ASPECTS OF DIGITAL IDENTITY IN E-COMMERCE

Sarbast Qader Mohamedamin

2025

ASPECTS OF DIGITAL IDENTITY IN E-COMMERCE

Sarbast Qader Mohamedamin

OTS
CANADIAN JOURNAL
OTTAWA, ONTARIO
CANADA

PUBLISHED BY

OTS CANADIAN JOURNAL
OTTAWA, ONTARIO
CANADA

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA
MOHAMEDAMIN SARBAST QADER , 2025

ASPECTS OF DIGITAL IDENTITY IN E-COMMERCE
ISBN: 978-1-7389655-5-7

CONTENTS

CONTENTS

PREFACE

In the rapidly evolving digital landscape, the concept of identity has undergone a profound transformation. What once was firmly rooted in physical documents and face-to-face interactions has now expanded into a complex web of data points, authentication methods, and regulatory frameworks. This book, Aspects of Digital Identity in E-Commerce, emerged from both academic inquiry and practical concern over how digital identities are created, managed, and secured in the dynamic environment of electronic commerce.

As a researcher and professional deeply engaged in the intersection of technology, law, and business, I have witnessed firsthand the critical role digital identity plays in shaping user trust, safeguarding privacy, and driving innovation. The increasing dependence on online transactions has made it imperative to understand the mechanisms behind digital identity, not merely as a technical construct but as a multifaceted phenomenon with social, economic, and legal dimensions.

This work aims to offer a comprehensive exploration of digital identity as it relates to the e-commerce sector. Drawing on case studies from various jurisdictions—including the United States, Canada, the European Union, and key international examples—it compares global approaches to digital identity management and investigates the role of regulations such as GDPR and eIDAS in shaping secure digital ecosystems. The journey of writing this book has been both intellectually enriching and personally rewarding. I am grateful to the mentors, colleagues, and institutions that have supported my research, and I sincerely hope that readers—whether scholars, practitioners, policymakers, or students—find the insights within these pages useful for navigating the future of identity in the digital economy.

Sarbast Qader Mohamedamin
Erbil, 2025

SUMMARY

This research explores the diverse facets of digital identity in the realm of e-commerce, investigating its creation, management, regulation, and practical applications. Through a comparative analysis of case studies from the United States, Canada, India, and the European Union, the study illuminates the varying approaches and challenges associated with digital identity frameworks in different countries. The findings highlight the critical role of digital identity verification in enhancing security, improving customer experiences, and reducing fraud in online transactions.

The study underscores the importance of robust digital identity verification mechanisms in e-commerce, emphasizing the need for businesses to prioritize user privacy and regulatory compliance to build trust with customers. Furthermore, the research offers insights into the transformative potential of digital identity verification in enhancing the overall customer journey and facilitating business expansion. Based on the findings, the study recommends further research to explore the efficacy of different digital identity verification methodologies, technologies, and their impact on customer trust and loyalty.

Additionally, there is a need to investigate the scalability and interoperability of digital identity solutions to meet the evolving demands of the e-commerce sector. In conclusion, this research underscores the critical role of digital identity verification in e-commerce, offering valuable insights for businesses looking to enhance security, customer satisfaction, and growth in the digital landscape.

This page intentionally left blank

CHAPTER ONE

1. Introduction

E-commerce is essential to the global economy in the modern digital era, and it has changed the landscape for businesses and how consumers experience the products and services around us. At the core of the shift to a device-centric economy is the notion of digital identity, or the unique identifiers and personal data that enable individuals to operate within the digital ecosystem. Digital identification in online business encompasses many domains, which include authentication, privacy, security, and user enjoy, performing a pivotal position in constructing consider and feature of online transactions.

In simple terms, most digital identities in e-commerce are artificial surrogates for individual people/entities that can be used in transactions in place of the personal identities of the parties involved. The identity comprises components of identity such as user names, passwords, biometric and digital certificates that be used to authenticate that the user is who they claim to be. The integrity of digital identity is paramount when it comes to safeguarding transaction fluidity, thwarting fraud, bolstering consumer confidence and impacting the national economy; all vitally important[1].

At the core of digital identity are authentication mechanisms — confirming that users are who they say they are. Mechanisms such as passwords are increasingly being augmented or replaced with more advanced techniques such as multi-factor authentication (MFA), biometric verification and

[1] Bădîrcea, R. M., Manta, A. G., Florea, N. M., Popescu, J., Manta, F. L., & Puiu, S. (2021). E-commerce and the Factors Affecting its Development in the Age of Digital Technology: Empirical Evidence at EU–27 level. *Sustainability*, *14*(1), 101.

blockchainxCFREE. These advances seek to boost security and diminish the risk of fraud and unauthorized access (significant issues in the digital marketplace)[2].

The management of digital identity and privacy and security issues are at key questions here. Consumers are wising up to data rights and data misuse This has subsequently forced businesses to manoeuvre through a complicated network of data protection regulations from the General Data Protection Regulation'(GDPR) to the California Consumer Privacy Act (CCPA). Adherence to these regulations is not only in place to maintain consumer safety, but is established as an essential component for building data trust and brand loyalty, which are the two key ingredients for successful e-commerce brands in the long-run[3].

Another key area that digital identity impacts is customer experience. Customer satisfaction will improve when the authentication process is both smooth and intuitive, thereby encouraging repeat business. In contrast, heavy-handed or intrusive identity verification can repel would-be customers and tarnish their perception of the brand. As a result, businesses need to ensure strong security measures elsewhere while ensuring that the digital commerce experience remains optimised for users[4].

In addition, the introduction of Decentralized Identities by the blockchain technology signals a major move in the way we currently manage and consume digital identity. Decentralized identities are designed to assign every single user the same level of data ownership and control that big

---

[2] Feher, K. (2021). Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. *Journal of information science*, *47*(2), 192-205.

[3] Tofan, M., & Bostan, I. (2022). Some implications of the development of E-commerce on EU tax regulations. *Laws*, *11*(1), 13.

[4] Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, *8*(1), 104-110.

companies have (the ones that keep getting hacked); Once every citizen in the digital universe has as simple a means to certify their identity online as companies do, the target is lowered for the hackers and centralized data controllers. Changing this paradigm has the potential to disrupt digital identity management in e-commerce by giving more freedom and control to consumers[5].

Moreover, features of digital identity in e-commerce: is not only digital, but includes authentication, security, privacy and user experience in general. With the rapid progress in the digital world, companies are constantly revising their strategies to cater to a mounting need for reliable, secure and easy-to-navigate identity services[6]. These parts that can actually make user rejoice are what he/she needs to fully understand and effectively deal with in order to gain trust, have the right consistency and ultimately succeed in the highly competitive world of e-commerce arena.

1.1 Background and Context

The e-commerce revolution of the last couple of decades has seamlessly orchestrated the digital marketplace and the purchasing habits of shoppers from all across the world with the opportunity to buy/sell products devoid of geographical constraints. Over time, the evolution in internet technology, combined with mobile connectivity and digital payment systems, has enabled a

[5] Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673-1685.

[6] Sepashvili, E. (2020). Digital chain of contemporary global economy: e-commerce through e-banking and e-signature. *Economia Aziendale Online-*, *11*(3), 239-249.

frictionless experience for consumers making transactions online. The challenge is, with the rise of e-commerce, the need to manage digital identity is more important than ever[7].

Digital identity is a crucial component of any secure online interaction, allowing the verifying and authenticating of individuals and thereby guaranteeing that transactions and interactions are real and safe. Traditional digital identities were simple username and password based identities. But the age-old methods have limitations and vulnerabilities and are now replaced by more advanced identity management solutions[8].

The early 2000s observed an explosive rise in incidents of identity theft and cybercrime, revealing the weak security of password-centric systems. The industry thus started investigating more sophisticated mechanisms for user authentication, one of them being multi-factor authentication (MFA), which utilizes a combination of aspects: something the user knows (password), something the user has (security token), and something the user is (biometric verification). This multi-tier approach vastly increases security, as it makes it much harder for unauthorized persons to access sensitive data[9].

At the same time, the growing computerization of much personal data posed major threats to privacy. With high-profile data breaches and increased concern about the ways in which data may be exploited, it focused attention onto businesses and how they collect, store and use personal

---

[7] Chin, S. H., Lu, C., Ho, P. T., Shiao, Y. F., & Wu, T. J. (2021). Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things. *Computer Standards & Interfaces*, *76*, 103504.

[8] Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395-410.

[9] Din, A. U., Han, H., Ariza-Montes, A., Vega-Muñoz, A., Raposo, A., & Mohapatra, S. (2022). The impact of COVID-19 on the food supply chain and the role of e-commerce for food purchasing. *Sustainability*, *14*(5), 3074.

information. There are regulatory frameworks such as the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) in the United States to respect the rights of data subjects, while tightening data protection regulations. These laws require businesses to have strong data security practices, and give individuals more visibility and control over their personal data[10].

One of the popular technical innovation that has also played its part in the evolution of digital identity management is blockchain. An immutable, decentralized ledger like blockchain can be a solution to transparency and security with digital identity, which is referred to as Self-Sovereign Identity. Decentralized: DIDs enable verifiable, self-owned identities that work online, for free, without the need for a central authority. It gets rid of the risks of having all data stored in a centralized location (ie a data breach that would affect all data) and it gives the user more control over personal information[11].

Additionally, the increasing number of mobile devices along with the advent ofmCommerce have brought a fresh twist to digital identity management. With the combination of biometric sensors and secure elements, mobile devices have become a great way to secure and authenticate users. This has been supplemented by the spawn of mobile wallets and payment apps that leverage these, further underscoring the need for a strong digital identity solution to transact securely on mobile.

[10] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

[11] Esmeli, R., Bader-El-Den, M., & Abdullahi, H. (2022). An analyses of the effect of using contextual and loyalty features on early purchase prediction of shoppers in e-commerce domain. *Journal of Business Research*, *147*, 420-434.

In the era of digital commerce, businesses must delicately balance collection, storage and management of identity data with security, privacy and customer experience. User must strike a balance of tight security features to shield against fraud and cyber threats but also offer authentication that is seamless enough that it does not worsen the customer experience. In addition, legal implications and trust in the given legal compliance with data protection regulations[12].

There is no doubt that the more knowledge acquired regarding the digital identity landscape in e-commerce, the better mechanisms and solutions can be developed, that go a long way in solving the many aspects attributed to this subject in an effective manner. Investing in technical innovations, whilst ensuring that these are in line with regulations, help businesses to deliver secure, private and frictionless digital experiences that instil consumer trust and power growth across the e-commerce space[13].

1.2 Purpose of the Research

The primary purpose of this research is to explore and analyze the various aspects of digital identity in the context of e-commerce. As e-commerce continues to expand and evolve, understanding the complexities and nuances of digital identity becomes crucial for businesses, consumers, and policymakers. This research aims to provide a comprehensive examination of the mechanisms, challenges, and innovations associated with digital identity management in e-commerce, with the ultimate goal of identifying best practices and strategies to enhance security, privacy, and user experience.

---

[12] Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.

[13] Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.

1.3 Research Objectives

- To investigate the current and emerging authentication mechanisms used in e-commerce to verify and authenticate users.
- To analyze the privacy and security issues associated with digital identity in e-commerce.
- To review the impact of data protection regulations, such as GDPR and CCPA, on digital identity management in e-commerce.
- To examine how digital identity management affects the user experience in e-commerce.
- To explore the role of emerging technologies, such as blockchain and decentralized identifiers (DIDs), in shaping the future of digital identity management in e-commerce.
- To develop a set of recommendations and best practices for businesses to effectively manage digital identities in e-commerce.

1.4 Scope and Limitations

1.4.1 Scope

Research that Address the various facets of Digital Identity in E-commerce :

- Authentication Mechanisms:

Analysis of different methods of authentication like use of passwords, multi-factor authentication (MFA), biometrics, and blockchain-based solutions[14].

- Privacy and Security:

[14] Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825.

Security threats related to digital identity – investigates popular modes of security threats such as identify theft, data breaches, and unauthorized access[15].

- Regulatory Frameworks:

AmStrong Compliant Data Protection Regulation May 6·8 min read Review of major compliance laws on data protection including GDPR and CCPA[16].

