DIGITAL IDENTITY TOWARDS SHARED PRINCIPLES FOR PUBLIC SECTORS ENTERPRISES

A Dissertation Submitted to the Office of the Dean, Faculty of Management in Partial Fulfillment of the Requirements for the Master of Business Studies (M.B.S.)

By:

Rohit Shrestha

Shanker Dev Campus

Campus Roll No.: 996/078

Exam Symbol No: 48202/023

T.U. Regd. No: 6-2-0040-0335-2015

Specialization: Finance

Kathmandu, Nepal

July, 2025

CERTIFICATE OF AUTHORSHIP

I hereby corroborate that I have researched and submitted the final draft of dissertation entitled **Digital Identity towards Shared Principles for Public Sectors Enterprises.** The work of this dissertation has not been submitted previously for the purpose of conferral of any degrees nor it has been proposed and presented as part of requirements for any other academic purposes. The assistance and cooperation that I have received during this research work has been acknowledged. In addition, I declare that all information sources and literature used are cited in the reference section of the dissertation.

.....

Rohit Shrestha

July, 2025

REPORT OF RESEARCH COMMITTEE

Mr. Rohit Shrestha has defended research proposal entitled **DIGITAL IDENTITY TOWARDS SHARED PRINCIPLES FOR PUBLIC SECTORS ENTERPRISES** successfully. The research committee has registered the dissertation for further progress. It is recommended to carry out the work as per suggestion and guidance of supervisor Indra Bahadur Bohara submit the dissertation for evaluation and vice-voce examination.

Indra Bahadur Bohara
Position……
Signature……

Dissertation Proposal Defended Date:
……

Dissertation Proposal Defended Date:
……

Asso. Prof. Dr. Sajeeb Kumar Shrestha
Head of Research Committee
Signature……

Dissertation Viva Voce Date:
……

APPROVAL SHEET

We have examined the dissertation entitled **DIGITAL IDENTITY TOWARDS SHARED PRINCIPLES FOR PUBLIC SECTORS ENTERPRISES** presented by Mr. Rohit Shrestha for the degree of Master of Business Studies (MBS Semester). We hereby certify that the dissertation acceptable for the award of degree.

.....
Indra Bahadur Bohara
Dissertation Supervisor

.....
Internal Examiner

.....
Internal Expert

.....
External Expert

.....
Asso. Prof. Dr. Sajeeb Kumar Shrestha
Chairperson Research Committee
.....

Asso. Prof. Dr. Kapil Khanal
Campus Chief

ACKNOWLEDGEMENTS

First of all, I would like to thank Tribhuvan University for giving chance to prepare the dissertation for a partial requirement to the fulfillment of Master Degree of Business Studies program held under Tribhuvan University. After many months of hard work and sincere effort from my side, this research has been conducted. I would like to acknowledge the following notable personalities who have contributed their valuable efforts in different ways in creation of this research. I would express my profound gratitude to my dissertation supervisor Indra Bahadur Bohara of Shanker Dev Campus for his valuable guidance and kind support to me all the way through this dissertation his co-operation in the revision of this dissertation has precisely helped me to groom and bring it in this form.

I would like to express cordial gratitude to Asso. Prof. Dr. Sajeeb Kumar Shrestha, Chairman of Research Committee for this timely and continuous guidance throughout the study. Likewise, I am grateful to Asso. Prof. Dr. Kapil Khanal, campus chief and also highly appreciate the efforts of all teacher and other members of Shanker Dev Campus. I want to give thanks for the staff members of campus library who provided the reference and regarding materials during the period of research.

I also owe deep gratitude to all reputed authors whose writings have provided me the necessary guidance and invaluable materials for the enrichment of my research papers in all possible ways. My special appreciation goes to my colleague and to all my family members, teachers and friends for their continuous encouragement and help to complete this work directly or indirectly. Perfection is anything can hardly be thought of knowing the universal fact "Human is Error", I Have taken utmost care to avoid errors, but I know they are inescapable, so I shall be obliged if they are forgiven.

Rohit Shrestha
Shanker Dev Campus
July, 2025

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

ABBREVIATIONS

EDII	:	Effectiveness of Digital Identity Implementation
IA	:	Inclusiveness and Accessibility
ICL	:	Institutional Capacity and Leadership
MBS	:	Master of Business Studies
PRR	:	Policy and Regulatory Readiness
SC	:	Stakeholder Collaboration
SPSS	:	Statistical Package for Social Science
TI	:	Technological Infrastructure
TU	:	Tribhuvan University
UTPP	:	User Trust and Privacy Perception
WB	:	World Bank

ABSTRACT

This study investigates the effectiveness of digital identity implementation (EDII) in Nepalese public sector enterprises by examining the influence of six key factors: policy and regulatory readiness (PRR), technological infrastructure (TI), institutional capacity and leadership (ICL), user trust and privacy perception (UTPP), inclusiveness and accessibility (IA), and stakeholder collaboration (SC). The primary objectives were to assess the current implementation status of these variables, explore their interrelationships, and analyze their impact on public trust in digital identity systems. Employing a descriptive and causal research design, data were collected from 384 respondents in Kathmandu Valley through a structured online questionnaire. The study used statistical techniques, including mean analysis, correlation, and multiple regression, to examine the relationships among the independent variables (PRR, TI, ICL, UTPP, IA, SC) and their collective effect on the dependent variable (EDII). Findings indicate that while digital identity principles are moderately implemented across Nepal's public sector, technological infrastructure (TI), institutional capacity and leadership (ICL), inclusiveness and accessibility (IA), and stakeholder collaboration (SC) exhibit higher levels of readiness and impact compared to policy and regulatory readiness (PRR). Correlation results demonstrate significant positive relationships among most variables, emphasizing their interconnected role in supporting effective digital identity implementation. Regression analysis confirms that TI, ICL, UTPP, IA, and SC significantly enhance EDII, thereby fostering public trust in digital identity systems. However, policy and regulatory readiness (PRR) showed a less pronounced effect in this context. Overall, the study highlights the critical need for a comprehensive approach that integrates technological capabilities, institutional leadership, inclusive access, and collaborative governance to build trusted and effective digital identity frameworks. These insights provide valuable guidance for policymakers, managers, and stakeholders striving to improve digital identity adoption and strengthen public trust within Nepal's public sector.

Keywords: Digital identity implementation, policy and regulatory readiness, technological infrastructure, institutional capacity, user trust, inclusiveness, stakeholder collaboration, public trust

CHAPTER I

INTRODUCTION

1.1 Background of the Study

The emergence of digital identity systems has become a cornerstone of digital governance, enabling more efficient, transparent, and inclusive service delivery across both developed and developing nations. As the world increasingly transitions toward e-governance, digital identity serves not only as a tool for authentication but as a gateway to public services, financial inclusion, and civil participation (Anand & Brass, 2021; Giannopoulou, 2023). These systems integrate technologies such as biometrics, blockchain, and cryptography to securely verify individuals and manage personal data in real-time transactions (Masiero & Bailur, 2021).

Globally, initiatives like Estonia's eID, India's Aadhaar, and the European Union's eIDAS demonstrate how digital identities can streamline bureaucratic processes, reduce fraud, and enhance administrative efficiency (Abraham, 2020; Kanwar et al., 2022).

Despite these advantages, the development of inclusive and trustworthy digital identity systems is still evolving, especially in public sector enterprises of lower-middle-income countries. Concerns about data misuse, lack of privacy safeguards, fragmented frameworks, and poor interoperability remain critical challenges (Landrigan et al., 2024; Rosner, 2014).

Many governments have not yet established universally agreed-upon principles to guide the implementation of digital identity systems, resulting in inconsistencies in design, user accessibility, and data protection (Allmann & Radu, 2023; Nishant & Brass, 2021). To mitigate these risks and ensure responsible use, several scholars and institutions advocate for shared principles that include inclusivity, transparency, user-centricity, and cross-sector collaboration (Jonathan, 2020; Klaaren, 2023).

In Nepal, digital transformation in the public sector has gained momentum through frameworks like the Digital Nepal Framework (2019) and platforms such as the Nagarik App, designed to provide centralized access to citizen services. The recent integration of the National Identity Card (NID) with digital services reflects growing efforts to streamline public administration (Online Khabar, 2025; Kathmandu Post, 2022). However, these efforts face structural limitations due to inadequate legal infrastructure, poor cyber security preparedness, and a persistent digital divide, particularly in rural and marginalized regions

(Singh, as cited in Kathmandu Post, 2022; Masiero & Bailur, 2021). The lack of a clearly defined and locally adapted framework for digital identity raises concerns about data privacy, equity, and long-term sustainability.

To maximize the transformative potential of digital identity in Nepal's public sector, it is essential to adopt shared guiding principles tailored to the country's socio-economic landscape. These principles should support cross-platform interoperability, foster citizen trust, ensure inclusion, and provide robust legal and technological safeguards (Sunil, 2020; Anandaram et al., 2021). Furthermore, collaboration between government, private sector, and civil society is key to building scalable, transparent, and people-centered digital identity ecosystems (Giannopoulou, 2023; Nishant & Brass, 2021). Without such coordinated and principled approaches, the digital divide may deepen, and the risks of exclusion and data exploitation may outweigh the intended benefits of digital governance.

Digital identity, when designed and implemented responsibly, can be a catalyst for achieving Nepal's development goals by ensuring inclusive access to government schemes, improving delivery mechanisms, and reducing corruption. Thus, the formulation of shared principles becomes not just a technical or administrative requirement but a national development imperative.

1.2 Problem Statement

Digital identity has become a cornerstone for delivering public services efficiently and securely in the digital age. For public sector enterprises, which include government agencies and state-owned organizations, implementing digital identity systems is crucial to providing seamless access to services while ensuring trust, privacy, and security. As governments worldwide move toward digital transformation, the need for shared guiding principles to govern the development and use of digital identity systems has become increasingly important. These shared principles help harmonize efforts across various agencies and sectors, fostering interoperability, accountability, and inclusiveness.

At the core of these principles lies the emphasis on user-centricity, which ensures that digital identity systems serve the needs of individuals, empowering them with control over their personal data and consent mechanisms. Public sector enterprises must prioritize transparency by clearly communicating how identity data is collected, stored, and used. This transparency is essential for building citizen trust and encouraging broader adoption of digital identity services.

Another fundamental principle is security and privacy by design. Given the sensitive nature of identity information, public sector enterprises must embed robust cybersecurity measures to protect data against unauthorized access, breaches, and misuse. Adhering to strict privacy standards, including data minimization and purpose limitation, prevents unnecessary data exposure and supports compliance with legal frameworks.

Inclusiveness and accessibility also form vital components of shared principles. Public sector digital identity initiatives must account for the diverse demographics they serve, including marginalized and vulnerable populations who might face barriers due to geographic, economic, or social factors. Ensuring equitable access to digital identity services is essential to avoid deepening existing inequalities.

Moreover, interoperability and standardization are critical to enabling seamless interactions across different government agencies and between public and private sectors. Shared technical standards and protocols allow various systems to communicate securely and efficiently, thereby enhancing the overall effectiveness of public service delivery.

Despite the growing global momentum toward digital transformation, many governments especially in developing countries like Nepal continue to face systemic challenges in implementing secure, inclusive, and interoperable digital identity systems within public sector enterprises. The absence of a unified framework grounded in shared principles such as privacy, inclusiveness, interoperability, and transparency has led to fragmented implementations across institutions, resulting in inefficiencies, redundancy, and user exclusion (Anand & Brass, 2021; Giannopoulou, 2023). In Nepal, although initiatives like the National Identity Card (NID) and the Nagarik App mark significant progress toward e-governance, these platforms operate within siloed ecosystems that lack coherent legal and technological alignment (Online Khabar, 2025; Kathmandu Post, 2022).

The sensitive nature of biometric and identity-related data necessitates stringent governance, yet Nepal has not established a comprehensive data protection law that aligns with international best practices (Masiero & Bailur, 2021; Klaaren, 2023). This regulatory gap, compounded by weak coordination among public sector entities, undermines public confidence in digital systems and heightens the risk of data misuse or breach. Citizens, particularly in rural and marginalized communities, remain disproportionately affected due to limited access to internet infrastructure, low digital literacy, and socio-economic exclusion (Nishant & Brass, 2021; Landrigan et al., 2024).

The lack of standardized protocols for interoperability restricts the ability of digital identity systems to function seamlessly across different platforms and sectors, reducing their efficiency and scalability. International cases highlight the importance of a principled and rights-based approach to digital identity, yet Nepal has yet to fully adapt these lessons within its socio-political context (Kanwar et al., 2022; Abraham, 2020).

Nepal's public sector digital identity initiatives face critical policy, infrastructural, and institutional deficiencies that hinder their effective implementation. Without the adoption of shared principles such as user-centricity, inclusiveness, privacy by design, and transparent governance Nepal risks creating a fragmented and inequitable digital identity ecosystem. Addressing these gaps is essential not only for improving public service delivery but also for strengthening trust, accountability, and democratic participation in Nepal's digital governance landscape (Allmann & Radu, 2023; Anandaram et al., 2021). The research problems of the study are presented as follows:

- What is the current status and implementation pattern of shared digital identity principles (such as user-centricity, privacy, interoperability, inclusiveness, and security) across public sector enterprises in Nepal?
- What is the relationship between adherence to shared digital identity principles and public trust in digital services provided by Nepalese public sector enterprises?
- Do shared digital identity principles namely user-centricity, inclusiveness, interoperability, privacy, security, and transparency have impact on public trust in digital identity systems within public sector enterprises in Nepal?

