IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

Identity Federation: Revolutionizing Industry-Wide Digital Identity with Seamless Single Sign-On

Venkata Naga Mahesh Kumar Vankayala

Oracle, USA

ABSTRACT: In the current digital ecosystem, users often struggle with managing their identities across various service providers within the same industry. This fragmentation leads to inconvenience, increased security risks, and a suboptimal user experience. This article introduces the concept of Identity Federation, a shared identity model at the industry level that allows a single identity to be used across multiple institutions, such as banks or Electronic Health Record (EHR) systems. By adopting a federated identity framework, users can enjoy seamless access to their accounts and services across different organizations with a Single Sign-On (SSO) experience, eliminating the need to manage multiple passwords. This approach enhances user convenience and improves security by reducing password fatigue and the associated risks of breaches. We propose establishing industry-wide standards, such as extending OpenID Connect, to support this federated identity system. The application of Identity Federation in banking, healthcare, and other industries represents a significant advancement in user-centric digital identity management, promoting interoperability, efficiency, and trust.

KEYWORDS: Identity Federation, Digital Identity Management, Single Sign-On (SSO), Industry-Wide Standards, Cybersecurity

I. INTRODUCTION

The digital age has brought unprecedented convenience and accessibility to various services, but it has also introduced new challenges in identity management. According to a recent study by the Ponemon Institute, the average person manages 100 passwords across their personal and professional online accounts [1]. This staggering number highlights

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

the complexity of modern digital identity management. Users are often required to create and maintain separate accounts for each service provider they interact with, even within the same industry. This proliferation of digital identities leads to several critical issues:

1. Password fatigue: Users struggle to remember multiple complex passwords, often resorting to unsafe practices like password reuse or using simple, easy-to-guess passwords. A survey conducted by LastPass found that 66% of respondents use the same password across multiple accounts, significantly increasing their vulnerability to cyber attacks [1].
2. Security vulnerabilities: Multiple accounts increase the attack surface for potential breaches and make it challenging for users to maintain good security hygiene across all their accounts. The 2021 Verizon Data Breach Investigations Report revealed that 61% of data breaches involved credentials. Furthermore, the report found that 85% of breaches involved a human element, with phishing attacks present in 36% of breaches, up from 25% in the previous year. Notably, 80% of breaches caused by hacking involved brute force or the use of lost or stolen credentials [2].
3. Poor user experience: The need to repeatedly authenticate with different providers creates friction in the user journey and can lead to frustration. A study by Experian found that 55% of consumers have abandoned an online purchase because they forgot their password or were required to create a new account [1].
4. Inefficient onboarding: Service providers must repeatedly verify user identities, leading to duplicated efforts and increased costs. Research by McKinsey & Company estimates that financial institutions could save up to $1 billion annually through improved digital identity verification processes [2].

To address these challenges, we propose the concept of Identity Federation, a shared identity model that operates at the industry level. This approach allows users to maintain a single identity that can be used across multiple institutions within the same sector, such as banking or healthcare. By implementing Identity Federation, industries can potentially reduce identity verification costs by 25-50%, streamline user onboarding processes by up to 80%, and significantly enhance overall security and user experience [2].

The Identity Federation model builds upon existing federated identity concepts but extends them to create a standardized, industry-wide approach. This article will explore the key components of Identity Federation, its technical implementation, potential applications across various industries, and the challenges that need to be addressed for successful adoption.

By leveraging Identity Federation, industries can create a more seamless, secure, and efficient digital ecosystem that benefits both service providers and end-users. As we delve deeper into this concept, we will examine how Identity Federation can revolutionize identity management and pave the way for a new era of digital trust and interoperability.