- User Experience:

A case study on how Digital Identity verification processes may affect user experience in e-commerce[17].

- Technological Innovations:

Research in new technologies such as Blockchain and DIDs and the place of these technologies in digital identity management[18].

1.4.2 Limitations

Although this research strived to provide a holistic insight into the topic of digital identity in e-commerce, a number of caution statements are warranted (Svobodová and Rajchlová, 2020).

- Technological Scope:

---

[15] Luo, N., Wang, Y., Zhang, M., Niu, T., & Tu, J. (2020). Integrating community and e-commerce to build a trusted online second-hand platform: Based on the perspective of social capital. *Technological Forecasting and Social Change*, *153*, 119913.

[16] Alsubari, S. N., Deshmukh, S. N., Al-Adhaileh, M. H., Alsaade, F. W., & Aldhyani, T. H. (2021). [Retracted] Development of Integrated Neural Network Model for Identification of Fake Reviews in E-Commerce Using Multidomain Datasets. *Applied Bionics and Biomechanics*, *2021*(1), 5522574.

[17] Kiba-Janiak, M., Marcinkowski, J., Jagoda, A., & Skowrońska, A. (2021). Sustainable last mile delivery on e-commerce market in cities from the perspective of various stakeholders. Literature review. *Sustainable Cities and Society*, *71*, 102984.

[18] Vieira, J., Frade, R., Ascenso, R., Prates, I., & Martinho, F. (2020). Generation Z and key-factors on e-commerce: A study on the portuguese tourism sector. *Administrative Sciences*, *10*(4), 103.

The fast-moving technology landscape may also result in newer, emerging technologies and solutions being explored only to a limited depth or going beyond what is currently covered in this study[19].

- Regulatory Variability:

The analysis is focused on well known regulations such as GDPR and CCPA It is not a full list for all global regulatory frames — in particular where legal landscapes are fast changing in certain regions[20].

- User Diversity:

The research also accepts that people's experiences and opinions with digital identity management are likely to differ significantly according to their age, technology literacy and the culture they represent[21].

- Data Availability:

The analysis is a desk review based on existing literature, case studies and available data, which may not provide insights on all aspects of digital identity management purposes[22].

---

[19] Landim, A. R. D. B., Pereira, A. M., Vieira, T., de B. Costa, E., Moura, J. A. B., Wanick, V., & Bazaki, E. (2022). Chatbot design approaches for fashion E-commerce: an interdisciplinary review. *International Journal of Fashion Design, Technology and Education*, *15*(2), 200-210.

[20] Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.

[21] Jain, G., Kamble, S. S., Ndubisi, N. O., Shrivastava, A., Belhadi, A., & Venkatesh, M. (2022). Antecedents of Blockchain-Enabled E-commerce Platforms (BEEP) adoption by customers–A study of second-hand small and medium apparel retailers. *Journal of Business Research*, *149*, 576-588.

[22] Achmad, W. (2023). MSMEs Empowerment through Digital Innovation: The Key to Success of E-Commerce in Indonesia. *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 469-475.

CHAPTER TWO

2. Digital Identity Role and Components

2.1 Definition and Importance of Digital Identity

In fact, digital identity is simply an identity of individuals, organizations, or electronic devices when interacting online. This is a bunch of numbers and information that user needed to act as a person in the digital world. Examples of these identifiers would be usernames, passwords, social media profiles, biometric data like fingerprints and facial recognition, digital certificates, and other authentication credentials. A digital identity is an online representation of an individual that is created, cultivated, amended and represented in given online environments and is used for access of services and resources[23]. Digital identity consists of many components including:

An Identifier is some piece of information that is unique to the user for that system. Usernames, email addresses, or national identification numbers. These IDs identify the users through the system, and if the user needs to be able to access a particular resource or perform that particular action, it is the right these IDs hold[24].

Legal attributes — Attributes about the user that pertain to their identity. This may include data about age, gender, location, and (or) preferences These are the properties which help in solidifying a users profile within a system and can be used to enrich their experience or provide better services[25].

---

[23] Lee, C. S. (2022). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13-14), 2529-2553.

[24] Hongmei, Z. (2021). A cross-border e-commerce approach based on blockchain technology. *Mobile Information Systems*, *2021*, 1-10.

[25] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, *5*(2), 206-221.

Authentication credentials are the methods of how to provide confirmation that it is new identity that is trying to sign in to the system. These can be passwords, PINs (like Personal Identification Numbers), biometric data (fingerprints, facial recognition) or multi-factor authentication (MFA). These are what determine whether an individual is or is not authorized to access a system or a resource[26].

Authorization information provides rules about what a user can do in a digital system. This may determine what operations or functions a user is allowed to perform, what resources the user can access, and what data the user can read or write. This is known as Authorization and is used for security and access within a system to make sure that users can only use resources and information that they are authorized to access (Willemyns, 2020).

2.2 Significance of Digital Identity

- Why Digital Identity Matters in E-commerce?

One aspect of the modern digital landscape that is of utmost importance is security, especially when it comes to online transactions or personal data. Secure authentication is important to prevent unauthorized access, and to reduce the risk of identity theft, fraud, and cyber-attacks. The implementation of secure digital identity management systems secures the access of specific services to specific groups of people, which significantly enhances security, especially in areas related to e-commerce, where there are a large number of transmitted sensitive data.

Trust and Confidence — The pillars of e-commerce. It customers need o feel safe that information, which is personal, is safe and the transaction towards threats. Identity management takes centre

[26] Li, H., Hu, Q., Zhao, G., & Li, B. (2022). The co-evolution of knowledge management and business model transformation in the post-COVID-19 era: insights based on Chinese e-commerce companies. *Journal of Knowledge Management*, *26*(5), 1113-1123.

stage in establishing this trust by verifying users and securing relationships between users and service providers.

Another area of digital identity management is the user experience. Such a system would serve the dual purpose of benefiting users in providing quick and easy access to services and agencies in ensuring the necessary security and integrity of services. Technologies like single sign-on (SSO) and biometric authentication can streamline the login process, positively impacting overall user experience. In the world of e-commerce, user experience plays a huge role in keeping customers with an online store. A good user experience can improve customer loyalty, and potentially be the success factor for long-term survival in the digital marketplace for any business[27].

- Regulatory Compliance:

Modern software services, especially those in the cloud-native world, are extraordinary data sensitive and therefore are held to some of the most stringent data protection standards out there (GDPR, CCPA, and more). These rules describe much better how personal data may be collected, saved, and used, to protect the private and safe handling of people's personal information[28].

Conforming to these regulations ensures that software services avails minimal legal risks and shows they are sincerely in data protection of the end user. Compliance also builds trust with consumers who are more cautious in their use of data than in the past. Compliance with these regulations allows companies to display more transparency and reliability, among many other factors which could boost customer trust as well as positive brand recognition. Not only is

[27] Xiong, X., Yuan, F., Huang, M., Cao, M., & Xiong, X. (2020). Comparative evaluation of web page and label presentation for imported seafood products sold on Chinese e-commerce platform and molecular identification using DNA barcoding. *Journal of food protection*, *83*(2), 256-265.

[28] Sutinen, U. M., Saarijärvi, H., & Yrjölä, M. (2022). Shop at your own risk? Consumer activities in fashion e-commerce. *International Journal of Consumer Studies*, *46*(4), 1299-1318.

integrating data protection compliance in software services good practice to adhere to the law, it is also consistent with ethical principles. Respecting the rights of individuals in the processing of their data, the company proves to be a player in compliance with good data management practices. This is a competitive differentiator, as consumers are much more willing to trust, and do business with those organizations that put their privacy and security[29].

- Innovation and Growth:

Technologies like blockchain and decentralized identifiers (DIDs) are examples of an evolving landscape of how digital identity management is coming to open the door for new opportunities for innovation. These innovations will translate to more secure, efficient and user-friendly identity products[30].

Adopting both of these innovations helps e-commerce businesses remain competitive, responsive to changing dynamics, and very importantly, seek new ways of doing business[31]. Digital identity forms the foundation of e-commerce business and directly affects security, trust, user experience, compliance, personalization, and innovation. As e-commerce flourishes and grows, managing digital identity becomes more and more critical. Companies will need to invest in advanced digital

[29] Lucas, G. A., Lunardi, G. L., & Dolci, D. B. (2023). From e-commerce to m-commerce: An analysis of the user's experience with different access platforms. *Electronic Commerce Research and Applications*, *58*, 101240.

[30] Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. *GSC Advanced Research and Reviews*, *18*(3), 066-077.

[31] Khrais, L. T., Zorgui, M., & Aboalsamh, H. M. (2023). Harvesting the digital green: A deeper look at the sustainable revolution brought by next-generation IoT in E-Commerce. *Periodicals of Engineering and Natural Sciences*, *11*(6), 5-13.

identity solutions that allow for secure, seamless and personalized interactions in the digital commerce space[32].

2.3 Key Components of Digital Identity

2.3.1 Identifiers

Digital identities are a key enabler to the digital world and identifier systems play a major role in the creation and management of digital identities. These identifiers find, which are unique data points that separate one user from another that are linked to every piece of account ID user needs to access myriad of digital services. Identifiers (usernames, email, social media handle, user ID, etc which is used to identify a user entity on a digital platform)[33].

Email addresses were used as both identifiers and communication gateways, connecting users to their accounts and services Another best-known identifier are phone numbers, that allows verification and two-factor authentication, serving to defend digital identities. In the United States, IDs like Social Security Numbers (SSN) or in the UK National Insurance Numbers (NIN) a National ID is a valid, officially official ID for identification purposes and for use in opening bank accounts and for official and legal purposes by the government[34].

Although IPs are not permanent, they can be used to identify where user lives, but also ISP. Though critical for establishing and maintaining digital identities, identities must be handled carefully to

---

[32] Kleisiari, C., Duquenne, M. N., & Vlontzos, G. (2021). E-Commerce in the Retail Chain Store Market: An Alternative or a Main Trend?. *Sustainability*, *13*(8), 4392.

[33] Al Mashalah, H., Hassini, E., Gunasekaran, A., & Bhatt, D. (2022). The impact of digital transformation on supply chains through e-commerce: Literature review and a conceptual framework. *Transportation Research Part E: Logistics and Transportation Review*, *165*, 102837.

[34] Li, M., Shao, S., Ye, Q., Xu, G., & Huang, G. Q. (2020). Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. *Robotics and Computer-Integrated Manufacturing*, *65*, 101962.

avoid privacy and security constraints for the user. Strong security precautions, to meet rising regulatory standards on data protection, are compulsory to preserve the integrity and credibility of digital identities[35].

2.3.2 Attributes

Attributes represent concrete characteristics or data that come with a digital identity to help us paint a thorough picture of the user. These qualifiers provide more context to who the user is and what they are interested in. Many unique or intelligent entities are used to process personal information, with the help of managing and analyzing digital identities-associated data[36].

Behavioural data is another extremely important feature, which relates directly to how a user is acting online. Whether it is what page they are browsing, the products they are buying or how they are interacting with a website or an app. We also introduced the concept of preferences which represent account settings like the language of preference, user specific settings for communication, etc[37].

It can also be equipped with the biometric data of the user and can use fingerprint, facial recognition data, retinal scans, etc., which is a unique way to identify an individual securely. Finally, using location-based services to create contextual context data (obtained with geolocation data provided through, for example: IP addresses, GPS, or equivalent, about places where the

---

[35] Ballerini, J., Yahiaoui, D., Giovando, G., & Ferraris, A. (2024). E-commerce channel management on the manufacturers' side: ongoing debates and future research pathways. *Review of Managerial Science*, *18*(2), 413-447.

[36] Geng, R., Wang, S., Chen, X., Song, D., & Yu, J. (2020). Content marketing in e-commerce platforms in the internet celebrity economy. *Industrial Management & Data Systems*, *120*(3), 464-485.

[37] Ahmad, A. Y. B., Gongada, T. N., Shrivastava, G., Gabbi, R. S., Islam, S., & Nagaraju, K. (2023). E-commerce trend analysis and management for Industry 5.0 using user data analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(11s), 135-150.

application is running). This can allow to serve targeted advertisement or product recomendation base on user geo-location and context data[38].