1.3 Objectives of the Study

To explore the implementation, relationships, and impact of shared digital identity principles on public trust within public sector enterprises in Nepal. The specific objectives of the study are as follows:

- To assess the current status and implementation patterns of shared digital identity principles including user-centricity, privacy, interoperability, inclusiveness, and security within Nepalese public sector enterprises.
- To examine the relationship between the implementation of shared digital identity principles and public trust in digital services provided by Nepalese public sector organizations.

- To analyze the impact of key digital identity principles (user-centricity, inclusiveness, interoperability, privacy, security, and transparency) on public trust in digital identity systems in the context of Nepal's public sector.

1.4 Research Hypothesis

The research hypothesis of the study are as follows:

- H1: There is a significant impact of user-centricity on public trust in digital identity systems within public sector enterprises in Nepal.
- H2: There is a significant impact of privacy and data protection on public trust in digital identity systems within public sector enterprises in Nepal.
- H3: There is a significant impact of interoperability on public trust in digital identity systems within public sector enterprises in Nepal.
- H4: There is a significant impact of inclusiveness on public trust in digital identity systems within public sector enterprises in Nepal.
- H5: There is a significant impact of security on public trust in digital identity systems within public sector enterprises in Nepal.
- H6: There is a significant impact of transparency and accountability on public trust in digital identity systems within public sector enterprises in Nepal.

1.5 Rationale of the Study

The integration of digital identity systems into public governance has become increasingly critical in the digital era, reshaping how governments interact with citizens and deliver essential services. As public sector enterprises adopt digital platforms, the establishment of shared guiding principles such as user-centricity, security, inclusivity, interoperability, and privacy has emerged as a necessary foundation for building trustworthy and effective digital identity systems. This study is particularly significant in the context of Nepal, where digital transformation is still evolving, and systemic challenges such as low digital literacy, infrastructure deficits, and weak regulatory frameworks continue to hinder inclusive and secure implementation.

Nepal's efforts, including the introduction of the National Identity Card and the Nagarik App, demonstrate a growing commitment to digital governance. However, the absence of unified principles and frameworks has resulted in fragmented approaches across government agencies, reducing the effectiveness, security, and public acceptance of these digital systems. By exploring the shared principles that underpin successful digital identity

frameworks, this study aims to address these critical gaps and offer strategic direction for policymakers and public administrators.

The primary audience for this research includes government agencies, policy designers, and institutional stakeholders responsible for digital identity initiatives. The study will offer practical insights into developing coherent, interoperable, and inclusive systems that can reduce redundancy, improve service integration, and foster public trust in digital governance. By promoting principles such as transparency and citizen empowerment, the research supports the development of identity frameworks that align with both national development goals and international digital governance standards.

Beyond government institutions, the study also benefits broader stakeholder groups including citizens, technology developers, legal experts, and civil society organizations. For citizens, improved digital identity systems ensure equitable access to services such as health, education, and social protection, particularly in rural and marginalized communities. For developers and technology providers, clear guidelines on standards and interoperability can enhance the design secure and scalable systems. Similarly, legal practitioners and data protection authorities can use the findings to strengthen regulatory frameworks that uphold individual privacy and digital rights.

This study is driven by the urgent need to develop inclusive, transparent, and secure digital identity ecosystems within Nepal's public sector. By identifying and advocating for shared principles, the research contributes to enhancing governance efficiency, protecting citizen rights, and promoting sustainable digital development. It also provides a framework for other developing nations facing similar challenges, offering evidence-based recommendations for advancing digital identity initiatives that are equitable, secure, and widely trusted.

1.6 Limitations of the Study

The limitations of the study are as follow:

- This study is only based on primary data, data are collect through field study.
- Given the uneven development of digital infrastructure and institutional capacity across Nepal’s federal system, findings from selected public sector organizations may not fully represent the broader national landscape. This introduces potential sampling bias, particularly in rural or underserved regions.

- Nepal’s digital governance and policy frameworks are in flux, with ongoing reforms and initiatives. As such, the findings of this study may quickly become outdated or not fully capture emerging technologies, regulatory changes, or new stakeholder dynamics that influence digital identity implementation.
- Due to time and logistical constraints, the study may underrepresent direct user perspectives especially those from marginalized communities on trust, accessibility, and privacy. This limits a full understanding of grassroots-level challenges and societal acceptance of digital identity systems.

CHAPTER II

LITERATURE REVIEW

2.1 Theoretical Review

The related theoretical review are as follows:

Technology Acceptance Model (TAM) and Its Application to Digital Identity towards shared principles for Public Sector Enterprises

The Technology Acceptance Model (TAM), introduced by Fred Davis in 1989, is a foundational framework used to explain how individuals come to accept and use new technologies. TAM identifies two primary factors influencing technology adoption: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). Perceived Usefulness refers to the degree to which a person believes that using a particular system enhances their performance, while Perceived Ease of Use relates to the degree to which a person believes using the system requires minimal effort. These two factors influence the user's attitude towards the technology, which then affects their behavioral intention to use it and ultimately determines actual system usage (Davis, 1989).

In the context of digital identity systems within public sector enterprises, TAM offers valuable insights into how citizens and government officials accept and engage with these platforms. Digital identity is increasingly crucial for accessing a wide range of government services efficiently and securely. For such systems to be effective, they must be perceived as both useful and easy to use by their intended users. For example, a citizen is more likely to adopt a digital identity platform if it significantly simplifies access to services such as healthcare, tax payments, or social welfare, representing high Perceived Usefulness. Equally, if the system is designed with user-friendly interfaces and clear instructions, reducing the learning curve, Perceived Ease of Use will be enhanced, encouraging adoption.

This model is particularly pertinent in countries like Nepal, where digital literacy varies widely across regions and demographics. Incorporating TAM principles in designing digital identity systems helps ensure these platforms accommodate diverse user needs, promoting inclusiveness a core shared principle in public sector digital identity initiatives. Furthermore, recent studies extending TAM emphasize the importance of trust and security as additional factors influencing acceptance, especially relevant for digital identity, which

involves sensitive personal data (Venkatesh & Bala, 2008). Users must trust that their personal information is securely managed and that privacy is safeguarded for them to willingly adopt digital identity systems.

Applying TAM enables policymakers and system designers to identify and address barriers to adoption by enhancing system usability and demonstrating clear benefits to users. It also highlights the importance of communication and training initiatives that increase user confidence and familiarity with digital identity technologies. Consequently, TAM serves as a critical theoretical framework guiding the development of shared principles such as user-centricity, security, and transparency that underpin successful digital identity implementation in public sector enterprises.

Institutional Theory and Its Relevance to Digital Identity towards shared principles for Public Sector Enterprises

Institutional Theory provides a framework to understand how organizations conform to the norms, rules, and expectations of their broader social, political, and legal environments to gain legitimacy and ensure survival (DiMaggio & Powell, 1983). In the public sector, government agencies and enterprises do not operate in isolation but are heavily influenced by institutional forces such as laws, regulations, cultural norms, and international standards. These pressures shape the adoption and design of digital identity systems.

In the context of digital identity for public sector enterprises, Institutional Theory explains why and how governments adopt shared principles such as privacy protection, data security, interoperability, and inclusiveness. These principles are often codified in legal frameworks and policy guidelines, which institutions are compelled to follow to meet expectations of transparency, accountability, and public trust. For example, Nepal's efforts to develop its National Identity Card system and the Nagarik App are influenced by national laws and global digital governance standards, reflecting institutional pressures to modernize while safeguarding citizen rights.

Institutional Theory also highlights isomorphism, the process by which organizations within the same field tend to become similar over time due to coercive, mimetic, and normative pressures (DiMaggio & Powell, 1983). Coercive pressures come from regulations and government mandates; mimetic pressures arise when organizations imitate successful digital identity models from other countries; and normative pressures stem from professional standards and networks among public sector officials. This leads to the

emergence of shared principles that guide digital identity initiatives across public enterprises.

Furthermore, this theory stresses that for digital identity systems to be effective and widely accepted, institutional support is critical. This support includes legal frameworks that protect citizens' data privacy, organizational policies that enforce security standards, and professional training that fosters expertise in managing digital identity technologies. Without such institutional backing, digital identity systems risk fragmentation, inconsistency, and low trust among users.

In Nepal and similar contexts, Institutional Theory underscores the importance of aligning digital identity strategies with both national regulatory environments and international best practices. It suggests that building robust institutional frameworks and fostering inter-agency collaboration are essential to realizing the benefits of digital identity namely, improved service delivery, enhanced security, and greater citizen empowerment.

Privacy Calculus Theory and Its Application to Digital Identity towards shared principles for Public Sector Enterprises

Privacy Calculus Theory offers an important perspective on how individuals decide whether to disclose personal information in digital environments by weighing the perceived benefits against the potential privacy risks (Culnan & Bies, 2003). This decision-making process is particularly relevant in the development and adoption of digital identity systems within public sector enterprises, where sensitive personal data is collected, stored, and used to provide various services.

According to the theory, users conduct a cognitive trade-off, balancing the advantages such as convenience, improved access to services, and personalized experiences against the risks of data breaches, identity theft, or misuse of personal information. For citizens to trust and actively use digital identity platforms such as Nepal's National Identity Card and related e-governance applications they must feel confident that their privacy concerns are adequately addressed. This necessitates that public sector enterprises embed strong data protection measures and transparent privacy policies in their digital identity frameworks, reflecting shared principles of security and accountability.

Moreover, Privacy Calculus Theory suggests that transparency and control over personal data are key factors influencing user trust. When users perceive that they have control over what information is shared and how it is used, and when organizations clearly communicate

data handling practices, the perceived risks decrease, thereby increasing willingness to participate in digital identity systems (Li et al., 2010). This aligns with the international principles of digital identity, which emphasize user-centric privacy controls and informed consent.

In the Nepalese context, where awareness of data privacy may be limited and legislative frameworks are evolving, understanding privacy calculus helps policymakers design systems that reassure users and encourage adoption. For example, ensuring compliance with data protection laws and implementing security certifications can reduce perceived risks. Simultaneously, highlighting benefits such as faster government service delivery and reduced fraud strengthens the perceived benefits side of the calculus.

Ultimately, Privacy Calculus Theory guides public sector enterprises in balancing innovation with ethical responsibility, encouraging a digital identity environment where users feel secure enough to share personal data while benefiting from efficient public services.

Systems Theory and Its Relevance to Digital Identity towards shared principles for Public Sector Enterprises

Systems Theory, originally proposed by Ludwig von Bertalanffy in 1968, views organizations as complex, interconnected systems composed of interrelated parts working together toward common goals. This theory emphasizes the importance of understanding the holistic interactions within and between components to ensure effective functionality (Von Bertalanffy, 1968). When applied to digital identity in public sector enterprises, Systems Theory highlights the necessity of integration, coordination, and interoperability among various government agencies, databases, and service platforms.

Digital identity ecosystems involve multiple stakeholders, including citizens, public institutions, private partners, and technology providers. For these systems to function efficiently, they must operate as unified entities rather than isolated silos. This integration aligns with shared principles such as interoperability, standardization, and collaboration, which are essential for ensuring seamless user experiences and secure data exchanges across services (Checkland, 1999).

In the Nepalese context, digital identity implementation faces challenges like fragmented infrastructure, inconsistent data standards, and lack of inter-agency coordination. Systems Theory provides a framework to address these issues by promoting a holistic approach

designing and managing digital identity as part of an integrated system that includes technical, organizational, and policy components. This perspective encourages policymakers to foster partnerships, develop common standards, and build interoperable platforms that improve service delivery and data security.

Furthermore, Systems Theory stresses feedback loops and continuous adaptation, meaning that digital identity systems should evolve based on user feedback and changing needs, reinforcing the shared principles of transparency and responsiveness. By adopting this systems approach, public sector enterprises can enhance the resilience and scalability of digital identity platforms, ensuring they meet the diverse and dynamic demands of citizens and government functions.

In summary, Systems Theory offers a comprehensive lens through which digital identity initiatives can be planned and implemented in public sector enterprises. It underscores the importance of viewing digital identity not as an isolated technology but as an interconnected system that supports efficient, inclusive, and trustworthy public service delivery.

Identity Theory and Its Application to Digital Identity towards shared principles for Public Sector Enterprises

Identity Theory explores how individuals develop and maintain their sense of self through social roles and interactions within society (Stryker & Burke, 2000). It posits that identity is formed based on the roles people occupy, and these identities influence behavior and social expectations. In the digital age, this theory becomes particularly relevant when examining digital identity the representation of an individual’s identity in online and electronic environments, especially within public sector enterprises.

Digital identity systems serve as formal mechanisms through which individuals prove their authenticity to access government services, benefits, and rights. Applying Identity Theory to digital identity highlights the importance of ensuring that these systems respect users' self-conceptions and social roles. If digital identities accurately reflect the diverse roles a citizen holds such as voter, taxpayer, student, or healthcare recipient they can promote trust and engagement in digital government services (Jenkins, 2014).

