such as Gaia-X demonstrate the objective of empowering consumers with greater authority over their personal data and promoting innovation in the digital domain.

In the future, it is important for research to concentrate on incorporating new technologies like blockchain and decentralized identification systems to improve the security and privacy of digital wallets and federated services. Furthermore, investigating the usability and user experience elements of these solutions might enhance their adoption and acceptance among users. Sustained endeavors in research and development will aid in tackling the intricate obstacles of digital identity management and guarantee its significance in the contemporary digital age.

Acknowledgement

This research was funded by the Federal Ministry of Education and Research (BMBF) under reference number COSMIC-X 02J21D144, and supervised by Projektträger Karlsruhe (PTKA).

References

[1] F. Stodt and C. Reich, “A review on digital wallets and federated service for future of cloud services identity management”, in *Service Computation 2023: The Fifteenth International Conference on Advanced Service Computing, June 26, 2023 to June 30, 2023, Nice, France*, 2023, pp. 16–20.

[2] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: A brief review", *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 421–426, 2019.

[3] S. Rajamanickam, S. Vollala, R. Amin, and N. Ramasubramanian, "Insider attack protection: Lightweight password-based authentication techniques using ecc", *IEEE Systems Journal*, vol. 14, no. 2, pp. 1972–1983, 2019.

[4] G. Ra, T. Kim, and I. Lee, "Vaim: Verifiable anonymous identity management for human-centric security and privacy in the internet of things", *IEEE Access*, vol. 9, pp. 75 945–75 960, 2021.

[5] Z. Song, G. Wang, Y. Yu, T. Chen, *et al.*, "Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior", *Security and Communication Networks*, vol. 2022, 2022.

[6] D. R. Malik, D. A. Kataria, and D. N. Nandal, "Analysis of digital wallets for sustainability: A comparative analysis between retailers and customers", *International Journal of Management*, vol. 11, no. 7, 2020.

[7] S. Chuhan and V. Wojnas, "Designing and evaluating a resident-centric digital wallet experience", in *International Conference on Human-Computer Interaction*, Springer, 2023, pp. 591–609.

[8] B. Otto, "A federated infrastructure for european data spaces", *Communications of the ACM*, vol. 65, no. 4, pp. 44–45, 2022.

[9] D. Pöhn, M. Grabatin, and W. Hommel, "Modeling the threats to self-sovereign identities", *Open Identity Summit 2023*, 2023.

[10] M. M. Alam, A. E. Awawdeh, and A. I. B. Muhamad, "Using e-wallet for business process development: Challenges and prospects in Malaysia", *Business Process Management Journal*, vol. 27, no. 4, pp. 1142–1162, 2021.

[11] M. Chen *et al.*, "Research on identity authentication of IoT devices based on blockchain", in *2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems (ICPICS)*, IEEE, 2022, pp. 458–465.

[12] M. A. Hassan and Z. Shukur, "Device identity-based user authentication on electronic payment system for secure e-wallet apps", *Electronics*, vol. 11, no. 1, p. 4, 2022.

[13] S. Gajek, H. Löhr, A.-R. Sadeghi, and M. Winandy, "Truwallet: Trustworthy and migratable wallet-based web authentication", in *Proceedings of the 2009 ACM workshop on Scalable trusted computing*, 2009, pp. 19–28.

[14] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials", *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021.

[15] R. Dhamija and L. Dusseault, "The seven flaws of identity management: Usability and security challenges", *IEEE Security & Privacy*, vol. 6, no. 2, pp. 24–29, 2008.

[16] B. Zwattendorfer, T. Zefferer, and K. Stranacher, "An overview of cloud identity management-models.", *WEBIST (1)*, pp. 82–92, 2014.

[17] B. Pfitzmann and M. Waidner, "Privacy in browser-based attribute exchange", in *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, 2002, pp. 52–62.

[18] N. Selvanathan, D. Jayakody, and V. Damjanovic-Behrendt, "Federated identity management and interoperability for heterogeneous cloud platform ecosystems", in *Proceedings of the 14th International conference on Availability, Reliability and Security*, 2019, pp. 1–7.

[19] S.-H. Kim, S.-R. Cho, and S.-H. Jin, "Context-aware service system architecture based on identity interchange layer", in *2008 10th International Conference on Advanced Communication Technology*, IEEE, vol. 2, 2008, pp. 1482–1486.

[20] A. Abraham, C. Schinnerl, and S. More, "SSI strong authentication using a mobile-phone based identity wallet reaching a high level of assurance.", in *SECRYPT*, 2021, pp. 137–148.

[21] T. South and R. Mahari, "Justice in a vaccum?", 2023.

[22] A. Kudra, "Self-sovereign identity (SSI) in deutschland: Projekte mit strahlkraft für die globale community", *Datenschutz und Datensicherheit-DuD*, vol. 46, no. 1, pp. 22–26, 2022.

[23] M. Gaedke, J. Meinecke, and M. Nussbaumer, "A modeling approach to federated identity and access management", in *Special interest tracks and posters of the 14th international conference on World Wide Web*, 2005, pp. 1156–1157.

[24] N. Jahnke and B. Otto, "Data catalogs in the enterprise: Applications and integration", *Datenbank-Spektrum*, pp. 1–8, 2023.

[25] V. Siska, V. Karagiannis, and M. Drobics, "Building a dataspace: Technical overview", 2023.

[26] S. Santhar, A. Das, M. Thomas, and S. Prasad, "Self-describing digital assets and their applications in an integrated science and engineering ecosystem", in *Accelerating Science and Engineering Discoveries Through Integrated Research Infrastructure for Experiment, Big Data, Modeling and Simulation: 22nd Smoky Mountains Computational Sciences and Engineering Conference, SMC 2022, Virtual Event, August 23–25, 2022, Revised Selected Papers*, Springer Nature, 2023, p. 274.

[27] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security SLAs for federated cloud services", in *2011 Sixth International Conference on Availability, Reliability and Security*, IEEE, 2011, pp. 202–209.

[28] M. R. Ahmed, A. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey", *IEEE Access*, vol. 10, pp. 113 436–113 481, 2022.

[29] P. N. Mahalle and P. N. Railkar, *Identity Management for Internet of Things*. CRC Press, 2022.

[30] M. Forti, "A legal identity for all through artificial intelligence: Benefits and drawbacks in using AI algorithms to accomplish SDG 16.9", in *The Ethics of Artificial Intelligence for the Sustainable Development Goals*, Springer, 2023, pp. 253–267.

[31] K. Lampropoulos, N. Kyriakoulis, and S. Denazis, "Identity management through a global discovery system based on decentralized identities", *arXiv preprint arXiv:2212.02185*, 2022.

[32] R. V. Manikandan, K. Gurunathan, D. Ravindran, M. Sanjai, and V. P. Raja, "An novel algorithm for cloud secure storage using cloud dispersion and block chain system", in *2023 4th International Conference on Signal Processing and Communication (ICSPC)*, IEEE, 2023, pp. 372–376.

[33] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications", *Information Processing & Management*, vol. 59, no. 6, p. 103 061, 2022.

[34] C. Cuijpers and J. Schroers, "eIDAS as guideline for the development of a pan european eID framework in FutureID", 2014.