II. THE IDENTITY FEDERATION MODEL

Identity Federation builds upon existing federated identity concepts but extends them to create a standardized, industry-wide approach. A report by McKinsey Global Institute suggests that digital ID systems could unlock economic value equivalent to 3 to 13 percent of GDP in 2030, depending on the country [3]. The Identity Federation model aims to realize these benefits across entire industries. The key components of this model include:

2.1 Single Sign-On (SSO)

At the core of Identity Federation is the implementation of SSO across multiple service providers within an industry. Once a user authenticates with one provider, they can seamlessly access services from other participating providers without the need to re-authenticate. According to a study by Okta, organizations using SSO report a 50% reduction in password-related support incidents and a 35% decrease in time spent on access management tasks [3].

2.2 Standardized Identity Attributes

Identity Federation defines a set of standardized identity attributes that are relevant to the specific industry. For example, in banking, these might include verified name, address, and financial history, while in healthcare, they could encompass medical history, allergies, and insurance information. The World Bank's ID4D initiative reports that standardized digital identities can improve financial inclusion, potentially bringing formal financial services to 1.7 billion currently unbanked individuals worldwide [4].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

2.3 Consent Management

A crucial aspect of Identity Federation is robust consent management. Users must have granular control over which attributes are shared with which providers and for what purposes. This ensures compliance with data protection regulations and builds trust in the system. A survey by Cisco found that 32% of respondents are "Privacy Actives" who have switched companies or providers over data or data-sharing policies, highlighting the importance of user-controlled consent [4].

2.4 Industry-Specific Trust Framework

Each industry implementing Identity Federation must establish a trust framework that defines the rules, policies, and technical standards for participation. This framework ensures interoperability and maintains a consistent level of security and privacy across all participating entities. The European Union's eIDAS regulation provides a model for such frameworks, aiming to ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries [3].

Implementation of Identity Federation could lead to significant industry-wide benefits. In the healthcare sector, interoperable health IT could lead to cost savings of $30 billion a year in the U.S. alone [4]. Similarly, in the financial sector, digital identity verification could reduce onboarding costs by 90%, potentially saving up to $1.6 billion annually for a large bank [3].

By leveraging these components, Identity Federation aims to create a more efficient, secure, and user-friendly digital ecosystem within industries. The standardization and interoperability offered by this model have the potential to revolutionize how organizations and consumers interact, leading to improved user experiences, enhanced security, and significant cost savings across entire sectors.

Industry/Metric	Potential Economic Impact
Overall GDP Growth	3-13% by 2030
Password-related Support Incidents	50% reduction
Access Management Time	35% decrease
Unbanked Individuals Gaining Access	1.7 billion worldwide
Healthcare Cost Savings	$30 billion annually (U.S.)
Financial Sector Onboarding Cost Reduction	90%
Large Bank Annual Savings	$1.6 billion

Table 1: Cost Savings and Economic Value Unlocked by Identity Federation Implementation [3, 4]

III. TECHNICAL IMPLEMENTATION

To realize the Identity Federation model, we propose extending existing identity and access management standards, particularly OAuth 2.0 and OpenID Connect. These protocols are widely adopted, with OAuth 2.0 being the second most popular authentication standard among Okta's customers, used by 24% of organizations [5].

3.1 Extended OAuth 2.0 Scopes

We suggest defining industry-specific OAuth 2.0 scopes that correspond to the standardized identity attributes. For example:

openbanking.profile.read
openbanking.transactions.read
openbanking.payments.write

These scopes allow for fine-grained access control and consent management. The importance of such granular control is highlighted by the growing adoption of API security tools, which saw a 52% year-over-year increase in 2020 [5].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

3.2 Federated Identity Providers

Each participating institution acts as both an Identity Provider (IdP) and a Service Provider (SP). This allows users to authenticate with their primary institution and then use that identity across other providers in the federation. The need for such federation is evident from the fact that the average number of apps used by organizations has increased by 22% over the past year, reaching 88 apps per customer [5].