Furthermore, Identity Theory underscores the need for digital identity platforms to support user control and autonomy over personal information. When users feel empowered to manage their digital identities and control how their data is shared, they are more likely to

accept and use these systems. This aligns with shared principles of transparency, consent, and user-centric design critical for successful digital identity implementation in public sectors. In the Nepalese context, where social roles are deeply intertwined with cultural and community identities, recognizing the multiplicity of identities a person holds is vital. Public sector digital identity systems should accommodate these complexities to ensure inclusivity and avoid marginalization. For instance, digital identity solutions must consider gender, ethnicity, and regional diversities to provide equitable access to government services. Finally, Identity Theory suggests that digital identities are dynamic and can evolve as individuals' social roles change over time. Public sector enterprises must therefore design flexible digital identity systems capable of adapting to these changes, ensuring the ongoing relevance and accuracy of identity data. Identity Theory provides a valuable lens for understanding how digital identities function in society and offers guidance for designing inclusive, user-centered digital identity frameworks that uphold citizens' dignity and social roles.

2.2 Empirical review

Bottarelli et al. (2025) assessed on the digital identity systems trustworthiness assessment framework (DISTAF), which evaluates electronic identity systems across six critical dimensions: security, privacy, ethics, resilience, robustness, and reliability. Designed to support government agencies and public institutions, the framework enables comprehensive life-cycle assessments of digital ID platforms. Using the Modular Open-Source Identity Platform (MOSIP) as a case study, the authors demonstrate how DISTAF can guide policymakers in ensuring system integrity and alignment with shared public sector values such as trust, resilience, and inclusivity. The framework is adaptable to emerging models, including decentralized and self-sovereign identity systems.

Stefanson (2025) examined on trust in various digital authentication methods used for public services in Iceland, a country where geographical challenges make digital access essential. Through a national survey, the authors find high public trust across demographics in e-ID systems, despite historical low institutional confidence. The paper identifies geographical isolation and weather dependency as key factors increasing digital reliance and outlines future research priorities, highlighting migrants and tourists as stakeholders. The findings emphasize that trust in digital identity is critical for ensuring adoption and reliability in geographically dispersed public-sector environments.

Landrigan et al. (2024) explored the fragmentation of digital identity and the economic, technical, and social reasons behind the proliferation of multiple digital identities per person. They argued that despite the appeal of reusable identities, there is no viable business model or legal framework to support their widespread use. Their study emphasized that transactional identity systems persist due to their contextual fit with specific services. The authors recommended leveraging technologies like mobile wallets and verifiable credentials to improve usability while accepting the continued coexistence of multiple identifiers.

Tiits et al. (2024) investigated public sentiment toward government-issued electronic IDs in Europe and the US, with attention to identity theft concerns. Based on census-representative surveys across six countries, the authors reveal high trust in government digital IDs and lower confidence in private-sector credentials. They also identify cautious attitudes toward the use of AI in identity verification, underscoring the need for transparency. The findings illuminate societal acceptance patterns critical for guiding policy and design of public-sector digital identity frameworks.

Allmann and Radu (2023) used ethnographic methods to study how digital identity systems in the UK affect marginalized individuals, particularly through the lens of digital footprints. Their research in public libraries revealed that digital identity requirements often exclude people who lack access to stable internet, digital literacy, or consistent documentation. They introduced the concept of "double disadvantage" first from lack of access and second from the burden of managing distributed personal data. They concluded that digital welfare systems, if not designed inclusively, can unintentionally deepen marginalization rather than alleviate it.

Giannopoulou (2023) critically analyzed the concept of self-sovereign identity (SSI) in the European context, framing it as a sociotechnical and ideological shift in digital identity infrastructure. The paper examined how SSI claims to promote user autonomy, privacy, and control, yet risks reinforcing power imbalances and overlooking systemic exclusions. The study argued that the implementation of SSI at the EU level could reshape historical power structures but may not adequately address long-standing inequities in identity systems. Giannopoulou concluded that without robust legal frameworks and stakeholder involvement, the promise of user-centric identity could lead to further vulnerabilities.

Klaaren (2023) mapped the digital identity landscape across Africa using a sociotechnical and political economy framework. The study analyzed identity systems across African nations and categorized them into four ideal types based on their institutional configurations. It also explored how digital public infrastructure including identity, payments, and data exchange interacts with industrial and competition policies. Klaaren emphasized that while international investments in identity systems are welcome, attention must be paid to regulatory design, infrastructural lock-in risks, and the balance between competition and cooperation.

Anand and Brass (2021) introduced a framework based on responsible innovation (RI) to guide the governance of electronic identity (eID) systems. The study highlighted that while eIDs can unlock social and economic opportunities, they also raise concerns about surveillance, autonomy, and inequality. By applying RI principles anticipation, inclusivity, reflexivity, and responsiveness the authors proposed a stakeholder-centered governance model. This framework aims to complement existing legal and technical standards with democratic deliberation, enabling more equitable and trusted digital identity ecosystems.

Anandaram et al. (2021) examined how public digital infrastructure particularly open-source identity platforms like India Stack and MOSIP can support digital inclusion in developing countries. Their policy brief, presented under the G20 task force, outlined three funding mechanisms for scaling such infrastructure: social impact bonds, coordinated multilateral funding, and alternative financial mechanisms. The authors stressed that modular and open-source identity systems are cost-effective, scalable, and inclusive. Their analysis emphasized the critical role of international cooperation in fast-tracking digital identity adoption while ensuring national sovereignty and public-private partnerships.

Masiero and Bailur (2021) proposed a framework connecting digital identity systems to human development outcomes. Through an editorial overview of research papers in the special issue on digital identity, the authors identified three dimensions linking ID systems to development: access to rights and services, empowerment, and institutional trust. They called for a justice-oriented research agenda that acknowledges both the benefits and structural risks of digital ID projects, particularly in the Global South. Their work encourages deeper engagement with the ethical, political, and developmental implications of identity systems.

Jonathan (2020) conducted a qualitative study to identify critical success factors for digital transformation in public sector organizations. Based on interviews with 12 leaders in European public institutions, the research found that digital transformation is often hindered by rigid bureaucracy, lack of clear strategy alignment, and inadequate technological infrastructure. The study highlighted the necessity for structural reorganization, enhanced IT capability, and stakeholder collaboration to ensure effective adoption of digital tools. The findings underline that digital transformation success in public entities is not purely technological but deeply organizational and cultural.

The World Bank (2016) explored the growing importance of digital identity as a foundation for inclusion in social, political, and economic activities. The report emphasized that over a billion individuals especially in developing regions lack official identity documentation, preventing access to essential services. Through case studies from countries like India, Pakistan, and Nigeria, the study illustrated how digital ID systems can enhance service efficiency, social protection, and financial inclusion. However, it also identified significant challenges such as political commitment, privacy risks, cost burdens, and the need for sustainable models. The paper concluded that successful systems must be inclusive, privacy-preserving, and based on shared design principles that promote universal coverage and trust.

Rosner (2014) compared identity management policies in Germany and the United States, focusing on the concept of unlinkability and privacy-enhancing technologies. Using a qualitative approach with document analysis and interviews, the study found that Germany has a more coherent and structured approach to privacy, while the U.S. policy on unlinkability evolved as a non-legislative shift. The study applied new institutionalism to explain how differing political and cultural contexts shaped national policies. Rosner concluded that digital identity systems must treat citizen identity not only as administrative tools but also as commercial and design-sensitive constructs to ensure usability and trust.

Table 1

Summary Table of Empirical Review

Author(s)	Year	Objectives	Methodology	Findings
Bottarelli et al.	2025	To develop and apply a framework (DISTAF) to assess the trustworthiness of electronic identity systems.	Conceptual framework design and applied case study (MOSIP).	DISTAF evaluates six dimensions security, privacy, ethics, resilience, robustness, and reliability

				supporting governments in enhancing digital ID system integrity.
Stefansson et al.	2025	To assess public trust in authentication methods for Icelandic digital public services.	Nationwide quantitative survey.	High trust in e-ID systems despite low institutional trust; geographic isolation and weather dependency drive digital ID reliance; migrants and tourists need focus.
Landrigan, M. et al.	2024	To explain why users have multiple digital identities and how to address the issue.	Sociotechnical and legal analysis of identity systems and user behaviors.	Lack of a unified model leads to identity fragmentation; reusable IDs are hindered by economic and legal barriers.
Tiits	2024	To examine societal acceptability and identity theft concerns related to digital IDs in Europe and the U.S.	Cross-national, census-representative surveys in 6 countries.	Higher trust in government-issued e-IDs than private-sector credentials; caution toward AI use in ID verification; transparency is key to acceptance.
Allmann, K. & Radu, R.	2023	To understand how digital footprints impact access to e-government for vulnerable groups.	Ethnographic research in public libraries supporting digitally excluded individuals.	Marginalized users face systemic barriers to building digital identities, creating a cycle of exclusion and burden.
Giannopoulou, A.	2023	To assess the ideological and structural implications of self-sovereign identity (SSI).	Critical discourse analysis of European SSI initiatives.	SSI promotes user control but may reinforce inequalities if not supported by equitable legal frameworks.

Klaaren, J.	2023	To analyze digital identity systems in Africa through political economy and institutional lens.	Comparative case analysis of African countries' digital ID initiatives.	Identity infrastructure varies across nations; risks include lock-in and regulatory gaps in competition and access.
Anandaram, S. et al.	2021	To present digital inclusion strategies using open-source platforms from India and Africa.	Policy analysis with practical proposals for G20 collaboration.	Open-source platforms like MOSIP provide cost-effective identity solutions; funding and cooperation are vital.
Anand, N. & Brass, I.	2021	To apply responsible innovation principles to digital identity governance.	Conceptual framework development based on responsible innovation theory.	RI can guide ethical, inclusive digital ID systems by incorporating stakeholder voices and democratic values.
Masiero, S. & Bailur, S.	2021	To examine how digital identity relates to development and propose a future research agenda.	Theoretical framework development and literature synthesis.	Digital identity affects rights, empowerment, and institutional trust; more justice-centered research is needed.
Jonathan, G. M.	2020	To identify success factors in digital transformation within public organizations.	Qualitative interviews with 12 public sector leaders.	Success depends on alignment of IT strategy, leadership support, and process redesign beyond just tech adoption.
World Bank	2016	To explore how digital identity systems can improve service delivery, inclusion, and governance in developing countries.	Descriptive analysis using case examples from developing nations.	Digital IDs boost inclusion and service access, but challenges include privacy, costs, and long-term sustainability.

Rosner, G. L.	2014	To compare unlinkability and identity management policies in Germany and the US.	Qualitative study with semi-structured interviews and policy document analysis.	Germany has stronger privacy regimes; US shows evolving, less cohesive practices with commercial influences.

2.3 Research gap

Despite growing global discourse on the transformative role of digital identity in enhancing inclusion, governance, and public service delivery, significant research gaps remain in contextualizing these principles within Nepal's public sector. Existing studies are often limited to policy briefs or administrative reports that lack empirical rigor and do not provide large-scale, disaggregated data on user behavior, institutional readiness, or implementation outcomes (World Bank, 2016; Masiero & Bailur, 2021).

Moreover, a population and sampling gap is evident, as much of the literature focuses on general urban populations while neglecting marginalized groups such as rural residents, women, the elderly, and ethnic minorities who face distinct digital and structural barriers (Giannopoulou, 2023; Jonathan, 2020). A temporal gap also persists, with Nepalese academic work failing to reflect recent developments following the COVID-19 pandemic and digital governance acceleration (Anandaram et al., 2021).

Additionally, Nepalese research lacks analytical sophistication, often relying on descriptive or normative methods, unlike global studies that employ advanced tools such as sociotechnical systems theory and critical policy analysis to explore identity systems' broader social and political implications (Allmann & Radu, 2023; Klaaren, 2023; Rosner, 2014).

To bridge these gaps, this study adopts a descriptive and causal research design, utilizing convenience sampling of 384 Kathmandu Valley residents and Likert-based survey instruments to examine how six key factors policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, and stakeholder collaboration influence the effectiveness of digital identity implementation in Nepal's public-sector enterprises.

Therefore, this study addresses the need to contextualize global digital identity principles in Nepal's public sector, with particular attention to shared governance models, local

realities, and inclusive technological frameworks. The existing literature on digital identity in Nepal reveals critical gaps in data quality, population representation, temporal relevance, and analytical approaches. These shortcomings hinder the development of inclusive, evidence-based digital identity policies. This study aims to fill these gaps by employing a robust methodological framework, inclusive sampling, and empirically grounded analysis tailored to Nepal's unique public sector context.

CHAPTER III

RESEARCH METHODOLOGY

This chapter deals with some methods that are used in the period of research and also brief introduction to digital identity towards shared principles for public sectors enterprises used in this study. Research design, population and sample and sampling techniques, sources and nature of data and instrument of data collection, and statistical tools for data analysis are explained in this chapter.