In summary, attributes are essential in defining the traits, attributes, and qualities of specific digital identities. It, therefore, enables an organization to tailor the experience with users and formulate behavior and preferences insights. But this data is very sensitive — it has to be handled with care to make sure users remain secure and private. Ensuring that digital identities comply with data protection laws and have sound security arrangements is a necessary foundation to keeping them trustworthy in the long term[39].

2.3.3 Authentication Methods

There is an authentication mechanism that helps confirm the genuineness of users and establishes only authenticated users are allowed to grant access to the resources and services they plan to use. These provide critical layer before digital identities enabling verify the genuineness of users before providing the access[40]. This can be user's password which is something user knows, a second factor (or third) that is something user has—such as smartphone— representing the case where biometric data is the second factor[41]. All of these mechanisms for authentication reduce the risk of unauthorized access, and ensure a degree of confidence that sensitive information is safe from

[38] Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: a framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054.

[39] Bădîrcea, R. M., Manta, A. G., Florea, N. M., Popescu, J., Manta, F. L., & Puiu, S. (2021). E-commerce and the Factors Affecting its Development in the Age of Digital Technology: Empirical Evidence at EU–27 level. *Sustainability*, *14*(1), 101.

[40] Feher, K. (2021). Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. *Journal of information science*, *47*(2), 192-205.

[41] Tofan, M., & Bostan, I. (2022). Some implications of the development of E-commerce on EU tax regulations. *Laws*, *11*(1), 13.

compromise. Organizations that adopt strong authentication will improve their Digital Identity security profile and protect the integrity of their Identity systems[42].

- Passwords:

The most widely recognized type of confirmation conventional passwords that expect clients to type in a secret word or expression with the end goal to validate access to their records. But classic passwords can be attacked in many ways, one of the lowest hanging fruits is brute-force attacks, where an attacker tries the password the brute way, see what sticks and what breaks[43].

To increase the security of user's password, it is recommended to use passwords with a more complex mixture of letters, digits, and symbols. It only makes the password more expensive to guess or to crack by any automated brute force type tools. In other words, the password becomes more secure if user uses multiple words or avoid using basic words or phrases for the password[44]. Also, user should have different passwords for different accounts, and change user's passwords regularly in order to reduce the likelihood of unauthorized access. Even if n attacker does manage to steal plaintext password, the damage will be limited since the secrets cannot be decrypted without the master key, protection keys, or other user's key enabling two-factor authentication (2FA)/multi-factor authentication (MFA)[45].

---

[42] Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, *8*(1), 104-110.

[43] Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673-1685.

[44] Sepashvili, E. (2020). Digital chain of contemporary global economy: e-commerce through e-banking and e-signature. *Economia Aziendale Online-*, *11*(3), 239-249.

[45] Chin, S. H., Lu, C., Ho, P. T., Shiao, Y. F., & Wu, T. J. (2021). Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things. *Computer Standards & Interfaces*, *76*, 103504.

- Multi-Factor Authentication (MFA)

Two-Factor Authentication (2FA for short) is a good choice for increasing the security of an account, and requires the use of two forms of identification before access is allowed. More often than not, this is something the user knows (like a password) and something the user has (like their mobile phone to receive a verification code). This has become much more secure, however, as even if the password is exposed by a breach, the second factor is required to gain access[46].

Multi-Factor Authentication (MFA) does just that, except user guessed it, instead of 2 there are more, components to the verification. Three-Factor Authentication, for instance, would combine something the user knows (password) with something the user has (such as a mobile phone to receive a verification code) and something the user is (biometric verification — fingerprint, face scan). That provides an additional layer of security against unauthorized access since it all combines different varieties of authentications which makes it more difficult for the attacker to bypass[47].

- Biometric Authentication:

Biometric authentication methods —(functions as a fingerprint scan, facial recognition, or retinal scan) have become a dominant tool for verifying users by assessing special biological traits[48].

---

[46] Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395-410.

[47] Din, A. U., Han, H., Ariza-Montes, A., Vega-Muñoz, A., Raposo, A., & Mohapatra, S. (2022). The impact of COVID-19 on the food supply chain and the role of e-commerce for food purchasing. *Sustainability*, *14*(5), 3074.

[48] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

Fingerprint scanning uniquely identifies a person using the unique ridges and valleys in their fingerprints. Because each of these patterns is unique to the individual, it is very hard to copy and therefore it is very secure form of authentication[49].

Facial recognition technology identifies and measures the characteristics of a face, such as the distance between the eyes, width of the nose, and shape of the cheekbones. This data is then utilized in the process of validating the person making the request which provides a seamless and secure manner in which to authenticate the users[50].

Inspired by this difference, they created a fingerprint-like pattern that can correctly identify a person as being exactly the who they claimes to be, using it as a gate to unlock a person's security system[51]. Biometric authentication methods can provide strong security and usability, and are well-suited to secure digital identities in a range of use cases, such as access control and web authentication.

- Token-Based Authentication:

Physical items that generate codes or responses in the authentication processHardware Tokens_generate time-sensitive codes or responses that must be submitted during the authentication process to prove identity within a certain timeframe. These tokens are typically issued in the form of a key fob or a smart card, and they provide an added layer of security, usually

[49] Esmeli, R., Bader-El-Den, M., & Abdullahi, H. (2022). An analyses of the effect of using contextual and loyalty features on early purchase prediction of shoppers in e-commerce domain. *Journal of Business Research*, *147*, 420-434.

[50] Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.

[51] Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.

used for two-factor authentication (2FA). Since these are codes or responses from hardware tokens, there is encryption and randomization built into the generation of each unique code/proper response[52].

Software tokens which are applications or software programs that serve the same function as hardware tokens. These are usually embedded in a smartphone or other device and generate one time passwords (OTPs) user can use to prove user's identity. Software tokens, on the other hand, are user-friendly because they do not require users to carry physical equipment, and they can be readily plugged in to existing systems[53].

This extra layer in the authentication process makes hardware and software tokens cryptographically secure, aiding in keeping digital identities secure from being targeted or accessed illegally[54].

- Behavioral Biometrics:

Behavioral traits can be a keystroke dynamics, mouse movements and so far can be used for the purpose of authentication and identification[55]. By contrast, keystroke dynamics represents the

[52] Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825.

[53] Luo, N., Wang, Y., Zhang, M., Niu, T., & Tu, J. (2020). Integrating community and e-commerce to build a trusted online second-hand platform: Based on the perspective of social capital. *Technological Forecasting and Social Change*, *153*, 119913.

[54] Alsubari, S. N., Deshmukh, S. N., Al-Adhaileh, M. H., Alsaade, F. W., & Aldhyani, T. H. (2021). [Retracted] Development of Integrated Neural Network Model for Identification of Fake Reviews in E-Commerce Using Multidomain Datasets. *Applied Bionics and Biomechanics*, *2021*(1), 5522574.

[55] Kiba-Janiak, M., Marcinkowski, J., Jagoda, A., & Skowrońska, A. (2021). Sustainable last mile delivery on e-commerce market in cities from the perspective of various stakeholders. Literature review. *Sustainable Cities and Society*, *71*, 102984.

analysis of the way an individual types on a keyboard and involves typing speed, pacing and how much pressure is used on keys. Everyone has a unique typing pattern, which can be helpful in recognizing their identity. Therefore, Keystroke dynamics provide a second layer of security alongside the traditional methods of authentication, such as password[56].

Meanwhile, mouse movement analysis is dedicated to how a person moves and works with a mouse or trackpad. … This may be the speed of movement, acceleration of movement, mouse coordinates.trace, etc. Homologous to keystroke dynamics, all of us do have a distinctive manner we shift the mouse and this can be employed to verify users[57].

Both keystroke dynamics and mouse movement analysis are an example of behavioural biometrics, which could Arm access controls with another security measure by measuring of how similar current actions correlate to historic actions in the form of patterns. These are particularly helpful for continuous authentication in systems that continually verify the identity of the user during the time they are using the system[58].

- Authentication based on blockchains

DID stands for Decentralized Identifiers, which are identifiers that are created and controlled by an entity (like a person, team, organization, etc) without the need of any centralized registration or coordination point. DIDs are usually placed on a blockchain — a secure, tamper evident way to

[56] Vieira, J., Frade, R., Ascenso, R., Prates, I., & Martinho, F. (2020). Generation Z and key-factors on e-commerce: A study on the portuguese tourism sector. *Administrative Sciences*, *10*(4), 103.

[57] Svobodová, Z., & Rajchlová, J. (2020). Strategic behavior of e-commerce businesses in online industry of electronics from a customer perspective. *Administrative Sciences*, *10*(4), 78.

[58] Landim, A. R. D. B., Pereira, A. M., Vieira, T., de B. Costa, E., Moura, J. A. B., Wanick, V., & Bazaki, E. (2022). Chatbot design approaches for fashion E-commerce: an interdisciplinary review. *International Journal of Fashion Design, Technology and Education*, *15*(2), 200-210.

handle digital identities. This will help people manage their virtual identity better, hence reducing the risks of identity theft and fraud using DIDs[59].

Digital identities comprise of attributes, authentication factor types, DIDs and more. Attributes: Individual characteristics or data points that are part of a digital identity and can paint a more nuanced picture of the person in question. Types of Authentication Factors are the ways people use to verify their identity — passwords, biometric data, hardware tokens[60].

Managing these well, and securing them, becomes essential to providing a safe and friendly experience. This includes using robust authentication, encrypting data, and keeping security measures up to date to stave off new threats. When these components are managed well, users can also have a greater degree of confidence in the security and privacy of their digital identities[61].

2.4 The Role of Digital Identity in E-Commerce

E-commerce — The operation of an e-commerce firm relies largely on digital identity, to handle operations, as well as customer contacts. It is necessary for security, trust, user experience, personalization, regulatory standards compliance Security — Since a digital identity confirms the identity of users and controls access to valuable information. Moreover, securing authentication

[59] Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.

[60] Jain, G., Kamble, S. S., Ndubisi, N. O., Shrivastava, A., Belhadi, A., & Venkatesh, M. (2022). Antecedents of Blockchain-Enabled E-commerce Platforms (BEEP) adoption by customers–A study of second-hand small and medium apparel retailers. *Journal of Business Research*, *149*, 576-588.

[61] Achmad, W. (2023). MSMEs Empowerment through Digital Innovation: The Key to Success of E-Commerce in Indonesia. *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 469-475.

mechanisms such as the use of biometric authentication will iron out fraud and unauthorised access[62].

In e-commerce, trust is key, and trust is only possible when personal data is secure, thanks to trusted digital identities. In addition, a smooth digital identify solution also does a service to the user experience as a whole. These features can enhance user experience and improve customer satisfaction and loyalty, too, with features integrating single sign-on and personalized recommendations based on user preferences[63].

Digital identity also significantly shapes personalization. Businesses can also customize service offerings and promotional messages to reflect customer preferences and behavior, driving higher consumer engagement and sales. Finally, it is vital to be compliant with regulatory standards like GDPR and CCPA. The company ensures compliance with the most stringent legislative security and privacy requirements thanks to its solid digital identity system, managing and protecting customer data in a secure manner[64].

In the near future, digital identity will further define e-commerce, especially for the new use cases. Could a completely new way to interact and transact online, based on standalone digital identities not limited to any particular platform be worth $33 billion? The incorporation of secure and

---

[62] Lee, C. S. (2022). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13-14), 2529-2553.

[63] Hongmei, Z. (2021). A cross-border e-commerce approach based on blockchain technology. *Mobile Information Systems*, *2021*, 1-10.

[64] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, *5*(2), 206-221.

convenient digital identity systems will likely give businesses an edge in an increasingly mature e-commerce world[65].

- Enhancing Security

In e-commerce, it is a piece in the puzzle of digital identity management geared towards preventing fraud. Identity checking stops fraudulent activities. Methods that use strong authentication, like multi-factor or biometric authentication, ensure that no one who is unauthorized can enter into the system[66].