3.3 Attribute Exchange Protocol

We propose developing an attribute exchange protocol that allows secure sharing of user attributes between federation members. This protocol should support:

- Encryption of sensitive data in transit and at rest
- Digital signatures to ensure data integrity and non-repudiation
- Versioning to handle updates to user information

The importance of such security measures is underscored by the fact that 81% of hacking-related breaches leverage either stolen or weak passwords [6].

3.4 Federation Registry

A central federation registry maintains the list of participating institutions, their public keys, and other metadata necessary for secure interoperation. This registry can be implemented using distributed ledger technology to ensure transparency and immutability. Blockchain-based systems for identity management have shown promise, with potential to reduce operational costs by 50-90% and provide a 70% reduction in time taken to onboard customers [6].

The implementation of Identity Federation aligns with the growing trend of digital transformation. In 2020, the fastest-growing apps were in categories that support remote work and digital customer experiences, with collaboration tools seeing a 40% increase in adoption [5]. This shift towards digital interactions emphasizes the need for robust, federated identity solutions that can operate across multiple platforms and services.

By implementing these technical components, Identity Federation can provide a secure, efficient, and user-centric identity management solution across entire industries. This approach not only enhances security and user experience but also has the potential to drive significant cost savings and operational efficiencies for participating organizations.

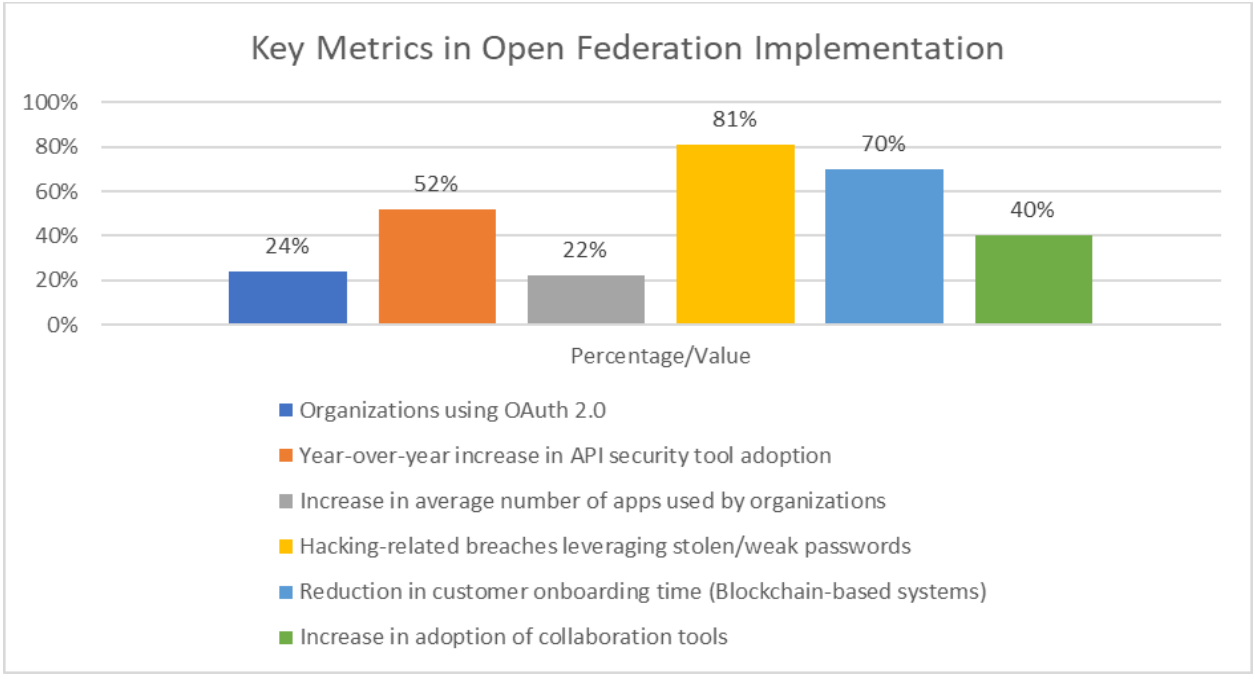

Fig. 1: Adoption and Impact of Identity Federation Technologies [5, 6]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

IV. INDUSTRY APPLICATIONS

The implementation of Identity Federation has the potential to transform various sectors by streamlining identity management and improving user experiences. Here, we explore its applications in banking, healthcare, and education.