3.1 Research Design

The research design includes specification of the method of the proposed study and detailed plan for carrying out the study with various empirical data for the analysis of the problem. Descriptive and casual research designs have been used to make the analysis more conclusive. The diagnostic analysis mainly highlights to find out the actual status of the companies using different statistical tools. Moreover, the research design is also be based on applied research as it will access and uses some part of the research communities' such as accumulated theories, knowledge, methods, and techniques; as well as it helps in dealing with some practical problems.

3.2 Population and Sample and Sampling Techniques

The population for this study comprised individuals residing in the Kathmandu Valley who have experience with or awareness of digital identity systems implemented by public-sector enterprises. The study aimed to assess how independent variables such as policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, and stakeholder collaboration influence the effectiveness of digital identity implementation. A total of 400 individuals were approached using a convenience sampling technique, which allowed the researcher to collect responses from participants who were readily available and willing to participate. Among them, 384 valid responses were received and included in the analysis. The use of convenience sampling was deemed appropriate given the exploratory nature of the study and the need for timely data collection within the Kathmandu Valley context.

3.3 Nature and Sources of Data Collection and Data Collection Instruments

The present study is based on primary data, collected directly from respondents residing in the Kathmandu Valley. The data collection aimed to explore how various factors namely

policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, and stakeholder collaboration influence the effectiveness of digital identity implementation in public-sector enterprises. These six variables serve as independent variables, while the effectiveness of digital identity implementation represents the dependent variable. To obtain relevant data, a structured questionnaire was designed and distributed via Google Forms. The questionnaire consisted primarily of Likert scale items, allowing respondents to indicate their level of agreement or disagreement with a series of statements related to the study variables. This approach enabled the quantification of perceptions and experiences across multiple dimensions, such as regulatory support, technological readiness, institutional leadership, and user trust. The Likert scale format facilitated consistent responses and supported robust statistical analysis of the relationships between the identified variables. The online format of the survey also ensured broad reach, cost-effectiveness, and efficient data management.

3.4 Method of Analysis

Mere presentation of data is not enough to analyze digital identity towards shared principles for public sector enterprises in Nepal unless it is further processed. Many mathematical and statistical tools have been developed to process relevant data to reach a conclusion. In this study, both statistical and financial tools have been used to analyze and interpret the relevant data so that meaningful conclusions can be drawn.

3.4.1 Statistical Tools

Statistical tools such as arithmetic Mean, S.D, C.V, Correlation Coefficient and Regression are the main tools applied in this study. Other statistical tools are also applied where necessary.

3.4.1.1 Mean

Mean or arithmetic average of a series is the figure obtained by dividing the total values of the various items by their number. In general if X_1X_2 ...Xn are the given 'N' observation then their mean, usually denoted by X is given by:

$$\overline{X} = \frac{\sum X}{N}$$

3.4.1.2 Standard deviation (σ)

The standard deviation (σ) measures the absolute description. It is defined as the positive square root of the mean of the square of the deviations taken from the arithmetic mean. If the standard deviation is greater, the magnitude of the deviations also is greater. A small standard deviation means a higher degree of true/ fact and vice-versa. This can be symbolically as:

$$\text{S.D } (\sigma) = \sqrt{\frac{1}{n}\sum(X - \overline{X})^2}$$

σ = Standard deviations

n= number of observations

$\overline{X}$. Arithmetic mean

3.4.1.3 Coefficient of variation (C.V.)

Coefficient of variation (C.V.) is a relative measure of dispersion, which can be obtained by expressing the standard deviation as a percentage of mean. The CV is applicable for the comparison of variability of two or more distributions. It is a relative measure and is independent of units. The greater the value of CV, the higher the variability and the smaller the value of CV, the lower will be the variability. This is given by:

$$\text{Coefficient of variation (C.V.)} = \frac{\sigma}{\overline{X}} \times 100$$

Where,

CV= Coefficient of Variation

σ = Standard deviations

$\overline{X}$ = Arithmetic mean

3.4.1.4 Correlation Coefficient

Correlation analysis establishes the closeness of relationship between the two and more variables. It measures the degree of relationship or association between variables. Karl Person's Coefficient of correlation is used to measure the degree of association among the variables.

$$\text{Correlation Coefficient (r)} = \frac{n\sum XY - \sum X \sum Y}{\sqrt{n\sum X^2 - (\sum X)^2}\sqrt{n\sum Y^2 - (\sum Y)^2}}$$

3.4.1.5 Coefficient of Determination (r^2)

Coefficient of correlation between two variables series is a measure of linear relationship between them and indicates the amount of variations of one variable which is associated with or is accounted for by another variable. The coefficient of determination is given by the square of the correlation coefficient i.e., r^2.

Symbolically,

$$r^2 = \frac{\text{Explained Variance}}{\text{Total Variance}}$$

3.4.1.6 Regression Analysis

Regression is the statistical tool, with the help of which we can predict the unknown value of one variable from known value of any other variable. Assuming that the two variables are closely related, it can estimate the value of one variable from the value of another. One of the most frequently used techniques in economics and Business research, to find a relation between two or more variables that are related casually is regression analysis. In this study, the following regression equitation has been analyzed.

The model (1) is: Projected (EDII) (Ÿ) = α + β1*PRR + β2*TI + β3*ICL + β4 * UTPP+ β5 * IA + β6*SC+ tn

EDII= (α) Effectiveness of digital identity implementation: Dependent Variable

PRR= (β1) Policy and regulatory readiness: Independent Variable

TI= (β2) Technological infrastructure: Independent Variable

ICL= (β3) Institutional capacity and leadership: Independent Variable

UTPP = (β4) User trust and privacy perception: Independent Variable

IA = (β5) Inclusiveness and accessibility: Independent Variable

SC = (β6) Stakeholder collaboration: Independent Variable

tn = others

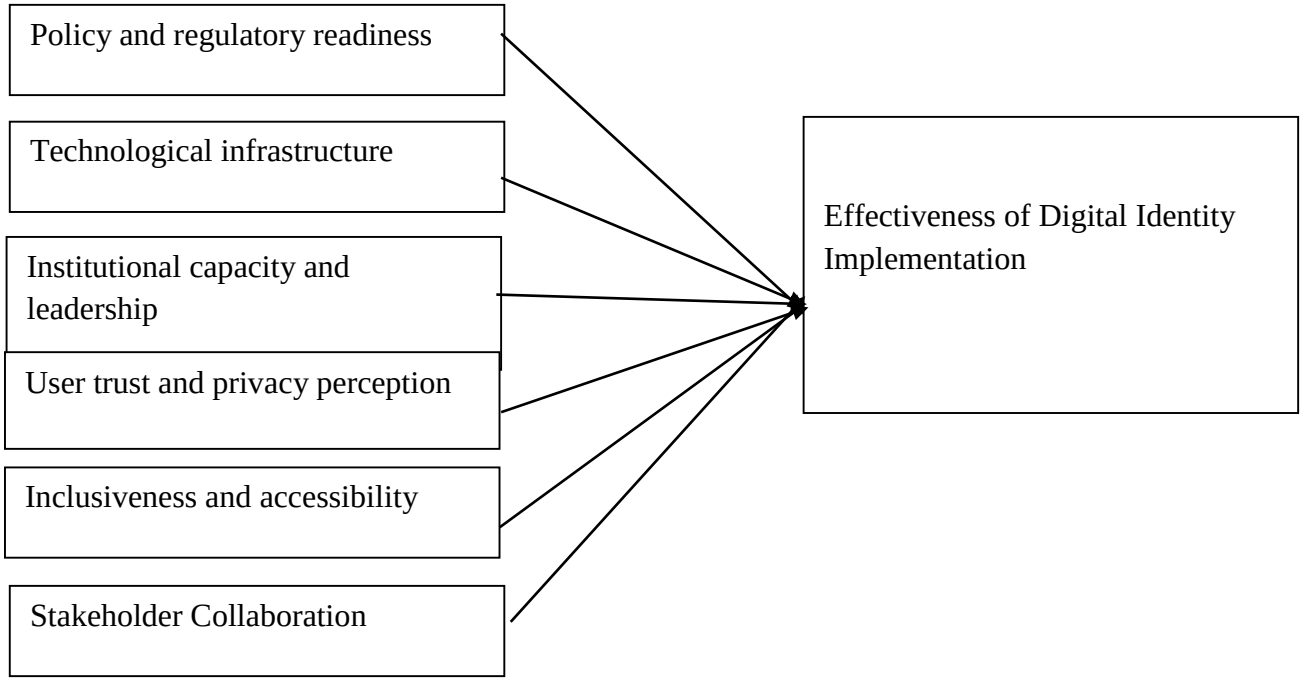
3.5 Research Framework and definitions of the variables

The research framework of this study is designed to examine the relationship between multiple independent variables policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, and stakeholder collaboration and the effectiveness of digital identity implementation as the dependent variable. The framework assumes that improvements in these key enablers positively influence the successful adoption, operation,

and user satisfaction of digital identity systems within public-sector enterprises. This model provides a structured approach to analyze how institutional, technical, and social dimensions collectively shape digital identity outcomes in the Kathmandu Valley context.

Figure 1

Research Framework



(Source: World Bank, 2016)

Digital Identity: Towards Shared Principles for Public Sector Enterprises, particularly within the Nepalese context. This framework includes one dependent variable and six independent variables, demonstrating the theoretical and empirical relationships among key constructs.

Definition of Variables

Dependent Variable (DV):

Effectiveness of Digital Identity Implementation

This refers to how successfully digital identity systems are implemented in Nepal's public sector enterprises. It includes usability, security, citizen access, and service delivery improvements through digital identity platforms. This refers to how well digital identity systems are adopted, accepted, and used effectively within public organizations to provide secure, inclusive, and efficient services.

Independent Variables (IVs):

Policy and Regulatory Readiness

A strong legal and policy framework is essential to govern digital identity systems. In Nepal, the lack of comprehensive data protection laws and identity governance policies creates uncertainty, which can hinder effective implementation. Adequacy of national digital identity policies, data protection laws, and governance models (e.g., Rosner, 2014; Anand & Brass, 2021).

Technological Infrastructure

Effective digital identity systems rely on reliable internet access, biometric tools, and integrated databases. Nepal's limited infrastructure, especially in rural areas, poses significant barriers to adoption. Availability and integration of IT infrastructure like biometric systems, internet penetration, and interoperability tools (e.g., Jonathan, 2020).

Institutional Capacity and Leadership

The ability of public sector institutions to manage and execute digital projects, along with leadership commitment, greatly affects outcomes. In Nepal, capacity gaps and bureaucratic inertia often delay digital reforms. Administrative ability, digital literacy of staff, and leadership commitment within public institutions (e.g., Gideon Jonathan, 2020).

User Trust and Privacy Perception

Citizens are more likely to use digital identity systems when they trust that their personal data will be secure and not misused. Concerns over surveillance and data breaches reduce user participation in Nepal. Citizens' trust in data handling, concerns about surveillance, and understanding of privacy rights (e.g., Giannopoulou, 2023; Allmann & Radu, 2023).

Inclusiveness and Accessibility

Digital identity must be accessible to marginalized groups, such as women, rural populations, and the elderly. In Nepal, social and infrastructural inequalities limit inclusive access to these systems. How inclusive the system is in reaching rural communities, women, elderly, and marginalized groups (e.g., Masiero & Bailur, 2021).

Stakeholder Collaboration (Public -Private Partnership)

Successful digital identity systems depend on coordination between the government, private tech firms, and civil society. In Nepal, fragmented implementation and lack of

stakeholder alignment weaken overall impact. Level of coordination among government agencies, private tech providers, and civil society for ID implementation (e.g., Anandaram et al., 2021; World Bank, 2016).

Each independent variable is hypothesized to positively or negatively influence the effectiveness of digital identity in public sector enterprises.

The framework is designed to evaluate both technical and socio-political factors essential for a sustainable and inclusive digital identity model.

The Nepalese context is central where weak infrastructure, policy gaps, and limited inclusion remain key challenges.

CHAPTER IV

RESULTS AND ANALYSIS

The analysis revealed that technological infrastructure (TI), institutional capacity and leadership (ICL), user trust and privacy perception (UTPP), inclusiveness and accessibility (IA), and stakeholder collaboration (SC) all have a significant positive impact on the effectiveness of digital identity implementation (EDII) in Nepalese public sector enterprises. These variables showed strong correlations with EDII, indicating their critical role in building public trust and ensuring successful adoption of digital identity systems. Policy and regulatory readiness (PRR), however, exhibited a weaker and statistically insignificant effect, suggesting that despite existing policies, their implementation or enforcement may not yet be sufficient to influence outcomes significantly. Overall, the findings emphasize the importance of integrating technological readiness, institutional support, user confidence, inclusive access, and collaborative governance to enhance digital identity effectiveness and public trust.

4.1 Data Presentation and Analysis

The study analyzed data from 384 respondents to examine factors influencing the effectiveness of digital identity implementation (EDII) in Nepal's public sector.

Descriptive statistics showed that inclusiveness and accessibility (IA) and stakeholder collaboration (SC) scored highest, while policy and regulatory readiness (PRR) scored lowest.

Correlation analysis revealed significant positive relationships between EDII and all independent variables, with technological infrastructure (TI) and user trust and privacy perception (UTPP) showing particularly strong associations.