Secure digital identity Data integration across all channelsEnsures safe and secure transactions It helps in ensuring the legitimacy of the operations and safeguards sensitive data including payment details, and user personally identifiable information against cyber threats and breaches[67].

Access control is crucial for the management of digital identity as well. It permits businesses to control secure areas of their e-commerce systems, providing access to higher systems and information by authorized personnel only that will help to stop unauthorized access to our data and avoid our data being hacked[68].

- Building Trust

---

[65] Li, M., Shao, S., Ye, Q., Xu, G., & Huang, G. Q. (2020). Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. *Robotics and Computer-Integrated Manufacturing*, *65*, 101962.

[66] Willemyns, I. (2020). Agreement forthcoming? A comparison of EU, US, and Chinese RTAs in times of plurilateral E-Commerce negotiations. *Journal of International Economic Law*, *23*(1), 221-244.

[67] Wang, Y., Lu, Z., Cao, P., Chu, J., Wang, H., & Wattenhofer, R. (2022). How live streaming changes shopping decisions in E-commerce: A study of live streaming commerce. *Computer Supported Cooperative Work (CSCW)*, *31*(4), 701-729.

[68] Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. *computers*, *9*(3), 66.

For Ecommerce Business, Good Customer confidence is much important. Consumers also know that if their data and identity are safe, and transactions are secure, they will be more likely to carry out transactions on the platform as well. This hinges on a strong foundation of digital identity that prioritizes security and privacy[69].

Trusted Identity and Brand Reputation, A strong digital identity strategy can also help build confidence in a brand by showing that its owner does take safety and privacy seriously. This in turn creates both confidence and customer trust. On the flip side, nothing can cast a brand in ill-repute and erode consumer trust more than a data breach or a security lapse[70]. It is clear that consumers trust businesses that value consumer confidence and brand reputation, and those engaged in e-commerce must place a premium on their digital identity practices in order to instill trust in their consumers and stand out in an over-saturated market[71].

- Improving User Experience

Authentication methods like single sign-on (SSO) and biometric-based authentication allow users to login fast and without frictions. This just-in-time authentication approach reduces the friction with the user making the authentication about invisible[72]. A user who logs into SSO will be able to log into other services without needing to repeat this process multiple times. In the same way,

---

[69] Yuan, C., Moon, H., Wang, S., Yu, X., & Kim, K. H. (2021). Study on the influencing of B2B parasocial relationship on repeat purchase intention in the online purchasing environment: an empirical study of B2B E-commerce platform. *Industrial Marketing Management*, *92*, 101-110.

[70] Xiong, X., Yuan, F., Huang, M., Cao, M., & Xiong, X. (2020). Comparative evaluation of web page and label presentation for imported seafood products sold on Chinese e-commerce platform and molecular identification using DNA barcoding. *Journal of food protection*, *83*(2), 256-265.

[71] Sutinen, U. M., Saarijärvi, H., & Yrjölä, M. (2022). Shop at your own risk? Consumer activities in fashion e-commerce. *International Journal of Consumer Studies*, *46*(4), 1299-1318.

[72] Murdiana, R., & Hajaoui, Z. (2020). E-Commerce marketing strategies in industry 4.0. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *2*(1), 32-43.

biometric authentication (which includes fingerprint or facial recognition) allow users to verify their identity through a simple gesture or gaze, removing the need for passwords[73]. This fluid and password-free authentication experience also empowers users to take their contextual architecture from one platform to another, and from one device to the next. Not only does this add more profit centers for them, but also gives stronger base and relevant user experience. The services can be reached on any device from anywhere on the planet without compromising convenience or security[74].

2.5 Challenges and Risks Associated with Digital Identity

Digital identity is essential for e-commerce to work smoothly and securely — but it even has its specific challenges and risks that must be addressed for its efficient operation. These challenges and risks are security vulnerabilities, privacy issues, legal and regulatory barriers, technical constraints, and end-user problems[75].

That makes it essential for the secure operation of e-commerce, and the protection of our digital identity. But, it comes with its own shortcomings & threats that should be mitigated for a well-maintained running of the technology[76].

---

[73] Lucas, G. A., Lunardi, G. L., & Dolci, D. B. (2023). From e-commerce to m-commerce: An analysis of the user's experience with different access platforms. *Electronic Commerce Research and Applications*, *58*, 101240.

[74] Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. *GSC Advanced Research and Reviews*, *18*(3), 066-077.

[75] Khrais, L. T., Zorgui, M., & Aboalsamh, H. M. (2023). Harvesting the digital green: A deeper look at the sustainable revolution brought by next-generation IoT in E-Commerce. *Periodicals of Engineering and Natural Sciences*, *11*(6), 5-13.

[76] Kleisiari, C., Duquenne, M. N., & Vlontzos, G. (2021). E-Commerce in the Retail Chain Store Market: An Alternative or a Main Trend?. *Sustainability*, *13*(8), 4392.

Cybercriminals are increasingly looking at secured online identities as their main target as they can enable them to gain unauthorized access to confidential information. When this occurs, both businesses and consumers suffer from data breaches and financial losses[77]. Digital identities commonly include sensitive personal information, and so privacy is often a primary concern. This might lead to privacy violation and may hurt individual reputation[78].

Where digital identity management is concerned, businesses must consider an assortment of laws and regulations (specifically regarding data protection and privacy), all while navigating the legal and regulatory barriers that come with the territory. Moreover, there are legal repercussions for failing to comply, and it could risk a lot of lost brand equity[79].

Digital identity management is a type of non-functional requirement of identity and access management (IAM), which is the science of storing all information on one specific Identity and storing some of this Information on a platform. Factors that are entirely dependent on end users, such as password fatigue and mixed-signal over what sorts of authentication methods to use, can also affect the effectiveness of digital identity management. Some of these issues can be alleviated by educating the users on how to use the system properly as well as providing user-friendly

[77] Al Mashalah, H., Hassini, E., Gunasekaran, A., & Bhatt, D. (2022). The impact of digital transformation on supply chains through e-commerce: Literature review and a conceptual framework. *Transportation Research Part E: Logistics and Transportation Review*, *165*, 102837.

[78] Esmeli, R., Bader-El-Den, M., & Abdullahi, H. (2022). An analyses of the effect of using contextual and loyalty features on early purchase prediction of shoppers in e-commerce domain. *Journal of Business Research*, *147*, 420-434.

[79] Ballerini, J., Yahiaoui, D., Giovando, G., & Ferraris, A. (2024). E-commerce channel management on the manufacturers' side: ongoing debates and future research pathways. *Review of Managerial Science*, *18*(2), 413-447.

authentication methods[80]. In all, it is very important to deal with these challenges and risks for the better functioning of the digital identity occurs with e-commerce. These challenges can be solved by adopting stringent security controls, compliant to legal and regulatory requirements, and providing better user experience in the e-commerce space[81].

- Security Vulnerabilities

Digital Identity Theft & Fraud — As risky as it can be. The Point of Sale (POS) Shop provides a wide span of services for cybercriminals to assist with credit card fraud, to include providing the stolen identity to commit lucrative financial crimes, and unauthorized purchases, or to gain access to sensitive data or systems. It has caused lots of money to change hands, and created chaos in the reputation of affected companies and people as well[82].

Bigger yet are data breaches which compromises vulnerabilities in personal and financial details to undesired parties. On platforms, depending on, hackers are supposed to have major bank of databases for private people where all can be used for identity theft and other sinister purposes. For those affected, these breaches can mean financial losses, and in some cases, even identity theft along with legal consequences[83].

---

[80] Geng, R., Wang, S., Chen, X., Song, D., & Yu, J. (2020). Content marketing in e-commerce platforms in the internet celebrity economy. *Industrial Management & Data Systems*, *120*(3), 464-485.

[81] Ahmad, A. Y. B., Gongada, T. N., Shrivastava, G., Gabbi, R. S., Islam, S., & Nagaraju, K. (2023). E-commerce trend analysis and management for Industry 5.0 using user data analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(11s), 135-150.

[82] Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: a framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054.

[83] Bădîrcea, R. M., Manta, A. G., Florea, N. M., Popescu, J., Manta, F. L., & Puiu, S. (2021). E-commerce and the Factors Affecting its Development in the Age of Digital Technology: Empirical Evidence at EU–27 level. *Sustainability*, *14*(1), 101.

Digital identities are compromised through techniques such as malware and hacking. By abusing software susceptibilities, cybercriminals can plunge categories or ransomware inside systems and take command of real accounts, or else hijack disciplined data. Such attacks may lead to financial losses, data leaks and the impersonation of someone's digital identity[84].

To safeguard from identity theft, fraud, data breaches, malware and hacking in general, it's crucial to use secure authentication mechanisms, encryption, and good security updates. In addition, users can be notified or educated on basic cybersecurity measures to help reduce these risks and secure digital identities[85].

- Privacy Concerns

Privacy of data: — digital age works on freedom on the side and with its access user data collection and storage, and we know that keeping personal data cannot be a fingerprint. People are getting smarter and want businesses to keep their personal information out of the hands of the wrong people[86].

Digital identities, on the other hand, bring problems of surveillance and tracking as well. Digital identities facilitate easy access to services and tailored experiences, but they also enable tracking

[84] Feher, K. (2021). Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. *Journal of information science*, *47*(2), 192-205.

[85] Tofan, M., & Bostan, I. (2022). Some implications of the development of E-commerce on EU tax regulations. *Laws*, *11*(1), 13.

[86] Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, *8*(1), 104-110.

and user profiling. This can lead to invasive monitoring as well as unethical monetization of private data such as targeted ads or more[87].

To prevent these from happening, companies and other institutions should instigate tight data security, such as encryption and access controls, to safeguard personal data against privacy breaches. Transparency with respect to data collection and use practices is also critical to establish trust with users and to protect their privacy rights. Protecting data privacy, of course, does not end there — governments and regulatory bodies have laws and regulations to enact and enforce ensuring ultimate data privacy — personal data is critical to that matter[88].

- Regulatory Compliance

The regulatory environment surrounding e-commerce and data protection is intricate and ever-changing. That multijurisdictional compliance can be complicated and scary, and global e-commerce companies are not the only ones who have to do it[89].

Rules and regulations are updated to reflect current needs, are strict enough to enforce data protection laws and become requirements over time. Industries need to listen to this wakeup call, evolve and take charge of their digital Identity Management. Businesses need to know these

[87] Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673-1685.

[88] Sepashvili, E. (2020). Digital chain of contemporary global economy: e-commerce through e-banking and e-signature. *Economia Aziendale Online-*, *11*(3), 239-249.

[89] Chin, S. H., Lu, C., Ho, P. T., Shiao, Y. F., & Wu, T. J. (2021). Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things. *Computer Standards & Interfaces*, *76*, 103504.

changes and modify their best practices to stay compliant and secure consumer data. Non-compliance in any of these areas can lead to fines, papers, and a hit a company's reputation[90].

3. Creation of Digital Identity

3.1 Processes and Technologies for Digital Identity Creation

Creating a digital identity refers to making a unique, secure identity for people and things in the digital world using a set of processes and technologies. Registration: The first step - this is ofcourse the sign up, where users put their basic information about them like name, email, phone number, etc to start the creation of their digital identity. That core information is then used to make up their digital identity[91].

Authentication is a key phase in digital identity creation where a number of methods like passwords, biometrics, and two-factor authentication (2FA) including public and private key use come into play. These methods are used to guarantee that the identification of the people is valid during the registration and later interactions, making it possible to validate that the access to the digital identity is permitted only to who has authorized[92].

Data collection — one of the key pillars of a full-fledged digital identity. Apart from name, address and other basic information, users can collect more granular data like demographic information,

---

[90] Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395-410.

[91] Din, A. U., Han, H., Ariza-Montes, A., Vega-Muñoz, A., Raposo, A., & Mohapatra, S. (2022). The impact of COVID-19 on the food supply chain and the role of e-commerce for food purchasing. *Sustainability*, *14*(5), 3074.

[92] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

preferences, behavioral data, etc. This extra data significantly extends the digital identity, painting a broader picture of the user[93].