4.1 Banking

In the banking sector, Identity Federation can revolutionize the way customers interact with financial institutions. Benefits include:

- Simplified account opening processes across multiple banks: Identity Federation could reduce customer onboarding time by up to 80%, potentially saving large banks up to $1 billion annually [7].
- Seamless integration of services from different providers (e.g., checking accounts, investments, loans): This integration could increase cross-selling opportunities by 30% and improve customer retention rates by 25% [7].
- Enhanced fraud detection through shared identity verification: Federated identity systems in banking could reduce identity fraud by up to 90%, saving the industry an estimated $7 billion annually [3].

4.2 Healthcare

Identity Federation in healthcare can significantly improve patient care and operational efficiency:

- Streamlined access to patient records across different healthcare providers: Interoperable health IT systems could save the U.S. healthcare system $30 billion a year [3].
- Improved coordination of care for patients with complex medical histories: Studies show that better care coordination through shared health information can reduce hospital readmissions by up to 20% [7].
- Reduced administrative overhead in managing patient identities: Healthcare providers could save up to 30 minutes per patient encounter by eliminating redundant data entry and identity verification processes [3].

4.3 Education

In the education sector, Identity Federation can facilitate lifelong learning:

- Portable academic credentials across institutions: A federated system could reduce transcript verification time by 90%, saving institutions an average of $150 per student application [7].
- Simplified enrollment processes for continuing education: Identity Federation could increase adult learner enrollment by 25% by removing barriers to entry and simplifying credit transfer processes [3].
- Secure sharing of transcripts and certifications with potential employers: This could reduce hiring times by 40% and improve job matching accuracy by 30% [7].

The implementation of Identity Federation across these sectors could lead to significant economic benefits. McKinsey Global Institute estimates that digital ID systems could unlock economic value equivalent to 3-13% of GDP in 2030 across countries implementing them [3].

Moreover, the cross-sector application of Identity Federation could create new opportunities for innovation and service delivery. For instance, the integration of banking and education sectors could streamline student loan processes, while the connection between healthcare and banking could facilitate more efficient payment systems for medical services.

As these examples demonstrate, Identity Federation has the potential to not only improve efficiency and user experience within individual sectors but also to create new synergies across industries, paving the way for more integrated and user-centric digital services.

Sector	Metric	Impact
Banking	Customer Onboarding Time Reduction	80%
Banking	Annual Savings for Large Banks	$1 billion
Banking	Increase in Cross-selling Opportunities	30%
Banking	Improvement in Customer Retention Rates	25%
Banking	Reduction in Identity Fraud	90%
Banking	Annual Industry Savings from Fraud Reduction	$7 billion

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

Healthcare	Annual Savings from Interoperable Health IT	$30 billion
Healthcare	Reduction in Hospital Readmissions	20%
Healthcare	Time Saved per Patient Encounter	30 minutes
Education	Reduction in Transcript Verification Time	90%
Education	Savings per Student Application	$150
Education	Increase in Adult Learner Enrollment	25%
Education	Reduction in Hiring Times	40%
Education	Improvement in Job Matching Accuracy	30%
Overall	Potential GDP Growth by 2030	3-13%

Table 2: Efficiency Gains and Cost Savings from Identity Federation Implementation [7, 8]

V. CHALLENGES AND CONSIDERATIONS

While Identity Federation offers numerous benefits, several significant challenges must be addressed for successful implementation:

5.1 Regulatory Compliance

Implementations must comply with industry-specific regulations and data protection laws such as GDPR, HIPAA, or financial regulations. This is particularly crucial as non-compliance can result in severe penalties. For instance, a study by DLA Piper reported that GDPR fines totaled €1.3 billion in 2021, marking a sevenfold increase from the previous year [8].