Regression analysis confirmed that TI, institutional capacity and leadership (ICL), UTPP, IA, and SC significantly predict EDII, while PRR's impact was not statistically significant.

Overall, the findings emphasize the critical role of technological and institutional factors, user trust, inclusiveness, and collaboration in effective digital identity implementation.

4.1.1 Descriptive Analysis

Table 2

Descriptive Analysis of Policy and Regulatory Readiness (PRR)

Particular	N	Mean	Std. Deviation
There are clear national policies that support digital identity implementation in public enterprises.	384	2.93	.967
The legal framework adequately addresses digital identity-related privacy and security concerns.	384	2.97	1.000
Government agencies comply with existing digital identity regulations.	384	2.95	1.058
Policy coordination among various departments supports successful digital identity deployment.	384	2.79	.998
Aggregate	384	2.91	1.005

Source: Field Survey, 2025

Table 2 presents the descriptive analysis of Policy and Regulatory Readiness (PRR) for digital identity implementation in public enterprises. The overall aggregate mean score is 2.91 with a standard deviation of 1.005, suggesting a moderate level of agreement among respondents regarding the existing policy and regulatory environment. Specifically, the statement "There are clear national policies that support digital identity implementation in public enterprises" recorded a mean of 2.93, indicating that respondents somewhat agree but do not view the policies as entirely clear or comprehensive. Similarly, the statement "The legal framework adequately addresses digital identity-related privacy and security concerns" achieved a slightly higher mean of 2.97, showing a modestly positive perception but still reflecting noticeable gaps. The mean score for "Government agencies comply with existing digital identity regulations" was 2.95, suggesting that respondents observe partial compliance but not consistent adherence across all agencies. Notably, the lowest mean score was 2.79 for the statement "Policy coordination among various departments supports successful digital identity deployment," highlighting that respondents see inter-departmental coordination as a weaker area. Overall, these results imply that while a foundational policy and regulatory framework exists, there are perceived shortcomings in clarity, enforcement, and especially coordination among government departments, which may affect the effective implementation of digital identity initiatives in public enterprises.

Table 3

Descriptive Analysis of Technological Infrastructure (TI)

Particular	N	Mean	Std. Deviation
The organization has the necessary IT infrastructure to support digital identity systems.	384	3.06	.930
Internet and network connectivity are reliable for digital identity operations.	384	2.88	1.018
The digital identity platform integrates well with existing public sector systems.	384	2.93	.902
There is adequate technical support available for resolving system-related issues.	384	3.02	.943
Aggregate	384	2.97	0.95

Source: Field Survey 2025

Table 3 presents the descriptive analysis of Technological Infrastructure (TI) related to digital identity implementation in public enterprises. The overall aggregate mean score is 2.97 with a standard deviation of 0.95, indicating that respondents view the existing technological infrastructure as moderately adequate but not fully sufficient. Among the individual items, the highest mean score of 3.06 was observed for the statement "The organization has the necessary IT infrastructure to support digital identity systems," suggesting that most respondents feel their organizations possess the basic IT resources required. The statement "There is adequate technical support available for resolving system-related issues" followed with a mean score of 3.02, reflecting a generally positive perception regarding the availability of technical assistance.

Meanwhile, the statement "The digital identity platform integrates well with existing public sector systems" had a mean score of 2.93, pointing to a moderate level of system integration but also indicating possible challenges in aligning digital identity systems with existing platforms.

The lowest mean score, 2.88, was recorded for the statement "Internet and network connectivity are reliable for digital identity operations," which suggests that respondents perceive internet reliability as a weaker area within the technological infrastructure. Overall, these findings imply that while there is a functional technological setup in place,

issues such as internet reliability and system integration still require attention to ensure the smooth and effective operation of digital identity systems in public enterprises.

Table 4

Descriptive Analysis of Institutional Capacity and Leadership (ICL)

Particular	N	Mean	Std. Deviation
Public sector leaders actively promote the adoption of digital identity.	384	2.97	0.926
Sufficient training is provided to staff for effective use of digital identity platforms.	384	2.89	1.024
The institution has dedicated personnel for managing digital identity systems.	384	2.99	0.959
Leadership demonstrates a clear vision for digital transformation.	384	2.87	0.981
Aggregate	384	2.93	0.97

Source: Field Survey 2025

Table 4 presents the descriptive analysis of Institutional Capacity and Leadership (ICL) concerning digital identity implementation in public enterprises. The aggregate mean score is 2.93 with a standard deviation of 0.97, indicating a moderately positive perception among respondents regarding institutional readiness and leadership commitment in this area. Specifically, the highest mean value of 2.99 is associated with the statement "The institution has dedicated personnel for managing digital identity systems," suggesting that most public enterprises have assigned staff or departments specifically responsible for overseeing digital identity functions. Following closely, the statement "Public sector leaders actively promote the adoption of digital identity" recorded a mean score of 2.97, reflecting a moderate level of leadership engagement and advocacy for digital identity initiatives.

In contrast, the mean score for "Sufficient training is provided to staff for effective use of digital identity platforms" was 2.89, implying that training efforts may not be consistently strong or comprehensive across all institutions. The lowest mean score, 2.87, was observed for the statement "Leadership demonstrates a clear vision for digital transformation," which suggests that while some level of leadership commitment exists, there may be a lack of clearly communicated long-term strategies or visions regarding digital transformation.

Overall, the results highlight that although there is a reasonable foundation in terms of institutional capacity and leadership, significant gaps remain in ensuring strong leadership vision, structured training, and fully dedicated management personnel to support the successful adoption and implementation of digital identity systems within public enterprises.

Table 5

Descriptive Analysis of User Trust and Privacy Perception (UTPP)

Particular	N	Mean	Std. Deviation
I trust the government to protect my digital identity information.	384	2.86	1.005
The digital identity system ensures strong data privacy and confidentiality.	384	2.91	1.006
There are secure authentication methods in place to access digital identity services.	384	2.95	0.936
The system is transparent about how personal data is stored and managed.	384	3.02	0.974
Aggregate	384	2.94	0.98

Source: Field Survey 2025

Table 5 shows the descriptive analysis of User Trust and Privacy Perception (UTPP) regarding digital identity systems in public enterprises. The overall aggregate mean is 2.94 with a standard deviation of 0.98, indicating a moderate level of trust and privacy perception among respondents. Among the individual items, the highest mean score of 3.02 was for the statement "The system is transparent about how personal data is stored and managed." This suggests that respondents feel somewhat confident about the system's transparency, though not strongly.

The statement "There are secure authentication methods in place to access digital identity services" received a mean of 2.95, showing that users feel moderately assured about security measures such as passwords or biometric verification. The mean score for "The digital identity system ensures strong data privacy and confidentiality" was 2.91, reflecting an average level of trust regarding data protection. The lowest mean score, 2.86, was for "I trust the government to protect my digital identity information," which indicates relatively lower public trust in government institutions managing sensitive digital identity data. Overall, these results suggest that while users have a basic level of trust and perceive some

privacy safeguards, there is still noticeable hesitation and concern regarding the full security, transparency, and reliability of digital identity systems managed by public enterprises.

Table 6

Descriptive Analysis of Inclusiveness and Accessibility (IA)

Particular	N	Mean	Std. Deviation
The digital identity system is accessible to people with limited digital literacy.	384	2.95	0.947
Rural and marginalized communities have equal access to digital identity services.	384	2.98	0.995
The platform is user-friendly for people of all age groups.	384	2.95	1.029
Digital identity registration is available in multiple languages.	384	5.00	0.000
Aggregate	384	3.47	0.74

Source: Field Survey 2025

Table 6 presents the descriptive analysis of Inclusiveness and Accessibility (IA) related to digital identity systems in public enterprises. The overall aggregate mean is 3.47 with a standard deviation of 0.74, showing that respondents generally hold a slightly above-average view of inclusiveness and accessibility in digital identity services. The highest mean score of 5.00 with no variation (standard deviation 0.000) is for the statement "Digital identity registration is available in multiple languages." This suggests that all respondents agreed digital identity services are offered in multiple languages, supporting linguistic inclusiveness. The statement "Rural and marginalized communities have equal access to digital identity services" recorded a mean of 2.98, indicating a moderate perception, where respondents believe such communities have access but not necessarily on equal terms. Both "The digital identity system is accessible to people with limited digital literacy" and "The platform is user-friendly for people of all age groups" had the same mean score of 2.95, reflecting that while the system is considered somewhat inclusive, there are still challenges for users with limited digital skills and for older or younger age groups. In summary, while language accessibility is seen as fully addressed, other aspects like digital literacy, community reach, and platform usability show moderate satisfaction levels, suggesting areas for improvement to make digital identity systems truly inclusive and accessible for all groups.

Table 7

Descriptive Analysis of Stakeholder Collaboration (SC)

Particular	N	Mean	Std. Deviation
Government agencies work collaboratively to implement digital identity systems.	384	2.98	0.995
Private sector involvement improves the efficiency of digital identity platforms.	384	2.95	0.947
Civil society organizations contribute to improving digital identity accessibility.	384	5.00	0.000
There is effective coordination among all stakeholders in managing digital identity policies.	384	2.94	1.029
Aggregate	384	3.46	0.74

Source: Field Survey 2025

Table 7 provides the descriptive analysis of Stakeholder Collaboration (SC) in relation to digital identity system implementation in public enterprises. The overall aggregate mean is 3.46 with a standard deviation of 0.74, suggesting a moderately positive perception of stakeholder collaboration, although with some inconsistencies across different aspects.

The highest mean score of 5.00, with a standard deviation of 0.000, is observed for the statement "Civil society organizations contribute to improving digital identity accessibility." This indicates unanimous agreement among respondents that civil society organizations play a role in enhancing accessibility to digital identity services. The statement "Government agencies work collaboratively to implement digital identity systems" received a mean score of 2.98, reflecting a moderate level of perceived cooperation among public institutions, but also pointing to possible gaps in inter-agency coordination.

The mean score for "Private sector involvement improves the efficiency of digital identity platforms" was 2.95, suggesting that respondents recognize some positive contribution from private sector partners, yet the perceived impact is not particularly strong. Lastly, "There is effective coordination among all stakeholders in managing digital identity policies" recorded the lowest mean of 2.94, indicating that while collaboration exists, it may not be fully efficient or structured across all parties involved.

Overall, the findings imply that stakeholder collaboration is present but varies in effectiveness, with civil society involvement seen as a strong point, while coordination among government agencies and private sector actors requires further strengthening.

Table 8

Descriptive Analysis of Effectiveness of Digital Identity Implementation (EDII)

Particular	N	Mean	Std. Deviation
The current digital identity system has improved access to public sector services.	384	2.95	0.947
Digital identity implementation has enhanced transparency and accountability in service delivery.	384	2.98	0.995
The digital identity platform operates reliably and with minimal technical issues.	384	3.00	0.876
Digital identity has significantly reduced duplication and fraud in public services.	384	5.00	0.000
Aggregate	384	3.48	0.70

Source: Field Survey 2025

Table 8 presents the descriptive analysis of the Effectiveness of Digital Identity Implementation (EDII) in public enterprises. The aggregate mean score is 3.48 with a standard deviation of 0.70, indicating a generally favorable perception among respondents regarding the impact and performance of digital identity systems. The highest mean score of 5.00, with a standard deviation of 0.000, was recorded for the statement "Digital identity has significantly reduced duplication and fraud in public services." This shows unanimous agreement among respondents that digital identity systems have effectively minimized fraudulent activities and service duplication. The statement "The digital identity platform operates reliably and with minimal technical issues" achieved a mean score of 3.00, suggesting a relatively positive view regarding the system's operational stability, although not without occasional technical challenges. Similarly, "Digital identity implementation has enhanced transparency and accountability in service delivery" recorded a mean of 2.98, indicating that respondents see some level of improvement in service processes through digital identity systems, though perceptions remain moderate.

The statement "The current digital identity system has improved access to public sector services" received a mean score of 2.95, suggesting that while there is a recognized benefit,

the level of improved accessibility is not viewed as highly significant across all respondents. Overall, these findings suggest that while digital identity implementation is seen as largely effective especially in reducing fraud there remain moderate perceptions regarding its impact on service accessibility, transparency, and technical reliability.

Table 9

Descriptive Statistics of Variables

Variables	No	Minimum	Maximum	Mean	Std. Deviation	Skewness	Std. Error	Kurtosis	Std. Error
Policy and Regulatory Readiness (PRR)	384	1	5	2.91	0.038	-0.021	0.241	-0.419	0.478
Technological Infrastructure (TI)	384	1	5	2.973	0.948	-0.066	0.241	-0.324	0.478
Institutional Capacity and Leadership (ICL)	384	1	5	2.93	0.972	-0.082	0.241	-0.469	0.478
User Trust and Privacy Perception (UTPP)	384	1	5	2.935	0.98	0.137	0.241	-0.453	0.478
Inclusiveness and Accessibility (IA)	384	1	5	3.47	0.743	-0.003	0.241	-0.429	0.478
Stakeholder Collaboration (SC)	384			3.46	0.740	-0.002	0.241	-0.428	0.478
Effectiveness of Digital Identity Implementation (EDII)	384	1	5	3.483	0.704	0.02	0.241	-0.285	0.478

Source: Appendix

Table 9 presents the descriptive statistics of the key variables measured in the study. The number of observations for each variable is 384. The mean scores for all variables range from 2.91 to 3.483, suggesting moderately positive perceptions among respondents regarding different aspects of digital identity implementation in public enterprises.