The tokenization process is not that simple, it is a mechanism to create a customer unique id to use in authentication or authorization purposes. This increases security and makes sure that every digital identity is separate and secure[94]. One of the newer uses for blockchain technology is to facilitate the use of decentralized identifiers (DIDs) for digital identities. This method allows digital identities to be established securely and tamper-proof, adding to the security and privacy[95]. Another important part of creating a digital identity is integration which means to integrate digital identity systems with other systems and services like CRM platforms and identity verification services. The integration will make it far more likely that Amazon security tools are consistent across all of the many different platforms and services that are coming into the AWS ecosystem.

3.2 Identity Proofing and Verification

During the on-boarding of a digital identity into an organization's system, identity proofing and verification play a vital role in ascertaining that the digital identity that just entered the system is real. Spring checks the hash by decoding the incoming JSON Web Token to read the signature used to test the hash along with the signed data to check the integrity of the token to test if the public key of the same signer calculates the hash from data in the token to verify. It ensures that

---

[93] Esmeli, R., Bader-El-Den, M., & Abdullahi, H. (2022). An analyses of the effect of using contextual and loyalty features on early purchase prediction of shoppers in e-commerce domain. *Journal of Business Research*, *147*, 420-434.

[94] Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.

[95] Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.

the party claiming the identity is exactly who they are and not an impostor or unauthorized person[96].

Verifying identity with document verification is as simple as it gets — after all, this is a standard method to confirm identity, where a user must simply upload photos of a document (for example passport or driver's licence). These documents are then verified against government databases or other reliable sources to make sure that they are real[97].

Another way of secured activation is to use biometric verification, which verifies user identity via unique biological traits like fingerprints or facial features. The above method is the highest secured method as the biometric traits are difficult to replicate or forge[98]. The user's knowledge of certain information like answers to security questions, personal details as in knowledge-based verification is usedto verify them. This is a powerful method, but it is susceptible to social engineering attacks if the information is too easy to guess or even easily accessible on the internet like user's phone number or mothers maiden name[99].

---

[96] Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825.

[97] Luo, N., Wang, Y., Zhang, M., Niu, T., & Tu, J. (2020). Integrating community and e-commerce to build a trusted online second-hand platform: Based on the perspective of social capital. *Technological Forecasting and Social Change*, *153*, 119913.

[98] Alsubari, S. N., Deshmukh, S. N., Al-Adhaileh, M. H., Alsaade, F. W., & Aldhyani, T. H. (2021). [Retracted] Development of Integrated Neural Network Model for Identification of Fake Reviews in E-Commerce Using Multidomain Datasets. *Applied Bionics and Biomechanics*, *2021*(1), 5522574.

[99] Kiba-Janiak, M., Marcinkowski, J., Jagoda, A., & Skowrońska, A. (2021). Sustainable last mile delivery on e-commerce market in cities from the perspective of various stakeholders. Literature review. *Sustainable Cities and Society*, *71*, 102984.

Two-factor authentication (2FA) is a security process that allows users to provide two different identification factors to validate themselves and secure their accounts. Adding this an additional security measure so if one type of identification gets hacked user's account will still remain secured[100]. In practice, these identity proofing & verification mechanisms serve to validate the creation of a digital identity, bridging the way forward for organizations to trust these identities and strengthen the fortitude against fraud with reduced access vulnerabilities[101].

3.3 Digital Identity Providers

Social ID Providers ecosystems provide services designed to help people and businesses create and control digital identities securely. One such service would be Identity as a Service, also known as IDaaS, which allows organizations to manage digital identities in the cloud. These typically have elements of enforcing some configured policies for Risk-Based Authentication and to give user management access, and provide a single stream-lined and secure way to handle identities across different platforms and services given the right integrations[102]. These providers also provide user-specific Identity Verification Services to ensure the safety of user identities Secure their identity using biometric and AI-powered technologies. Through verification of user identities via

[100] Vieira, J., Frade, R., Ascenso, R., Prates, I., & Martinho, F. (2020). Generation Z and key-factors on e-commerce: A study on the portuguese tourism sector. *Administrative Sciences*, *10*(4), 103.

[101] Svobodová, Z., & Rajchlová, J. (2020). Strategic behavior of e-commerce businesses in online industry of electronics from a customer perspective. *Administrative Sciences*, *10*(4), 78.

[102] Landim, A. R. D. B., Pereira, A. M., Vieira, T., de B. Costa, E., Moura, J. A. B., Wanick, V., & Bazaki, E. (2022). Chatbot design approaches for fashion E-commerce: an interdisciplinary review. *International Journal of Fashion Design, Technology and Education*, *15*(2), 200-210.

these services, fraudulent activities are curtailed with their use cases confined to masking fraud and aiding unauthorized access[103].

The Authentication Services are also a major area which could add benefit, bringing added security and UX developments. These services might be provided by single sign-on (SSO) and multi-factor authentication (MFA), and they help ensure that only people who are supposed to see sensitive data and systems are being allowed access[104].

Digital Wallet service Some Digital Identity Providers also offer a Digital Wallet service. It can integrate digital payment details and loyalty cards, making it easier and safer to create and use all online identities. In summary, these services are significant for assisting people as well as corporate organizations in keeping their digital identities in check by providing unique and personalised solutions that suit their different wants and needs[105].

3.4 Security Measures in Digital Identity Creation

A number of important security features exist in order to protect and maintain the integrity of user's digital identity. One of the basic security measures, is the encryption of information at rest or on transit (storage and in transit encryption) It helps to protect data by encrypting data so that only the authorized users can access it, also, minimizing the risk of unauthorized access and data

[103] Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.

[104] Jain, G., Kamble, S. S., Ndubisi, N. O., Shrivastava, A., Belhadi, A., & Venkatesh, M. (2022). Antecedents of Blockchain-Enabled E-commerce Platforms (BEEP) adoption by customers–A study of second-hand small and medium apparel retailers. *Journal of Business Research*, *149*, 576-588.

[105] Achmad, W. (2023). MSMEs Empowerment through Digital Innovation: The Key to Success of E-Commerce in Indonesia. *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 469-475.

breach[106]. Biometric and multi-factor authentication serve as strong authentication mechanisms ensuring an additional level of security making it harder for attackers to impersonate legitimate users[107].

Sensitive data must be protected with access controls. This access control measures help in allowing the right person to access the right data, thereby reducing the threat of data theft or unauthorized intrusion[108]. Detecting and responding accordingly to unauthorized activities or potential security incidents may only be possible when checking the systems properly, so regular auditing and monitoring are very important[109].

Monitoring systems to identify threats: Security teams can quickly detect and respond to threats, thus limiting the scope of data exposure. Meets standards that ensure data security and compliance with data user data protection laws like GDPR and CCPA. Organizations can follow these standards and save themselves from penalties related to user data[110]. Lastly, organization and

[106] Lee, C. S. (2022). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13-14), 2529-2553.

[107] Hongmei, Z. (2021). A cross-border e-commerce approach based on blockchain technology. *Mobile Information Systems*, *2021*, 1-10.

[108] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, *5*(2), 206-221.

[109] Wang, Y., Lu, Z., Cao, P., Chu, J., Wang, H., & Wattenhofer, R. (2022). How live streaming changes shopping decisions in E-commerce: A study of live streaming commerce. *Computer Supported Cooperative Work (CSCW)*, *31*(4), 701-729.

[110] Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.

implementation of such processes, technologies, and securities are critical to maintaining digital identity in a secure, usable way and to mitigate the risk of fraud and unauthorized access[111].

4. Digital Identity Lifecycle Management

4.1 Introduction to Digital Identity Lifecycle

A digital identity cycle is the various stages and practices that a digital identity must do from its beginning to the end which is deactivating or retiring it. Companies are required to orchestrate each point of this lifecycle in order to satisfy the trio of security, compliance and user experience requirements. This covers the methods, technologies, and standards that help a digital entity to create an identity, a way of sharing it, the attestation of it, and the life-cycle management of it[112]. The first stage in a digital identity lifecycle is creation where the user registers or onboarded into the system finding their resting place if it is for system use or public consumption. Collecting and verifying the user's real-world identity information to form their digital identity After digital identity is created, it enters its maintenance stage, keeping it up to date to be accurate and relevant. This phase can include updating personal details as well as any form of permissions linked in the digital identity[113].

---

[111] Yuan, C., Moon, H., Wang, S., Yu, X., & Kim, K. H. (2021). Study on the influencing of B2B parasocial relationship on repeat purchase intention in the online purchasing environment: an empirical study of B2B E-commerce platform. *Industrial Marketing Management*, *92*, 101-110.

[112] Xiong, X., Yuan, F., Huang, M., Cao, M., & Xiong, X. (2020). Comparative evaluation of web page and label presentation for imported seafood products sold on Chinese e-commerce platform and molecular identification using DNA barcoding. *Journal of food protection*, *83*(2), 256-265.

[113] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, *5*(2), 206-221.

The usage phase is when the digital identity is actively used by the user to interact with different systems, services, or applications. In this phase, industry veterans are responsible for carrying out authentication and verification procedures within such systems to ensure that access is secure while ensuring that the digital identity is not infringed upon. Ultimately, when a digital identity is no longer deemed necessary, or ceases to be valid, it goes to the deactivation or retirement phase[114]. Lifecycle Governance of a digital identity cannot be properly managed, it does not have security controls to protect against the common attacks, it does not follow on data privacy standards and regulation so on so forth Therefore, a company can mitigate security risks, follow regulations, and even improve user trust and satisfaction by efficiently managing the lifecycle of digital identities[115].

4.2 Stages of the Digital Identity Lifecycle

4.2.1 Registration

Detail: The account creation process is the process of the user inputting some basic information to open an account on the system and establish their credentials.

Steps: When users signed up, they entered standard details as part of a sign-up form — such as name, email, and password. Afterwards, an email verification may also be required to verify the

[114] Willemyns, I. (2020). Agreement forthcoming? A comparison of EU, US, and Chinese RTAs in times of plurilateral E-Commerce negotiations. *Journal of International Economic Law*, *23*(1), 221-244.

[115] Wang, Y., Lu, Z., Cao, P., Chu, J., Wang, H., & Wattenhofer, R. (2022). How live streaming changes shopping decisions in E-commerce: A study of live streaming commerce. *Computer Supported Cooperative Work (CSCW)*, *31*(4), 701-729.

email and turn on the account. The user is secured by basic authentication methods that prevent access to the user other than the authorized person[116].

Tech: User registration forms Email Confirmation (Check if the Email is of User) This endpoint is authenticated with Basic Authentication methods, like username and password to authenticate the user and secure the account[117].

4.2.2 Issuance

The Slot that the User identity assign in order to login and be identified on the system.

Method: This method enables users to authenticate themselves through the application of identifiers that uniquely identify individuals, i.e., user names or digital certificates[118].

Tech: These individualized units are created and controlled using: tokenization, blockchain identifiers and cryptography. Tokenization: Tokenization is the conversion of sensitive data to non sensitive “tokens” making the information safe to move around and store. Identity management with blockchain-based identifiers Cryptography — to make a set of procedures that prevent others from reading transmitted data (confidentiality) or altering them in their locker (integrity) — in other words, using cryptography to make sure that only the people involved in the transaction can understand the data at hand[119].

---

[116] Vieira, J., Frade, R., Ascenso, R., Prates, I., & Martinho, F. (2020). Generation Z and key-factors on e-commerce: A study on the portuguese tourism sector. *Administrative Sciences*, *10*(4), 103.

[117] Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: a framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054.

[118] Tofan, M., & Bostan, I. (2022). Some implications of the development of E-commerce on EU tax regulations. *Laws*, *11*(1), 13.

[119] Tammpuu, P., Masso, A., Ibrahimi, M., & Abaku, T. (2022). Estonian E-Residency And Conceptions Of Platformbased State-Individual Relationship. *Trames: A Journal of the Humanities & Social Sciences*, *26*(1).

4.2.3 Usage

Scope - Explores the step of the journey where the digital identity is leveraged for interaction with services & resources.

Scope: Interaction with Services and Resources using digital identity.

Process: According to this a user logs into any e-commerce site and initiates a transaction to avail the platform. That is done when those users utilize their digital identity credentials to establish new sessions and thus be able to access the platform services/resources[120].