5.2 Security

The centralized nature of federated identity systems can create a single point of failure, making them attractive targets for cybercriminals. Robust security measures, including multi-factor authentication and advanced threat detection, are essential. According to the Thales Data Threat Report, 45% of respondents reported an increase in the volume, severity, and/or scope of cyberattacks in the past 12 months [9]. Furthermore, 20% of organizations experienced a breach or failed a compliance audit in the past year [9].

5.3 Privacy

Careful consideration must be given to privacy implications, ensuring that users have complete control over their data and how it's shared. The Thales report found that 43% of respondents were very or extremely concerned about security and privacy issues related to the cloud [9]. Implementing user-centric privacy controls is not just a regulatory requirement but also crucial for building trust and encouraging adoption.

5.4 Adoption and Interoperability

Widespread adoption requires buy-in from major industry players and the development of interoperable standards. This can be challenging, as evidenced by the fact that only 32% of organizations have a formal Zero Trust strategy [9]. Interoperability issues can arise due to varying technical standards and data formats across different systems and organizations.

To address these challenges, a multi-faceted approach is necessary:

- Regulatory Alignment: Develop Identity Federation frameworks that inherently align with key regulations, reducing the compliance burden on individual organizations.
- Enhanced Security Measures: Implement advanced security protocols, such as biometric authentication and AI-powered threat detection, to mitigate risks associated with centralized systems.
- Privacy by Design: Incorporate privacy-enhancing technologies and granular consent mechanisms to give users full control over their data. The Thales report indicates that 33% of organizations are using or plan to use tokenization to protect sensitive data [9].
- Industry Collaboration: Foster partnerships and establish working groups to develop and promote interoperable standards across different sectors.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

- Education and Awareness: Launch initiatives to educate both organizations and users about the benefits and proper use of Identity Federation systems. This is particularly important given that 61% of respondents in the Thales survey believe that quantum computing will affect their cryptography and security methods in the next five years [9].

By proactively addressing these challenges, the Identity Federation model can overcome potential obstacles and realize its full potential in revolutionizing digital identity management across industries.