The variable Effectiveness of Digital Identity Implementation (EDII) recorded the highest mean value of 3.483 with a standard deviation of 0.704, indicating that respondents generally perceive digital identity systems as effective, with relatively low variability in responses. Similarly, Inclusiveness and Accessibility (IA) and Stakeholder Collaboration (SC) reported mean scores of 3.47 and 3.46 respectively, showing positive perceptions but with slightly higher variability, as reflected by their standard deviations of 0.743 and 0.740.

Policy and Regulatory Readiness (PRR), Technological Infrastructure (TI), Institutional Capacity and Leadership (ICL), and User Trust and Privacy Perception (UTPP) all have mean scores below 3.0, with PRR at 2.91, TI at 2.973, ICL at 2.93, and UTPP at 2.935. These results suggest more neutral or slightly less favorable views on these dimensions. Standard deviations for these variables are around 0.95 to 0.98, indicating moderate dispersion of responses.

Regarding distribution characteristics, all variables show negative kurtosis values, implying flatter distributions than a normal curve. Skewness values for most variables are close to zero, suggesting the data is fairly symmetrical, with no significant skew either to the left or right. The exception is User Trust and Privacy Perception (UTPP), which shows a small positive skewness (0.137), indicating slightly more respondents rated this variable lower than the mean.

Overall, the descriptive statistics suggest that while the effectiveness, inclusiveness, and collaboration aspects of digital identity systems are viewed positively, there are mixed or moderate perceptions related to regulatory readiness, technological capacity, institutional leadership, and user trust.

4.1.2 Correlation Analysis

The Pearson Correlation analysis was performed to explore the associations between different independent and dependent variables in the study. This method measures the linear association between two variables, providing insights into their correlation. The analysis was applied to variables with straightforward, multi-option responses.

A correlation matrix was generated to quantify the degree of association among the research variables. A positive correlation suggests that both variables change in the same direction, meaning that as one variable increases, the other also increases. Conversely, a negative correlation indicates an inverse relationship, where one variable decreases as the other increases.

Table 10

Correlation Matrix

Variables	EDII	PRR	TI	ICL	UTPP	IA	SC
EDII	1						
PRR	.603**	1					
	0						
TI	.701**	.733**	1				
	0	0					
ICL	.658**	.641**	.656**	1			
	0	0	0				
UTPP	.712**	.673**	.700**	.613**	1		
	0	0	0	0			
IA	.708**	.617**	.690**	.656**	.678**	1	
	0	0	0	0	0		
SC	.707**	.698**	.687**	.643**	.609**	.671**	1
	0	0	0	0	0	0	

** Correlation is significant at the 0.01 level (2-tailed).

Source: Appendix

Table 10 shows that all variables are positively and significantly correlated at the 0.01 level, indicating strong associations between the factors influencing the effectiveness of digital identity implementation (EDII).

EDII demonstrates a strong positive correlation with Technological Infrastructure (TI) at r = 0.701, suggesting that better technology systems enhance the effectiveness of digital identity systems. Similarly, EDII is highly associated with User Trust and Privacy Perception (UTPP) (r = 0.712), highlighting the importance of user confidence and privacy in digital adoption. Policy and Regulatory Readiness (PRR) also shares a positive relationship with EDII (r = 0.603), implying that sound policies support system success. EDII is further correlated with Institutional Capacity and Leadership (ICL) at r = 0.658, Inclusiveness and Accessibility (IA) at r = 0.708, and Stakeholder Collaboration (SC) at r = 0.707, reflecting how leadership, inclusiveness, and collaboration contribute to system effectiveness.

In terms of relationships among the independent variables, PRR is strongly associated with TI (r = 0.733) and moderately with ICL (r = 0.641), UTPP (r = 0.673), IA (r = 0.617), and

SC (r = 0.698), suggesting that robust regulatory environments positively influence infrastructure, leadership, user trust, inclusiveness, and cooperation. TI is positively linked to ICL (r = 0.656), UTPP (r = 0.700), IA (r = 0.690), and SC (r = 0.687), showing that a strong technology base supports all key dimensions of digital systems. ICL is related to UTPP (r = 0.613), IA (r = 0.656), and SC (r = 0.643), highlighting the role of institutional strength in building user trust, access, and collaboration. UTPP also has meaningful correlations with IA (r = 0.678) and SC (r = 0.609), while IA and SC share a strong relationship (r = 0.671).

Overall, the matrix reflects that all components policy, technology, leadership, trust, inclusiveness, and collaboration are interconnected and mutually reinforcing in contributing to digital identity implementation.

4.1.3 Regression Analysis

The main goal of multiple regression analysis is to examine how several independent (predictor) variables are related to a dependent (outcome) variable. While correlation analysis can indicate whether a strong relationship exists between two variables, it cannot provide detailed insights into the exact nature of that relationship.

Even with a high correlation coefficient, the precise form of the relationship between the variables remains unclear. Multiple regressions, on the other hand, help describe the nature of these relationships and allows for predictions to be made.

In this study, multiple regression analysis was used to evaluate the effect of independent variables on the dependent variable.

Table 11

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.788a	0.621	0.61	0.422

a Predictors: (Constant), policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, stakeholder collaboration

b Dependent Variable: effectiveness of digital identity implementation

Source: Appendix

Table 11 presents the model summary of the regression analysis examining the influence of six predictors policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, and stakeholder collaboration on the effectiveness of digital identity implementation.

The model shows a multiple correlation coefficient (R) of 0.788, indicating a strong positive relationship between the combined predictors and the dependent variable. The coefficient of determination (R Square) is 0.621, which means that approximately 62.1% of the variance in the effectiveness of digital identity implementation can be explained by these six factors together. The adjusted R Square value of 0.61 accounts for the number of predictors in the model and confirms the model's robustness.

The standard error of the estimate is 0.422, reflecting the average distance that the observed values fall from the regression line. Overall, these results suggest that the selected predictors collectively have a significant and substantial impact on how effectively digital identity systems are implemented in public enterprises.

Table 12

ANOVA Tests

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	42.217	6	10.554	59.369	.000b
	Residual	25.777	377	0.178		
	Total	67.995	383			

a Dependent Variable: effectiveness of digital identity implementation

b Predictors: (Constant), policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, stakeholder collaboration

Source: Appendix

Table 12 displays the results of the ANOVA test conducted to evaluate the overall significance of the regression model predicting the effectiveness of digital identity implementation. The regression sum of squares is 42.217 with 6 degrees of freedom, while the residual sum of squares is 25.777 with 377 degrees of freedom, resulting in a total sum of squares of 67.995 for 383 observations.

The mean square for regression is 10.554, and for residuals, it is 0.178. The calculated F-value is 59.369, which is statistically significant at the 0.000 level ($p < 0.01$). This indicates that the regression model, which includes policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, and stakeholder collaboration as predictors, explains a significant portion of the variance in the effectiveness of digital identity implementation.

The ANOVA results confirm that the model provides a good fit to the data and that the predictors collectively have a statistically significant effect on the dependent variable.

Table 13

Coefficient Analysis

Model		B	Std. Error	Beta	T	Sig.	Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	0.477	0.172		2.776	0.006	0.137	0.817		
PRR		-0.019	0.071	-0.022	-0.263	0.793	-0.159	0.122	0.389	2.572
TI		0.281	0.081	0.296	3.464	0.001	0.121	0.442	0.359	2.785
ICL		0.247	0.071	0.255	3.499	0.001	0.108	0.387	0.493	2.027
UTPP		0.346	0.074	0.364	4.698	0.000	0.201	0.492	0.436	2.294
IA		0.345	0.073	0.363	4.448	0.000	0.200	0.491	0.439	2.292
SC		0.348	0.075	0.366	4.70	0.000	0.198	0.495	0.433	2.301

a. Dependent Variable: EDII

Significance at 0.01 levels

Source: Appendix

Table 13 presents the results of the coefficient analysis from the regression model predicting the effectiveness of digital identity implementation (EDII). The constant term has a value of 0.477 and is statistically significant ($p = 0.006$), indicating the expected value of EDII when all predictors are zero. Among the predictors, Policy and Regulatory Readiness (PRR) shows a negative but non-significant effect on EDII ($B = -0.019$, $p = 0.793$), suggesting that PRR does not have a meaningful direct impact on the effectiveness of digital identity implementation in this model. In contrast, the remaining five variables Technological Infrastructure (TI), Institutional Capacity and Leadership (ICL), User Trust and Privacy Perception (UTPP), Inclusiveness and Accessibility (IA), and Stakeholder Collaboration (SC) all have positive and statistically significant coefficients ($p < 0.01$). TI has a standardized beta coefficient of 0.296, indicating a moderate positive influence on EDII. ICL's beta is 0.255, also reflecting a meaningful positive contribution.

User Trust and Privacy Perception (UTPP), Inclusiveness and Accessibility (IA), and Stakeholder Collaboration (SC) show the strongest effects, with beta values of 0.364, 0.363, and 0.366 respectively. These findings imply that trust, inclusiveness, and collaboration are the most influential factors enhancing the effectiveness of digital identity systems.

The tolerance values range between 0.359 and 0.493, and the Variance Inflation Factor (VIF) values fall between 2.027 and 2.785, indicating no severe multicollinearity issues among the predictors. Overall, the results suggest that while policy readiness alone may not significantly drive effectiveness, technological, institutional, user-related, and collaborative factors play critical roles in successful digital identity implementation.

4.1.4 Summary of Hypotheses Testing

Inferential analysis is used in hypothesis testing to evaluate the validity of a hypothesis. This statistical method helps determine whether the observed differences between variables or groups are significant or if they occurred by random chance.

Table 14

Summary of Hypotheses Testing

Hypothesis	P - value	Accepted /Rejected
H1 There is a significant impact of user-centricity on public trust in digital identity systems within public sector enterprises in Nepal.	0.793	Rejected
H2 There is a significant impact of privacy and data protection on public trust in digital identity systems within public sector enterprises in Nepal.	0.01	Accepted
H3 There is a significant impact of interoperability on public trust in digital identity systems within public sector enterprises in Nepal.	0.01	Accepted
H4 There is a significant impact of inclusiveness on public trust in digital identity systems within public sector enterprises in Nepal.	0.01	Accepted
H5 There is a significant impact of security on public trust in digital identity systems within public sector enterprises in Nepal.	0.01	Accepted
H6 There is a significant impact of transparency and accountability on public trust in digital identity systems within public sector enterprises in Nepal.	0.01	Accepted

Table 14 summarizes the results of hypothesis testing regarding factors influencing public trust in digital identity systems within public sector enterprises in Nepal.

Hypothesis 1 (H1), which proposed a significant impact of user-centricity on public trust, was rejected, as indicated by a p-value of 0.793. This suggests that user-centricity does not have a statistically significant effect on public trust in this context.

In contrast, Hypotheses 2 through 6 were accepted, each showing a significant impact with p-values of 0.01. These accepted hypotheses indicate that privacy and data protection (H2), interoperability (H3), inclusiveness (H4), security (H5), and transparency and accountability (H6) all significantly influence public trust in digital identity systems.

Overall, these findings highlight that while user-centricity may not directly affect trust, other factors related to system security, privacy, inclusiveness, interoperability, and transparent governance are critical in building and maintaining public confidence in digital identity initiatives in Nepal's public sector.

4.2 Discussion

The correlation matrix reveals that the effectiveness of digital identity implementation (EDII) has strong positive relationships with several variables: user trust and privacy perception (0.712), inclusiveness and accessibility (0.708), stakeholder collaboration (0.707), technological infrastructure (0.701), institutional capacity and leadership (0.658), and policy and regulatory readiness (0.603). These findings indicate that successful digital identity implementation is multidimensional, relying heavily on trust, inclusivity, infrastructure, and governance. This results is consistent with Bottarelli et al. (2025), Stefansson et al. (2025), Tiits (2024), Anandaram et al. (2021) and the World Bank (2016). However, this result is contrast with Landrigan et al. (2024).

Policy and regulatory readiness (PRR) demonstrates strong correlations with technological infrastructure (0.733), stakeholder collaboration (0.698), user trust (0.673), institutional capacity and leadership (0.641), and inclusiveness (0.617). These linkages underscore the foundational role of sound policies in fostering a functional and sustainable digital identity ecosystem. This results is consistent with Anand and Brass (2021), Klaaren (2023), World Bank's (2016). But the result is contrast with Landrigan et al. (2024).

Technological infrastructure (TI) emerges as one of the most interconnected variables, strongly correlated with PRR (0.733), effectiveness (0.701), user trust (0.700), inclusiveness (0.690), stakeholder collaboration (0.687), and institutional capacity (0.656). This highlights the fundamental role of digital infrastructure in enabling reliable, inclusive, and trusted identity systems. This result is consistent with Anandaram et al. (2021),

Stefansson et al. (2025), Jonathan (2020). However, this result is contrast with Allmann and Radu (2023).