Technologies — The technologies include the chosen authentication method to validate the user, access control mechanisms to control which resources a user can access, and system integration for the e-commerce platform to interact smoothly with the user[121].

4.2.4 Maintenance

Identity Management – this is how user keep digital identities up to date and accurate as time passes.

Workflow: Users can change their own particulars, reset their password, and handle their profile in self-service portals, or user account managers Notification Streams — They might be notified on these changes through notification streams[122].

---

[120] Svobodová, Z., & Rajchlová, J. (2020). Strategic behavior of e-commerce businesses in online industry of electronics from a customer perspective. *Administrative Sciences*, *10*(4), 78.

[121] Sutinen, U. M., Saarijärvi, H., & Yrjölä, M. (2022). Shop at your own risk? Consumer activities in fashion e-commerce. *International Journal of Consumer Studies*, *46*(4), 1299-1318.

[122] Sullivan, C. (2013). Digital identity, privacy and the right to identity in the United States of America. *Computer Law & Security Review*, *29*(4), 348-358.

Components: User account managers allow consumers to self-manage updates and changes. The obvious value that self-service portals add is allowing users to take care of their profiles on their own. Notification streams keep users posted on their digital identity updates / changes[123].

4.2.5 Deactivation and Termination

Deactivate/Delete Profile: This is the final stage to deactivate/delete a digital profile for easy identification and management.

Process: Users leave the services, request their accounts closed or frozen, or close them down by the services for being inactive or for security reasons. Users can also request deletion of their account, accounts may also be de-activated as a result of long term inactivity, or due to security concerns like suspected unauthorised access[124].

The process to close down these accounts is handled and implemented in the technologies, such as Account deactivation workflows. Globally, data also will be deleted, and all user data held in association with their account permanently deleted. Audit logs are kept to log the steps taken in the deactivation or deletion process for transparency and accountability[125].

4.3 Managing Digital Identities in E-Commerce

Identity Lifecycle Management Systems (ILM), enable the most seamless transition from one stage to the next to maintain the lifecycle of our digital identity. For example, these systems can

---

[123] Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.

[124] Sepashvili, E. (2020). Digital chain of contemporary global economy: e-commerce through e-banking and e-signature. *Economia Aziendale Online-*, *11*(3), 239-249.

[125] Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395-410.

automatically handle the process of adding or removing an account, in order to simplify identity management[126].

Integrating with e-commerce platforms is a prerequisite for easy and secure access. When implemented to the limit, Identity Management systems can provide best security and control over transactions made by users which also increase the user interaction safeguarding[127].

Digital Identities are one of the most important aspect of managing them, In case of compliance and security. Users need to be educated and identity management must follow compliance regulations and security best practices to prevent identity theft and theft[128].

It is in user education and awareness that the management of digital identities hinges. This will also help the people to understand the importance of handling the digital identity of the citizens and the risks of digital identity theft or fraud[129].

The Deployment Management API of Apigee provides a way for deploying and promoting proxies between environments in Apigee and helps in managing and organizing proxies in apigee. In

[126] Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. *GSC Advanced Research and Reviews*, *18*(3), 066-077.

[127] Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.

[128] Murdiana, R., & Hajaoui, Z. (2020). E-Commerce marketing strategies in industry 4.0. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *2*(1), 32-43.

[129] Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, *8*(1), 104-110.

conclusion, this method provides a way to manage the lifecycle of the customers to make sure they have secure access to services[130].

5. The eIDAS Regulation

5.1 Overview of the eIDAS Regulation

In the development of secure electronic transactions with the EU, the eIDAS Regulation is a fundamental EU regulation. It creates a legal basis for electronic authentication and trust services, and thus includes rules on electronic signatures, seals, time stamps, documents and registered delivery services. This framework strengthens reliability, security, and trustability of related illegal transactions in the same way as making faster cross-border transactions possible within the EU[131]. In place as of 2014 and mandatory since 2018, eIDAS outdates the previous Electronic Signature Directive. A key initiative here is the push for electronic identification (eID) schemes making it possible for people and businesses to use their electronic identities not only in their own country, but across all EU countries. The harmonisation helps to cut red-tape and to create a truly Digital

[130] Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing digital identity goals–the case study of Aadhaar in India. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18* (pp. 489-501). Springer International Publishing.

[131] Luo, N., Wang, Y., Zhang, M., Niu, T., & Tu, J. (2020). Integrating community and e-commerce to build a trusted online second-hand platform: Based on the perspective of social capital. *Technological Forecasting and Social Change*, *153*, 119913.

Single Market[132]. The eIDAS Regulation is sine qua non for supporting secure, efficient electronic transactions in the EU, fueling the digital drive and fostering trust in online services[133].

5.2 Key Provisions and Requirements

The eIDAS Regulation provides a wide-ranging structure for electronic trust services, defining them in a variety of senses. One of the key provisions electronic signatures, which the regulation divides into three types —simple, advanced, and qualified -with different juridical consequences. In terms of security and legal validity, a simple signature is an elementary electronic signature, which is what we a qualified electronic signature and an advanced electronic signature provide an advanced and the highest level of security[134].

Similar to electronic signatures, eIDAS also defined a new category, the electronic seals, which many businesses or organizations use to sign instead of the natural person. The regulation establishes a legal framework for the use of electronic seals and confirms the validity and reliability in using electronic seals in electronic transactions[135].

Electronic documents may also be time-stamped electronically to prove their integrity and authenticity, and eIDAS regulates this as well. Timestamps give proof that this file is present on this date and has not been changed since then or in this case modified after this date. The regulation

---

[132] Lucas, G. A., Lunardi, G. L., & Dolci, D. B. (2023). From e-commerce to m-commerce: An analysis of the user's experience with different access platforms. *Electronic Commerce Research and Applications*, *58*, 101240.

[133] Li, M., Shao, S., Ye, Q., Xu, G., & Huang, G. Q. (2020). Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. *Robotics and Computer-Integrated Manufacturing*, *65*, 101962.

[134] Li, H., Hu, Q., Zhao, G., & Li, B. (2022). The co-evolution of knowledge management and business model transformation in the post-COVID-19 era: insights based on Chinese e-commerce companies. *Journal of Knowledge Management*, *26*(5), 1113-1123.

[135] Lee, C. S. (2022). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13-14), 2529-2553.

establishes a regime of electronic time stamps in order to ensure the security and credibility of electronic documents[136].

Moreover, eIDAS lays down that documents in electronic form cannot be refused with legal effect or as evidence in legal proceedings due to the fact that they are in electronic form. This clause allows electronic documents to have the same legal status as those on paper and helps to promote e-documents used in legal transactions[137].

The regulation, finally, supports the use of eID throughout the EU, so that people and companies can use their national eID when using online services in another country of the EU. Such interoperability improves convenience and security when it comes to cross-border transactions and services and thereby reinforces the digital single market in the EU[138].

5.3 Impact of eIDAS on Digital Identity in E-Commerce

The eIDAS Regulation has completely changed digital identity management in e-commerce within the EU, bringing in some great improvements. Cross-border transactions have been one of its most significant impacts. One such move is the eIDAS, which has provided a legal foundation for

[136] Landim, A. R. D. B., Pereira, A. M., Vieira, T., de B. Costa, E., Moura, J. A. B., Wanick, V., & Bazaki, E. (2022). Chatbot design approaches for fashion E-commerce: an interdisciplinary review. *International Journal of Fashion Design, Technology and Education*, *15*(2), 200-210.

[137] Kleisiari, C., Duquenne, M. N., & Vlontzos, G. (2021). E-Commerce in the Retail Chain Store Market: An Alternative or a Main Trend?. *Sustainability*, *13*(8), 4392.

[138] Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673-1685.

electronic identification and trust services, making it easier for businesses and citizens to get into cross-border e-commerce activities and eliminating various barriers and administrative hassles[139]. In addition to this, security standards in e-commerce have been also improved by the regulation. This encourages the use of electronic signatures, seals, and time stamps to improve the integrity and reliability of electronic transactions. A proactive security measure taken to prevent such fraudulent activities makes it significantly low the risk of fraud and unauthorized access, making it more secure for all the stakeholders involved in the e-commerce[140].

eIDAS has been a game-changer for improving the experience of users. The regulation has enabled individuals and businesses to authenticate themselves when they use their national eIDs to access the cross-border online services in other EU countries. This makes for less of a headache where users have to maintain multiple accounts and passwords, meaning a more pleasant overloaded ecommerce experience for users[141].

Furthermore, adoption of a legal framework for electronic trust services played a role in the increase of trust in electronic transactions. For the e-commerce consumer, this produces a new level of trust in participating in transactions over the internet knowing that the consumer is protected by significant legal thresholds. This has established trust among businesses and

[139] Kiba-Janiak, M., Marcinkowski, J., Jagoda, A., & Skowrońska, A. (2021). Sustainable last mile delivery on e-commerce market in cities from the perspective of various stakeholders. Literature review. *Sustainable Cities and Society*, *71*, 102984.

[140] Khrais, L. T., Zorgui, M., & Aboalsamh, H. M. (2023). Harvesting the digital green: A deeper look at the sustainable revolution brought by next-generation IoT in E-Commerce. *Periodicals of Engineering and Natural Sciences*, *11*(6), 5-13.

[141] Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825.

consumers, fueling a rise in e-commerce in the EU that has been accompanied by growth and innovation[142]. The eIDAS Regulation completely revolutionized digital identity management in e-commerce in the EU making it possible to cross the borders, increasing security, boosting the user experience and creating trust in electronic transactions[143].

5.4 Comparison with Other International Standards

eIDAS is the most advanced and comprehensive regulation on electronic identification and trust services. However, it is not the only such international standard. In the U.S., the ESIGN Act is a legal framework for setting items up in a digital format, which includes eSignatures that are accepted for legal proceedings, while the UETA specifically addresses the enforceability of electronic signatures and records and their counterparts, but may have slightly different requirements or provisions than other national laws[144].

With this in mind, eIDAS stands alone in its goal to enable cross-border electronic transactions in the EU. This is a key differentiator because it is designed to promote frictionless electronic interaction across the EU in supporting economic & political integration across borders. EUwide interoperability & increased cross-border collaboration : A standardised framework offered by

[142] Jain, G., Kamble, S. S., Ndubisi, N. O., Shrivastava, A., Belhadi, A., & Venkatesh, M. (2022). Antecedents of Blockchain-Enabled E-commerce Platforms (BEEP) adoption by customers–A study of second-hand small and medium apparel retailers. *Journal of Business Research*, *149*, 576-588.

[143] Hongmei, Z. (2021). A cross-border e-commerce approach based on blockchain technology. *Mobile Information Systems*, *2021*, 1-10.

[144] Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. *computers*, *9*(3), 66.

eIDAS that ensures the acceptance and recognition of electronic identification and trust services across all states in the EU[145].

Moreover, eIDAS highlights security and reliability of electronic transactions in a great deal. This is evident from its exhaustive provisions for electronic signatures, seals and time-stamping mechanisms formulated to guarantee the provenance and trustworthiness of electronic interactions. This: the necessary strict rules on security under the regulation decrease the risks related to electronic operations like fraud or an unauthorized person using the payment and therefore increases the trust between the parties to the transactions[146].

In short, other international standards such as the ESIGN Act and UETA are legislation specific to electronic transactions, The unique point about eIDAS is its focus on cross-border and the security mechanism associated with it. This makes of eIDAS a ground-breaking law in the field of electronic identification and trust services there is nothing of the kind[147].

6. National Laws

6. 1. National Legislation on Digital Identity

Digital identity is a maturing field and is subject to a range of legislation in many countries. Some key examples include:

[145] Geng, R., Wang, S., Chen, X., Song, D., & Yu, J. (2020). Content marketing in e-commerce platforms in the internet celebrity economy. *Industrial Management & Data Systems*, *120*(3), 464-485.

[146] Feher, K. (2021). Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. *Journal of information science*, *47*(2), 192-205.

[147] Esmeli, R., Bader-El-Den, M., & Abdullahi, H. (2022). An analyses of the effect of using contextual and loyalty features on early purchase prediction of shoppers in e-commerce domain. *Journal of Business Research*, *147*, 420-434.