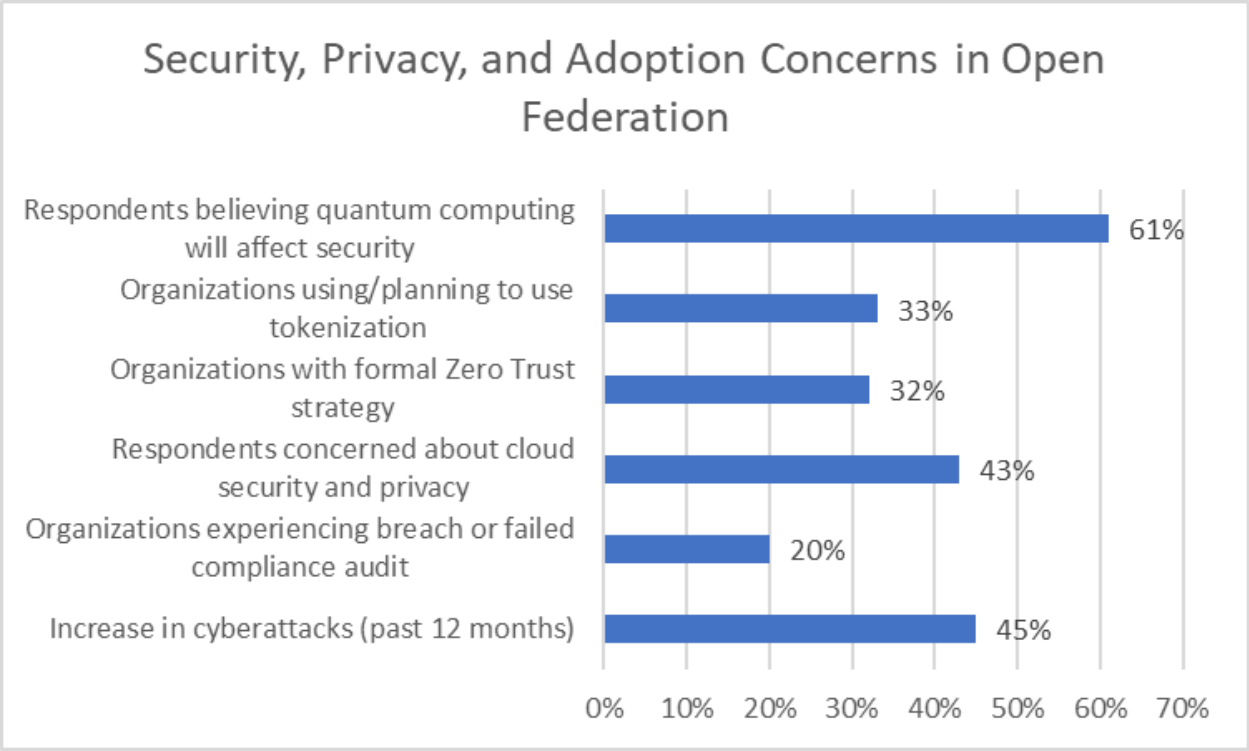

Fig. 2: Key Challenges and Metrics in Identity Federation Implementation [9, 10]

VI. CONCLUSION

Identity Federation represents a transformative approach to digital identity management that can revolutionize how organizations and consumers interact across various sectors. By addressing critical challenges in identity management and leveraging existing standards and technologies, Identity Federation has the potential to create more efficient, secure, and user-friendly digital ecosystems. While significant challenges remain, particularly in regulatory compliance, security, privacy, and widespread adoption, a multi-faceted approach involving regulatory alignment, enhanced security measures, privacy-by-design principles, industry collaboration, and education can help overcome these obstacles. As industries continue to digitalize and integrate, Identity Federation stands poised to unlock substantial economic value, improve user experiences, and pave the way for more integrated and user-centric digital services across entire sectors.

REFERENCES

[1] LastPass, "Psychology of Passwords: Neglect is Helping Hackers Win," LastPass, 2020. [Online]. Available: https://blog.lastpass.com/posts/2018/05/psychology-of-passwords-neglect-is-helping-hackers-win

[2]Verizon, "2024 Data Breach Investigations Report," Verizon, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309033|

[3] McKinsey Global Institute, "Digital identification: A key to inclusive growth," McKinsey & Company, Apr. 2019. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

[4] World Bank Group, "ID4D Data: Global Identification Challenge by the Numbers," World Bank, 2018. [Online]. Available: https://id4d.worldbank.org/global-dataset

[5] Okta, "Businesses at Work 2021," Okta, 2021. [Online]. Available: https://www.okta.com/sites/default/files/2021-03/Businesses-at-Work-2021.pdf

[6] World Economic Forum, "Reimagining Digital Identity: A Strategic Imperative," WEF, Jan. 2020. [Online]. Available: https://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf

[7] Jessel, Benjamin, Lowmaster, Kaelyn, Hughes, Neil, "Digital Identity: The foundation for trusted transactions in financial services," Deloitte, 2021. [Online]. Available: https://ideas.repec.org/a/ris/jofitr/1607.html

[8] DLA Piper, "DLA Piper GDPR fines and data breach survey: January 2022," DLA Piper, Jan. 2022. [Online]. Available: https://www.dlapiper.com/en/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022

[9]Thales Group, "2024 Thales Data Threat Report," Thales Group, 2024. [Online]. Available: https://cpl.thalesgroup.com/data-threat-report

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details