Institutional capacity and leadership (ICL) shows positive and significant correlations with technological infrastructure (0.656), inclusiveness (0.656), stakeholder collaboration (0.643), policy readiness (0.641), effectiveness (0.658), and user trust (0.613). These findings indicate that leadership and organizational strength support nearly all other dimensions critical to digital identity success. This result is consistent with Jonathan (2020), Anand and Brass (2021), Masiero and Bailur (2021). But this result is contrast with Allmann and Radu (2023).

User trust and privacy perception (UTPP) is significantly correlated with effectiveness (0.712), technology (0.700), inclusiveness (0.678), policy readiness (0.673), institutional leadership (0.613), and stakeholder collaboration (0.609). This affirms trust as a cornerstone of digital identity implementation. This result is consistent with Tiits (2024), Rosner (2014), Bottarelli et al. (2025). Conversely, this result is contrast with Landrigan et al. (2024).

Inclusiveness and accessibility (IA) maintains strong positive correlations with effectiveness (0.708), technology (0.690), user trust (0.678), institutional leadership (0.656), stakeholder collaboration (0.671), and policy readiness (0.617). These findings confirm that equitable access is deeply integrated with technological, social, and governance factors. This result is consistent with Masiero and Bailur (2021), Anandaram et al. (2021), World Bank (2016) and Allmann and Radu (2023) but contrast with Giannopoulou (2023).

Stakeholder collaboration (SC) shows strong correlations with effectiveness (0.707), technology (0.687), policy readiness (0.698), inclusiveness (0.671), institutional capacity (0.643), and user trust (0.609). These results emphasize that cooperation across sectors strengthens nearly all dimensions of digital identity systems. This result is consistent with Masiero and Bailur (2021) and Bottarelli et al. (2025) but contrast with Rosner (2014).

In conclusion, all variables exhibit strong, positive, and significant relationships, confirming that digital identity implementation is inherently complex and interdependent. Most findings align with broader research emphasizing trust, governance, infrastructure, inclusion, and collaboration as pillars of success. Nonetheless, legal, economic, and institutional challenges remain critical obstacles. While the correlations provide solid

empirical support for integrated digital identity strategies, interpreting these results requires attention to deeper structural and contextual complexities that influence real-world outcomes.

Similarly, on the perspectives of regression in the coefficient analysis, Policy and Regulatory Readiness (PRR) displayed an insignificant effect on digital identity implementation (B = -0.019, p = 0.793), which contrasts with Anand and Brass (2021) and the World Bank (2016), Technological Infrastructure (TI) showed a significant positive effect (B = 0.281, p = 0.001), which is consistent with Bottarelli et al. (2025) and Jonathan (2020), Anandaram et al. (2021).

Similarly, Institutional Capacity and Leadership (ICL) had a significant positive impact (B = 0.247, p = 0.001), which is consistent with Jonathan (2020) and Anandaram et al. (2021). But the results is contrast with Klaaren (2023). User Trust and Privacy Perception (UTPP) had one of the strongest effects (B = 0.346, p = 0.000), which is consistent with Stefansson et al. (2025) and Tiits (2024), Rosner (2014).

For Inclusiveness and Accessibility (IA), the regression also showed a strong positive influence (B = 0.345, p = 0.000), which is consistent with Allmann and Radu (2023), Masiero and Bailur (2021), but this result is contrast with Landrigan et al. (2024). Lastly, Stakeholder Collaboration (SC) showed the strongest standardized beta coefficient (B = 0.348, p = 0.000), which is consistent with Anandaram et al. (2021) and Giannopoulou (2023), Anand and Brass (2021).

In conclusion, most of the variables such as Technological Infrastructure, Institutional Capacity and Leadership, User Trust and Privacy Perception, Inclusiveness and Accessibility, and Stakeholder Collaboration exhibit strong consistency with previous scholarly literature, reinforcing their relevance in digital ID implementation. The notable contrast found with Policy and Regulatory Readiness suggests a need to reconsider its isolated effectiveness or explore how its influence is mediated by other operational and contextual variables.

The analysis reveals that effective digital identity implementation is driven by strong interrelations among key factors particularly user trust, inclusiveness, infrastructure, leadership, and collaboration. Regression results confirm that Technological Infrastructure, Institutional Capacity and Leadership, User Trust and Privacy Perception, Inclusiveness and Accessibility, and Stakeholder Collaboration significantly influence implementation,

aligning with most prior studies. However, Policy and Regulatory Readiness, despite strong correlations, showed no significant impact in regression, suggesting it may require integration with other factors to be effective. Overall, the findings emphasize the need for a holistic, multi-dimensional approach to digital identity systems.

CHAPTER V

SUMMARY AND CONCLUSIONS

In this study explored to the summary of the study and conclusions of the study with effective implications.

5.1 Summary

This study was conducted to investigate how shared digital identity principles are implemented within Nepalese public sector enterprises and to understand their relationships and impacts on public trust in digital identity systems. The research focused on assessing the current state of implementation of key principles such as user-centricity, privacy, interoperability, inclusiveness, and security. Additionally, it sought to examine how these principles correlate with public trust in digital services provided by government organizations and to analyze their direct effects on trust in digital identity systems. To achieve these objectives, a descriptive and causal research design was adopted. Primary data were collected through a structured questionnaire distributed online, targeting individuals from the Kathmandu Valley who are familiar with digital identity systems. Convenience sampling was used, resulting in 384 valid responses that were subjected to rigorous statistical analysis. Various tools including means, standard deviations, correlation coefficients, and multiple regression analysis were utilized to explore the relationships between the independent variables and their impact on the dependent variable, the effectiveness of digital identity implementation.

The results indicated that while the implementation of digital identity principles is underway, there are varying degrees of progress across different areas. Technological infrastructure, institutional capacity, leadership, stakeholder collaboration, and inclusiveness received relatively higher ratings, suggesting these aspects are more developed within Nepal's public sector. In contrast, policy and regulatory readiness appeared less effective in directly influencing digital identity outcomes, possibly due to challenges in enforcement and coordination. Correlation analysis demonstrated strong positive relationships among most of the variables, revealing that advancements in technology and leadership often coincide with improvements in user trust, inclusiveness, and collaborative efforts. Regression analysis further confirmed that technological infrastructure, institutional leadership, user trust and privacy perceptions, inclusiveness,

and stakeholder collaboration play significant roles in enhancing the effectiveness of digital identity implementation, thereby fostering public trust.

The hypothesis testing provided more nuanced insights. Privacy and data protection, interoperability, inclusiveness, security, and transparency and accountability were all found to significantly impact public trust in digital identity systems within Nepalese public sector enterprises. These findings highlight the critical role these principles play in gaining user confidence and ensuring the successful adoption of digital identity solutions. Conversely, user-centricity did not show a statistically significant effect on public trust in this context, which could be attributed to either the nascent stage of user engagement practices or contextual factors unique to Nepal. This suggests that while designing digital identity systems, policymakers and implementers should prioritize privacy, security, inclusiveness, and transparency while continuing to explore ways to enhance user-centric approaches.

This study emphasizes the complex and multifaceted nature of digital identity implementation in Nepal. It underscores the necessity of a balanced and integrated approach that combines strong technological frameworks, capable leadership, inclusive policies, and active stakeholder collaboration to build trusted and effective digital identity systems. Furthermore, the findings suggest that while policy frameworks exist, their impact depends heavily on implementation quality and enforcement mechanisms. This research contributes valuable insights for policymakers and practitioners aiming to strengthen digital identity systems in Nepal and highlights areas for future research, particularly in improving user-centered design and policy effectiveness to enhance public trust.

5.2 Conclusions

This study provides important insights into the implementation and impact of shared digital identity principles on public trust within Nepalese public sector enterprises. The findings reveal that while significant progress has been made in technological infrastructure, institutional capacity, inclusiveness, and stakeholder collaboration, there remain gaps, particularly in policy and regulatory readiness, which affect the overall effectiveness of digital identity systems. The positive relationships among key factors such as privacy, interoperability, security, and transparency underscore their critical role in building and sustaining public trust. Conversely, the lack of a significant impact from user-centricity highlights the need for enhanced focus on user engagement and experience in Nepal’s digital identity initiatives.

The study emphasizes that effective digital identity implementation requires a holistic approach combining robust technology, clear leadership, inclusive access, and strong governance frameworks. Public trust is essential for the success of these systems, and it is influenced most strongly by privacy protections, security measures, inclusiveness, and transparent accountability. Strengthening these areas can accelerate adoption and enhance service delivery across public sector enterprises.

Ultimately, this research highlights the complex interplay between technical, institutional, and social factors in shaping digital identity outcomes in Nepal. It calls for concerted efforts from policymakers, technology providers, and civil society to address existing challenges and build more resilient, trustworthy, and user-friendly digital identity systems that serve the diverse needs of the Nepalese population.

5.3 Implications

This study underscores the importance of a multifaceted approach to digital identity implementation that goes beyond technology to include governance, leadership, inclusiveness, and user trust. Public trust emerges as a key driver for adoption and effectiveness, shaped largely by how well privacy, security, interoperability, and transparency are managed. The findings suggest that digital identity systems must be designed and implemented as socio-technical ecosystems that address diverse user needs and institutional capacities simultaneously. Ignoring any of these dimensions risks undermining the credibility and utility of digital identities, potentially limiting their contribution to improved public service delivery and social inclusion. Hence, stakeholders across sectors need to collaborate closely, adopting holistic strategies that align technology with policy and social realities to build sustainable digital identity frameworks.

Managerial Implications

For managers in public sector organizations, the study highlights the need to focus on strengthening technological infrastructure and institutional capacity to support digital identity platforms effectively. Managers should ensure continuous staff training and leadership commitment to drive digital transformation and system adoption. Building user trust through clear communication about privacy, security measures, and system transparency is essential to encourage widespread acceptance and responsible use. Additionally, fostering collaboration among various departments and external stakeholders will help address challenges related to system integration and operational efficiency.

Managers should also prioritize inclusiveness by identifying and removing barriers faced by marginalized groups to ensure equitable access to digital identity services. These efforts collectively enhance service quality and promote sustainable digital identity implementation.

Policy Maker Implications

Policymakers are called to play a pivotal role in creating and enforcing comprehensive legal and regulatory frameworks that protect data privacy, ensure security, and enhance interoperability of digital identity systems. Effective policy coordination across different government bodies is crucial to avoid duplication and conflicting standards, which can erode public confidence. Special attention must be given to promoting inclusiveness by formulating policies that facilitate access for rural, marginalized, and digitally illiterate populations. Continuous review and adaptation of policies will be necessary to keep pace with technological advancements and emerging risks. Furthermore, transparency and accountability mechanisms should be institutionalized within policy frameworks to foster greater trust and participation from the public. Sound policy foundations will enable the successful scaling and sustainability of digital identity initiatives nationwide.

Implications for Concerned Stakeholders

Civil society organizations, technology providers, and advocacy groups hold an essential role in bridging the gap between government initiatives and citizen needs. These stakeholders can champion digital literacy programs and awareness campaigns that empower users to engage confidently with digital identity systems. Their involvement ensures that marginalized and vulnerable populations are not left behind, addressing inclusivity challenges highlighted by the study. Moreover, by participating in policy dialogues and oversight, these actors can help enhance transparency, data protection, and ethical standards in digital identity management. Collaborative partnerships with public sector entities will foster a more accountable and user-responsive digital ecosystem, which is vital for sustaining public trust and encouraging broad-based adoption of digital identity services.

Implications for Further Research

The study opens several avenues for future research, particularly concerning the unexpected finding that user-centricity did not significantly impact public trust. Researchers could explore this phenomenon through qualitative approaches, such as

interviews or focus groups, to understand user experiences and barriers to engagement more deeply. Investigations focusing on rural and marginalized communities are also crucial to identify specific challenges in inclusiveness and accessibility of digital identity systems. Longitudinal studies tracking changes in public trust and adoption over time would provide valuable insights into the dynamics of digital identity implementation. Comparative research across countries or regions could offer lessons on best practices and policy effectiveness. Ultimately, further research should aim to develop more nuanced models that integrate technical, institutional, and social factors influencing digital identity success.

References

Abraham, S. (2020). *Building trust: Lessons from Canada's approach to digital identity*. ORF Issue Brief No. 367.

Allmann, K., & Radu, R. (2023). Digital footprints as barriers to accessing e-government services. *Global Policy, 14*(1), 84–96. https://doi.org/10.1111/1758-5899.13140

Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. *Data & Policy*, *3*, e35. https://doi.org/10.1017/dap.2021.35

Anandaram, S., Chetty, K., Josie, J., & Kripalani, M. (2021). *Digital inclusion strategies for the G20: Lessons in public-private cooperation from India and Africa*. G20 Task Force 4.

Bottarelli, M., Epiphaniou, G., Mahmood, S., Hooper, M., & Maple, C. (2025). Assessing the trustworthiness of electronic identity management systems: Framework and insights from inception to deployment, *International Journal of Management, 6*(4), 321-342.

Checkland, P. (1999). *Systems Thinking, Systems Practice*. Wiley.