6.1.1 United States

ESIGN (Electronic Signatures in Global and National Commerce)–Makes it legal electronic signatures for interstate and international organizations. ESIGN enables the use of electronic signatures by providing a legal framework to the process, thereby allowing transactions to be conducted digitally, which means businesses and individuals do not have to rely on paper and other manual processes. The adoption and implementation of electronic signatures in the United States was largely popularized by this act and years later has continued to serve as a foundation for the passing of established digital transaction laws globally.

Uniform Electronic Transactions Act (UETA): Most states in the U.S. have adopted this act which gives legal status to electronic signatures and documents. UETA will make a difference to both type of commerce (eCommerce and digital business practices) by assuring the legal equivalence of electronic and paper based methods of commerce. UETA standardizes the legal framework for electronic transactions on a state level, thus providing a base of uniform rules and consistent and clear expectations of conduct for businesses and customers participating in e-commerce across multiple states.

Together the UETA and ESIGN Act lay the necessary legal bedrock for the acceptance of electronic signatures and records across the United States, facilitating seamless secure electronic transactions in both domestic and international commercial transactions.

6.1.2 Canada

Personal Information Protection and Electronic Documents Act (PIPEDA): Clarifies how private-sector organizations may collect, use and disclose personal information in the course of commercial activities. PIPEDA guarantees that companies handle personal information responsibly and with respect for privacy rights. It is what dictates the principles of fair information

practices that organizations must comply with to put the individual back in control of their own personal data, and demand transparency into how that data gets used[148].

Digital Privacy Act: An act which amended PIPEDA to introduce breach notification and a new security safeguards standard. The proposed amendments ask organizations to alert the OPC and victims, in the event of a successful breach of security safeguards involving personal information and a real risk of significant harm. It also requires companies to document all data breaches and take every care to ensure the protection of personal information. The Digital Privacy Act enhances the safeguards for personal information in Canada by requiring accountability and transparency when breaches do occur[149].

PIPEDA and the Digital Privacy Act together establish a comprehensive law for the safeguarding of personal data for Canadian businesses in the private sector and ensure that these businesses meet high standards of privacy and security when handling data[150].

6.1.3 European Union

eIDAS Regulation(eIDAS): As covered, eIDAS is a regulation which deals with electronic identification and trust services for electronic transactions in the European Union. It is intended to enable secure electronic signatures and transactions in the EU by establishing a legal model for

---

[148] Din, A. U., Han, H., Ariza-Montes, A., Vega-Muñoz, A., Raposo, A., & Mohapatra, S. (2022). The impact of COVID-19 on the food supply chain and the role of e-commerce for food purchasing. *Sustainability*, *14*(5), 3074.

[149] de Andrade, N. N. G. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, *28*(2), 153-162.

[150] Chin, S. H., Lu, C., Ho, P. T., Shiao, Y. F., & Wu, T. J. (2021). Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things. *Computer Standards & Interfaces*, *76*, 103504.

electronic identification (e-ID) and trust services across the EU. eIDAS allows for the usage of electronic signatures, just as digital signatures and time stamps — ensuring the legitimacy and truthfulness of electronic transactions; thereby aiding greater cross-border e-commerce within the EU community[151].

GDPR (General Data Protection Regulation): It is more of a widespread data protection regulation, but has sections which pertain to control over digital identity management, as well. GDPR is designed to protect data and privacy for all individuals within the EU and the EEA. There are strict conditions for the collection, handling, storage of personal data and individuals will retain the control of his personal data. The GDPR principles of data minimization (GDPR Article 5(1)(c)), purpose limitation (GDPR Article 5(1)(b)) and data security (GDPR Article 7/32) lay the key foundations for digital identity management practice, ensuring that personal data linked to digital identities is processed in a secure and transparent manner[152].

Both have built a solid legal basis for digital identity management in the EU, eIDAS focusing on electronic identification and trust services and GDPR securing the broader protection of personal data and privacy rights[153].

---

[151] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

[152] Boysen, A. (2021). Decentralized, self-sovereign, consortium: The future of digital identity in canada. *Frontiers in Blockchain*, *4*, 624258.

[153] Ballerini, J., Yahiaoui, D., Giovando, G., & Ferraris, A. (2024). E-commerce channel management on the manufacturers' side: ongoing debates and future research pathways. *Review of Managerial Science*, *18*(2), 413-447.

6.1.4 Other Key Countries

The Electronic Transactions Act 1999 (Cth) which establishes a regime for electronic transactions and the application of electronic signatures as evidence. The Act helps in electronic communication in various businesses and government transactions which approved the legality of the electronic signatures to be used for signing contracts, agreements and much more. This Act facilitates the wider use of e-commerce and digital identity usage as there will be already a legal structure for electronic transactions[154].

Japan : In Japan, the use of electronic signatures and certification services is regulated by the Act on Electronic Signatures and Certification Services. The Act of Electronic Signatures, which is the legal framework of the recognition and use of electronic signatures, its validity, in electronic transactions. It also regulates certification service providers to guarantee that electronic signatures are used securely and effectively in a wide array of applications in government, commerce and personal transactions[155].

eCourts Services in India: First is the Information Technology Act, 2000 which gives recognition to electronic records and digital signatures in India. This Act allows the act of electronic communication, and it is related to eCourts services in the judicial system. The Act enables the government to enable and enforce the validity of digital signatures and electronic records, thereby eliminating the need for paperwork with traditional ones This new addition is by no doubt an

[154] Bădîrcea, R. M., Manta, A. G., Florea, N. M., Popescu, J., Manta, F. L., & Puiu, S. (2021). E-commerce and the Factors Affecting its Development in the Age of Digital Technology: Empirical Evidence at EU–27 level. *Sustainability*, *14*(1), 101.

[155] Alsubari, S. N., Deshmukh, S. N., Al-Adhaileh, M. H., Alsaade, F. W., & Aldhyani, T. H. (2021). [Retracted] Development of Integrated Neural Network Model for Identification of Fake Reviews in E-Commerce Using Multidomain Datasets. *Applied Bionics and Biomechanics*, *2021*(1), 5522574.

effective enabler for the current government to drive judicial systems and other services devoid of paper[156].

6.2 Harmonization and Consistency of National Laws

National diversity in legal systems, cultural norms, and national capacity means all laws related to digital identity are unlikely ever to be harmonised around the world. This is an issue that can produce legal contradictions, where not only are certain laws unenforceable at the same time, but they are a contradiction on a basic level. Efforts are being made for the digital identity to have uniform because they exclude a combined legal and standard framework[157].

With all this being said, the European Union (EU) and the legal frameworks of the EU, and especially the eIDAs Regulation, are good examples that illustrate how harmonization can be successful when facing extreme adversities. The eIDAS Regulation is the cornerstone for the provision of secure, trusted and easy to use electronic identification and trust services in the EU. Global harmonization at this level, however, would have to be reconciled with different legal and regulatory environments[158].

Cultivating such a legal system to exist in a more continuous manner and be more global surrounding the issue of digital identity would be an exercise in reconciling these differences and finding solidarity. This process had to take into account the differences in technological

---

[156] Al Mashalah, H., Hassini, E., Gunasekaran, A., & Bhatt, D. (2022). The impact of digital transformation on supply chains through e-commerce: Literature review and a conceptual framework. *Transportation Research Part E: Logistics and Transportation Review*, *165*, 102837.

[157] Ahmad, A. Y. B., Gongada, T. N., Shrivastava, G., Gabbi, R. S., Islam, S., & Nagaraju, K. (2023). E-commerce trend analysis and management for Industry 5.0 using user data analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(11s), 135-150.

[158] Achmad, W. (2023). MSMEs Empowerment through Digital Innovation: The Key to Success of E-Commerce in Indonesia. *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 469-475.

development, legal traditions and culture in the attitudes of users in terms of privacy and security. This harmonization would be challenging to achieve and tedious to implement, but could increase the security, user trust, and interoperability of global digital identity systems allowing for streamlined and safer global digital interactions[159].

[159] Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.

CHAPTER THREE

3. Introduction

The European Digital Identity Regulation, Regulation (EU) 2024/1183, popularly known as eIDAS 2.0, will offer a series of strong requirements and take steps to fulfill the vision of a European Digital Identity Framework that began with the creation of eIDAS 1.0. The regulation published in the Official Journal of the European Union on 30 April 2024 and entering into force on 20 May 2024 would require EU Member States to make the EU Digital Identity Wallet available to their citizens within 24 months of the adoption of Implementing Acts to be introduced. These acts will define the technical requirements and the certification modes and the European Commission is due to author an implementation decision containing a list of reference standards and specifications by November 21, 2024 (Article 5a).

This regulation modifies Regulation (EU) 910/2014 (eIDAS Regulation) to take into account the growing digitalisation of society that has been rapidly progressed following the COVID-19 pandemic. All EU citizens, residents, and businesses will benefit from the European Digital Identity with the possibility to use it to access services, easily and privately, online and offline anywhere in the EU.

Before Regulation (EU) 2024/1183, digital identification systems of the EU countries were hamstrung by a host of problems such as limited access to the entire public due to online public service restrictions and difficulty in accessing services cross-border. By providing citizens with the possibility to verify their identity, authenticate documents and confirm attributes (e.g. age), offering full control over their data, the EU Digital Identity Wallets brought a definitive solution to these flaws. Delivering new opportunities for Europeans to benefit from the full range of digital

services available elsewhere in the world, this upgraded systembodes well forintroducing much-needed e-management convenience, support, and cross-E.U. interoperability.

3.1 Research Methodology

The research strategy was a case study method with national digital-identity e-commerce legislation in four regions: The United States., Canada, The European Union, And the Rest of the Key National Legislation Across four Provinces / Region as follows. The purpose is to delve in deep into the distinction in legislative framework, the way it is applied on ground and how it affects digital identity onboarded in the e-commerce domain.

3.2 Qualitative Approach

To delve into the richness and intricacy of the types of national laws for digital identity in e-commerce, we adopt a qualitative methodical approach in this research. This provides a useful insight into the mechanics of the law and its practical applications.

3.3 Case Study Analysis

Case study analysis is employed to offer a full screen to digital identity legislation in the four regions. This approach is appropriate when considering the particularities of the legal system of each territory.

3.4 Data Collection

Academic journals, government publications, legal documents, and industry reports will provide secondary data. This data will help in getting a basic idea of the legislative environment and background of the issue.

CHAPTER FOUR

4. Data Analysis

4.1 Comparative Analysis

A comparative analysis will be conducted to highlight similarities and differences between the legislative frameworks of the four regions. This will involve comparing key aspects such as regulatory scope, enforcement mechanisms, and compliance requirements.

4.2 Case Studies

4.2.1 United States

A case study of the United States will include federal and state laws regarding digital identity, such as the E-SIGN Act and NIST guidelines.

4.2.2 Canada

The Canadian case study will foreground the Personal Information Protection and Electronic Documents Act (PIPEDA) and other relevant provincial laws It will also take a look at rising initiatives such as the Pan-Canadian Trust Framework.

4.2.3 European Countries

The EU case will involve analysis of the General Data Protection Regulation (GDPR) and the eIDAS Regulation. It will evaluate how well these regulations coordinate digital identity standards within the member states.

4.2.4 Other Key Countries

The next case study will delve into other leading countries that have strong digital identity systems such as Australia, Japan, and South Korea. This will concentrate instead at their laws and agreements made internationally.

4.3 Case Analysis

It features different case studies covering several facets of the digital identity in the e-commerce domain across countries such as the United States of America, Canada, European Countries, and many more. For example, in the United States, Sullivan[160] charts the rise of digital identity as a legal issue, partly in response to federal government services going online. From the legal dimension of digital identity to vulnerabilities and possible implications for individuals. This study highlights the need for strong legislation to protect online identities.

Meanwhile, Boysen[161] sets sights on the digital identity lands of tomorrow in the snows of Canada, through the creation of a decentralized, blockchain-based self-sovereign identity (SSI) network,

[160] Sullivan, C. (2013). Digital identity, privacy and the right to identity in the United States of America. *Computer Law & Security Review*, *29*(4), 348-358.