Consult Nepal. (2023). *E-Governance in Nepal: Status and Challenges*. Retrieved from https://consultnepal.com/e-governance-in-nepal/

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342. https://doi.org/10.1111/1540-4560.00067

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. https://doi.org/10.2307/249008

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. https://doi.org/10.2307/2095101

Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*, *2*(18). https://doi.org/10.1007/s44206-023-00049-z

Jenkins, R. (2014). *Social Identity* (4th ed.). Routledge.

Jonathan, G. M. (2020). Digital transformation in the public sector: Identifying critical success factors. In *Lecture Notes in Business Information Processing*, l(381), 223–235. Springer. https://doi.org/10.1007/978-3-030-45002-1_20

Kanwar, S., Reddy, A., Kedia, M., & Manish, M. (2022). The emerging era of digital identities: Challenges and opportunities for the G20. *Asian Development Bank Institute*. https://doi.org/10.56506/XCNN8924

Kathmandu Post. (2022). *Digital divide and legal framework issues limit Nepal's digital identity efforts*. Retrieved from https://kathmandupost.com

Klaaren, J. (2023). Changing digital identity systems across Africa. *Digital Society, 2*(18), 1–20. https://doi.org/10.1007/s44206-023-00049-z

Landrigan, M., Wilson, S., & Fraser, H. (2024). Why are there so many digital identities? *Law, Technology and Humans, 6*(1), 1–15. https://doi.org/10.5204/lthj.3096

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 50(1), 62–71. https://doi.org/10.1080/08874417.2009.11645305

Masiero, S., & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development, 27*(1), 1–12. https://doi.org/10.1080/02681102.2021.1859669

Nishant, A., & Brass, I. (2021). Responsible innovation for digital identity systems. *Data & Policy, 3*, e35. https://doi.org/10.1017/dap.2021.35

OnlineKhabar. (2025). *National ID now integrated with Nagarik app: Passport applications made easier*. Retrieved from https://english.onlinekhabar.com/national-id-now-integrated-with-nagarik-app-passport-applications-made-easier.html

Rosner, G. L. (2014). *Identity management policy and unlinkability: A comparative case study of the US and Germany* [Doctoral dissertation, University of Nottingham]. University of Nottingham Repository.

Scott, W. R. (2014). *Institutions and Organizations: Ideas, Interests, and Identities* (4th ed.). Sage Publications.

Stefansson, B., Helgadóttir, A. G., Nizon-Deladoeuille, M., Neukirchen, H., & Welsh, T. (2025). Understanding trust in authentication methods for Icelandic digital public services. *International Journal of Financial Management, 3*(11), 213-224.

Stryker, S., & Burke, P. J. (2000). The past, present, and future of an identity theory. *Social Psychology Quarterly*, 63(4), 284–297. https://doi.org/10.2307/2695840

The Kathmandu Post. (2022). *A legion of safety concerns surrounds national ID scheme*. Retrieved from https://kathmandupost.com/national/2022/09/23/a-legion-of-safety-concerns-surrounds-national-id-scheme

Tiits, M., Kalvet, T., & McBee, D. (2024). Identity theft and societal acceptability of electronic identity in Europe and in the United States, *International Journal of Social Sciences, 7*(3), 196-213.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Von Bertalanffy, L. (1968). *General System Theory: Foundations, Development, Applications*. George Braziller.

World Bank. (2016). *Digital identity: Towards shared principles for public and private sector cooperation*. International Bank for Reconstruction and Development / the World Bank. https://www.worldbank.org

APPENDIX

Questionnaire

There is a structured questionnaire designed using statement-based items on a 5-point Likert scale (Strongly Disagree to Strongly Agree), based on the study topics "Digital Identity Towards Shared Principles for Public Sector Enterprises."

Please indicate the level of agreement with the following statements by choosing one of the options below:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

Q.N.	Statements	SD	D	N	A	SA
Effectiveness of Digital Identity Implementation (EDII)						
$EDII_1$	The current digital identity system has improved access to public sector services.					
$EDII_2$	Digital identity implementation has enhanced transparency and accountability in service delivery.					
$EDII_3$	The digital identity platform operates reliably and with minimal technical issues.					
$EDII_4$	Digital identity has significantly reduced duplication and fraud in public services.					
Policy and Regulatory Readiness (PRR)						
PRR_1	There are clear national policies that support digital identity implementation in public enterprises.					
PRR_2	The legal framework adequately addresses digital identity-related privacy and security concerns.					
PRR_3	Government agencies comply with existing digital identity regulations.					
PRR_4	Policy coordination among various departments supports successful digital identity deployment.					

Technological Infrastructure (TI)						
TI_1	The organization has the necessary IT infrastructure to support digital identity systems.					
TI_2	Internet and network connectivity are reliable for digital identity operations.					
TI_3	The digital identity platform integrates well with existing public sector systems.					
TI_4	There is adequate technical support available for resolving system-related issues.					
Institutional Capacity and Leadership (ICL)						
ICL_1	Public sector leaders actively promote the adoption of digital identity.					
ICL_2	Sufficient training is provided to staff for effective use of digital identity platforms.					
ICL_3	The institution has dedicated personnel for managing digital identity systems.					
ICL_4	Leadership demonstrates a clear vision for digital transformation.					
User Trust and Privacy Perception (UTPP)						
$UTPP_1$	I trust the government to protect my digital identity information.					
$UTPP_2$	The digital identity system ensures strong data privacy and confidentiality.					
$UTPP_3$	There are secure authentication methods in place to access digital identity services.					
$UTPP_4$	The system is transparent about how personal data is stored and managed.					
Inclusiveness and Accessibility (IA)						
IA_1	The digital identity system is accessible to people with limited digital literacy.					

IA_2	Rural and marginalized communities have equal access to digital identity services.					
IA_3	The platform is user-friendly for people of all age groups.					
IA_4	Digital identity registration is available in multiple languages.					
Stakeholder Collaboration (SC)						
SC_1	Government agencies work collaboratively to implement digital identity systems.					
SC_2	Private sector involvement improves the efficiency of digital identity platforms.					
SC_3	Civil society organizations contribute to improving digital identity accessibility.					
SC_4	There is effective coordination among all stakeholders in managing digital identity policies.					

The End!

Descriptive Analysis of Policy and Regulatory Readiness (PRR)

Particular	N	Mean	Std. Deviation
There are clear national policies that support digital identity implementation in public enterprises.	384	2.93	.967
The legal framework adequately addresses digital identity-related privacy and security concerns.	384	2.97	1.000
Government agencies comply with existing digital identity regulations.	384	2.95	1.058
Policy coordination among various departments supports successful digital identity deployment.	384	2.79	.998
Aggregate	384	2.91	1.005

Source: Field Survey, 2025

Descriptive Analysis of Technological Infrastructure (TI)

Particular	N	Mean	Std. Deviation
The organization has the necessary IT infrastructure to support digital identity systems.	384	3.06	.930
Internet and network connectivity are reliable for digital identity operations.	384	2.88	1.018
The digital identity platform integrates well with existing public sector systems.	384	2.93	.902
There is adequate technical support available for resolving system-related issues.	384	3.02	.943
Aggregate	384	2.97	0.95

Source: Field Survey 2025

Descriptive Analysis of Institutional Capacity and Leadership (ICL)

Particular	N	Mean	Std. Deviation
Public sector leaders actively promote the adoption of digital identity.	384	2.97	0.926
Sufficient training is provided to staff for effective use of digital identity platforms.	384	2.89	1.024
The institution has dedicated personnel for managing digital identity systems.	384	2.99	0.959
Leadership demonstrates a clear vision for digital transformation.	384	2.87	0.981
Aggregate	384	2.93	0.97

Source: Field Survey 2025

Descriptive Analysis of User Trust and Privacy Perception (UTPP)

Particular	N	Mean	Std. Deviation
I trust the government to protect my digital identity information.	384	2.86	1.005
The digital identity system ensures strong data privacy and confidentiality.	384	2.91	1.006
There are secure authentication methods in place to access digital identity services.	384	2.95	0.936
The system is transparent about how personal data is stored and managed.	384	3.02	0.974
Aggregate	384	2.94	0.98

Source: Field Survey 2025

Descriptive Analysis of Inclusiveness and Accessibility (IA)

Particular	N	Mean	Std. Deviation
The digital identity system is accessible to people with limited digital literacy.	384	2.95	0.947
Rural and marginalized communities have equal access to digital identity services.	384	2.98	0.995
The platform is user-friendly for people of all age groups.	384	2.95	1.029
Digital identity registration is available in multiple languages.	384	5.00	0.000
Aggregate	384	3.47	0.74

Source: Field Survey 2025

Descriptive Analysis of Stakeholder Collaboration (SC)

Particular	N	Mean	Std. Deviation
Government agencies work collaboratively to implement digital identity systems.	384	2.98	0.995
Private sector involvement improves the efficiency of digital identity platforms.	384	2.95	0.947
Civil society organizations contribute to improving digital identity accessibility.	384	5.00	0.000
There is effective coordination among all stakeholders in managing digital identity policies.	384	2.94	1.029
Aggregate	384	3.46	0.74

Source: Field Survey 2025

Descriptive Analysis of Effectiveness of Digital Identity Implementation (EDII)

Particular	N	Mean	Std. Deviation
The current digital identity system has improved access to public sector services.	384	2.95	0.947
Digital identity implementation has enhanced transparency and accountability in service delivery.	384	2.98	0.995
The digital identity platform operates reliably and with minimal technical issues.	384	3.00	0.876
Digital identity has significantly reduced duplication and fraud in public services.	384	5.00	0.000
Aggregate	384	3.48	0.70

Source: Field Survey 2025

Descriptive Statistics of Variables

Variables	No	Minimum	Maximum	Mean	Std. Deviation	Skewness	Std. Error	Kurtosis	Std. Error
Policy and Regulatory Readiness (PRR)	384	1	5	2.91	0.038	-0.021	0.241	-0.419	0.478
Technological Infrastructure (TI)	384	1	5	2.973	0.948	-0.066	0.241	-0.324	0.478
Institutional Capacity and Leadership (ICL)	384	1	5	2.93	0.972	-0.082	0.241	-0.469	0.478
User Trust and Privacy Perception (UTPP)	384	1	5	2.935	0.98	0.137	0.241	-0.453	0.478
Inclusiveness and Accessibility (IA)	384	1	5	3.47	0.743	-0.003	0.241	-0.429	0.478
Stakeholder Collaboration (SC)	384			3.46	0.740	-0.002	0.241	-0.428	0.478
Effectiveness of Digital Identity Implementation (EDII)	384	1	5	3.483	0.704	0.02	0.241	-0.285	0.478

Correlation Matrix

Variables	EDII	PRR	TI	ICL	UTPP	IA	SC
EDII	1						
PRR	.603**	1					
	0						
TI	.701**	.733**	1				
	0	0					
ICL	.658**	.641**	.656**	1			
	0	0	0				
UTPP	.712**	.673**	.700**	.613**	1		
	0	0	0	0			
IA	.708**	.617**	.690**	.656**	.678**	1	
	0	0	0	0	0		
SC	.707**	.698**	.687**	.643**	.609**	.671**	1
	0	0	0	0	0	0	

** Correlation is significant at the 0.01 level (2-tailed).

Regression Analysis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.788a	0.621	0.61	0.422

a Predictors: (Constant), policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, stakeholder collaboration

b Dependent Variable: effectiveness of digital identity implementation

ANOVA Tests

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	42.217	6	10.554	59.369	.000b
	Residual	25.777	377	0.178		
	Total	67.995	383			

a Dependent Variable: effectiveness of digital identity implementation

b Predictors: (Constant), policy and regulatory readiness, technological infrastructure, institutional capacity and leadership, user trust and privacy perception, inclusiveness and accessibility, stakeholder collaboration

Coefficient Analysis

Model		B	Std. Error	Beta	T	Sig.	Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	0.477	0.172		2.776	0.006	0.137	0.817		
PRR		-0.019	0.071	-0.022	-0.263	0.793	-0.159	0.122	0.389	2.572
TI		0.281	0.081	0.296	3.464	0.001	0.121	0.442	0.359	2.785
ICL		0.247	0.071	0.255	3.499	0.001	0.108	0.387	0.493	2.027
UTPP		0.346	0.074	0.364	4.698	0.000	0.201	0.492	0.436	2.294
IA		0.345	0.073	0.363	4.448	0.000	0.200	0.491	0.439	2.292
SC		0.348	0.075	0.366	4.70	0.000	0.198	0.495	0.433	2.301

a. Dependent Variable: EDII

Significance at 0.01 levels

PAPER NAME

DIGITAL IDENTITY TOWARDS SHARED P RINCIPLES FOR PUBLIC SECTORS ENTE RPRISES

AUTHOR

Rohit Shrestha

WORD COUNT

14794 Words

CHARACTER COUNT

94657 Characters

PAGE COUNT

53 Pages

FILE SIZE

104.2KB

SUBMISSION DATE

Jul 31, 2025 2:59 PM GMT+5:30

REPORT DATE

Jul 31, 2025 3:01 PM GMT+5:30

8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 7% Internet database
- 2% Publications database
- Crossref database
- Crossref Posted Content database
- 0% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Small Matches (Less then 10 words)