[161] Boysen, A. (2021). Decentralized, self-sovereign, consortium: The future of digital identity in canada. *Frontiers in Blockchain*, *4*, 624258.

built to get them all. The findings of this study provide insights into the value proposition of SSI and its relevance in the context of Canada's digital identity ecosystem.

De Andrade[162] stated the perspective to the field of electronic identity (eID) with a feasibility study on European eID legal action after the Treaty of Lisbon. The report explores legal competences and possible legal foundations of a European system of an electronic identity such as the importance of a secure EU-eID, which is convenient and user-friendly.

Turning to India, Mir[163] focus on the Aadhaar digital identity initiative and its role in providing access to essential services. They draw out the objectives of Aadhaar — uniqueness, privacy, and security — and the challenges and (so far, positive) lessons stemming from the Aadhaar exercise, as they apply to future digital identity initiatives in India and globally.

Finally, in Estonia, Tammpuu[164] stated Algorhythmic governance of the e-residency in altos. This paper considered how one form of transnational belonging, e-residency, mediates state membership, through an analysis of e-residency in which digital identity is integral to new meanings of citizenship, governances, etc.

---

[162] de Andrade, N. N. G. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, *28*(2), 153-162.

[163] Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing digital identity goals–the case study of Aadhaar in India. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18* (pp. 489-501). Springer International Publishing.

[164] Tammpuu, P., Masso, A., Ibrahimi, M., & Abaku, T. (2022). Estonian E-Residency And Conceptions Of Platformbased State-Individual Relationship. *Trames: A Journal of the Humanities & Social Sciences*, *26*(1).

Both case studies offer unique perspectives on the complex architecture that digital identity presents to e-commerce, and include important lessons and recommendations for policymakers, suppliers, and consumers everywhere.

First case study was conducted about united states of America, based on the transition of federal government services to the web, digital identity comes into focus as a legal concept in the US. This first analysis explores the different characteristics and functions of digital identity as well as related legal implications, examining the ways in which digital identity may be utilised, but also exploited, especially in relation to transactions.

The big reveal is that the nominative linking the digital identity registered with a private sector service provider and the individual behind that cloud of family data is a very vulnerable data point. However, despite the breach, all transactions made from the digital identity are automatically attributed to the registered individual, even if they did not make that transaction. This kind of mismatch can be extremely bad even for the genuinely innocent people, and the integrity of the scheme is also put in question.

In the US, privacy has been the home of personal data protection, in both legal scholarship and jurisprudence. The article, however, contends that privacy is not enough to preserve the transaction part of digital identity because of its fundamentally public nature. This does not mean that the kind of protection one might be after under this scheme can be supplanted by the right to identity in the United States; rather, the author advises that acknowledging such a thing as right to identity in the United States may afford a more stable form of comprehensive protection for individuals under this scheme, given its reality of built-in vulnerabilities.

At the end, Sullivan's study highlights the intricacies and problems associated with the landscape of digital identity in the US, shedding light on the requirement for a sophisticated legal framework dealing specifically with digital identity to proficiently support people's rights.

Furthermore, A case study from Canada by Boysen [165]examines the digital identity landscape in Canada by looking at its potential future against the backdrop of a self-sovereign identity (SSI) network built on blockchain technology created by SecureKey Technologies Inc. The research highlights how SecureKey worked with a variety of business and government stakeholders as well as consumers to develop an open, decentralized, self-sovereign, consortium model for digital identity.

This stands in stark contrast to the present centralized digital identity model that revolves around fragmented identities siloed within specific online properties, the article says. SSI principles provide users complete control and ownership of their digital identity attributes by using the blockchain as a secure base that allows any misuse or publication of their information.

The case of Verified which is one of the main features of this study It is a fully open-source project, built using SSI principles and in collaboration with blockchain technology. Me — digital identity platform This platform is a showcase of how developers can apply blockchain technologies to not only solve the problems in the current identity silos market but also plays a part to connect all the industry players into a trusted identity network. This paper concludes with a discussion of the practical implications of the results and considerations for future implementations of SSI using

[165] Boysen, A. (2021). Decentralized, self-sovereign, consortium: The future of digital identity in canada. *Frontiers in Blockchain*, *4*, 624258.

blockchain, and offers recommendations for wider adoption of decentralized identity initiatives in the Canadian and global landscape.

With the case study of Boysen, we conclude that SSI with blockchain has the power to transform the digital ID sector and that it outlines that collaboration, creativity and user-centric identity solutions are so much needed.

Moreover, a case study from India by Mir[166] case study, focusing on the Aadhaar digital identity program in India and its relevance in the context of the Fourth Industrial Revolution. In doing so, the study emphasizes the role and utility of digital identity in getting access to critical services such as voting, education, getting a job, insurances, and health. Although identity is critical, about 1 billion people around the globe are without establishing records, which disproportionately affects rural populations, women, children and poorer families.

United Nations' Sustainable Development Goal 16 highlights the importance of ensuring that every person has a legal identity by 2030. Aadhaar is an important step in that direction as it is a massive identity, that the government has created. But creating a national identity scheme is what authors Nick Dowson, Geraint Price and Akintunde Popoola refer to as a 'complicated and expensive process', demanding 'significant budgets, time and domain expertise.

[166] Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing digital identity goals–the case study of Aadhaar in India. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18* (pp. 489-501). Springer International Publishing.

It is a qualitative study which attempts to identify as well as rank the most overarching goals of Aadhaar through use of focus group discussions towards data collection and secondary data for triangulation. Uniqueness, privacy and security are the most important goals, while scalability and future-proofing of technology is of least importance. The importance of each of these goals is identified using Total Interpretive Structural Modeling (TISM). This type of analysis would be a useful reference for other countries who are thinking of launching a similar biometric identity program for their citizens. It illustrates the inevitability of digital identity in today's world and offers lessons on what these programs intended to, albeit principally on facets of privacy, security, and scalability.

A case study about European countries by de Andrade, this case study discusses the eID regulation of the European Union (EU) after the launch of the Treaty of Lisboa. It essentially researches the possibility of EU action in the field of eID, looking at the division of legal competences between EU institutions and the fresh legal basis established by the Treaty of Lisbon. This project will determine “the legal anchor” for the concept of a pan-European electronic identity in EU law and examine competences and legal basis issues that are associated with this. Identifying the different competences that potentially may be used to as a legal basis for a framework for regulation of eID at an EU level, the study discusses several suggested candidates as well as a number of different criteria, and comes to the conclusion that a combination of different appropriate treaty articles should serve as the foundation for eID regulation within the EU.

This research uses legal analysis methodologically. To establish the legal competences and basis for eID regulation within the EU framework the thesis examines the Treaty of Lisbon and relevant EU treaties The research, among other things, examines areas of competence and potential legal bases for European eID regulation.

The study's conclusions lead to identify a cluster of EU treaty articles as the most appropriate legal basis for eID regulation in the EU. It makes the case for a basis in Article 16 TFEU — right to the protection of personal data. In addition, the study recommends, the "Article 3 of the Treaty on European Union (TEU) and Articles 26 and 114 of the Treaty on the Functioning of the European Union (TFEU) that deal with the establishment and the functioning of the Internal Market should be included". Together, these articles provide a broad legal foundation for pursuing regulation of eID in the EU. This conclusion highlights the need for a specific EU FinReg for eID which due to TTOL needs a clear legal basis, therefore an EU FinReg concerning eID must be found on this new basis. By finding the appropriate legal basis and competences as regards eID regulation, the EU can trigger the development of a harmonized and secure eID framework, helping to boost trust and interoperability in the digital single market.

Lastly, a case study by Tammpuu[167], the theoretical grounding of this state-individual relationship is deepened through an investigation of platform-based state-individual relationships, with a case study on the e-residency program course of Estonia. This initiative by the government here enables non-residents to apply for a digital ID card issued by the state which gives them complete control over public information and private services throughout e-Estonia. Drawing on phantomization as a lens, the paper discusses how HWWS shapes ideas about the individual-state relationship.

Using qualitative interviews with a sample of e-residents holding a digital ID, the study explores the discourses constructed by e-residents about the meaning of e-residency in their relationship with the state. Beyond the provision of transaction-based functions, e-residency is a discovery of a community membership that transcends the state and thus lays a move towards a form of

[167] Tammpuu, P., Masso, A., Ibrahimi, M., & Abaku, T. (2022). Estonian E-Residency And Conceptions Of Platformbased State-Individual Relationship. *Trames: A Journal of the Humanities & Social Sciences*, *26*(1).

transnational reconsignment through technical means. Nikolic argues that this view describes the digital state not as a platform manager and service provider, but as a membership organization that operationalizes its rules of inclusion in digital ID schemes.

4.4 Comparative Analysis of Digital Identity in E-Commerce

4.4.1 Similarities

1. Focus on Digital Identity: All case studies center around digital identity, exploring its various aspects such as privacy, security, and legal implications.
2. Legal and Regulatory Context: Each case study discusses the legal and regulatory frameworks surrounding digital identity, highlighting the need for appropriate laws and regulations to govern these systems.
3. Implications for Individuals: The studies consider the impact of digital identity on individuals, discussing issues such as rights, responsibilities, and the potential for exploitation or misuse.
4. Technology and Innovation: The case studies highlight the role of technology, such as blockchain, in reshaping digital identity systems and promoting self-sovereignty.
5. Global Relevance: While each study focuses on a specific country or region, they all touch on global themes and implications, highlighting the universal challenges and opportunities presented by digital identity.

4.4.2 Differences

1. Geographical Focus: Each case study examines digital identity within a specific geographical context, leading to different regulatory frameworks and approaches.

2. Technological Solutions: The studies differ in their emphasis on technological solutions, with some focusing more on blockchain and others on biometric systems like Aadhaar.

3. Legal Analysis: The European Union case study delves into legal analysis, discussing the specific treaty articles that could serve as a legal basis for eID regulation, which is not as prominent in the other case studies.

4. Focus on Citizenship: The Estonia case study uniquely focuses on the concept of citizenship and belonging, exploring how e-residency can transcend traditional notions of state membership.

Overall, while the case studies share common themes and concerns regarding digital identity, they also reflect the diverse approaches and contexts in which these systems are developed and implemented.

4.3 Use Cases and Benefits of Digital Identity Verification in E-Commerce

4.3.1 Use Cases of Digital Identity Verification

Digital Identity verification is the bedrock of secure e-commerce transactions it builds trust and security in numerous situations:

4.3.1.1 Online Shopping

In online shopping, this helps with Identity verification which verifies that the person making a purchase, is in fact, the authentic cardholder which drastically reduces fraud. Businesses can prevent fraudulent activities by confirming the identity of the user which can be done with several verification methods such as biometrics, two-factor authentication (2FA), knowledge-based

questions and more[168]. By assisting in tightening the security of online transactions, it will also promote confidence and trust among consumers which will further attract prospective persons to participate in e-commerce without any fear of identity theft or fraud[169].

4.3.1.2 Digital Banking

For identifying users who use online banking services through digital banking to limit unauthorised access and protect confidential financial data, digital banking uses identity verification heavily. The direct and indirect investments made on online banking platforms call for secure identity verification processes to prevent unauthorized transactions by illegitimate account holders[170]. By using enhanced verification methods, including multi-factor authentication, biometric scans and secure token systems, banking institutions are able to prevent their customers' financial information from falling into the wrong hands - and keep their online services safe and sound. This will not only strengthen the security of financial operations but will also instill trust and confidence in clients and will push them towards a wider use of digital banking services[171].

---

[168] Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.

[169] Yuan, C., Moon, H., Wang, S., Yu, X., & Kim, K. H. (2021). Study on the influencing of B2B parasocial relationship on repeat purchase intention in the online purchasing environment: an empirical study of B2B E-commerce platform. *Industrial Marketing Management*, *92*, 101-110.

[170] Xiong, X., Yuan, F., Huang, M., Cao, M., & Xiong, X. (2020). Comparative evaluation of web page and label presentation for imported seafood products sold on Chinese e-commerce platform and molecular identification using DNA barcoding. *Journal of food protection*, *83*(2), 256-265.

[171] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, *5*(2), 206-221.

4.3.1.3 Online Services and Subscriptions

As a verification flow becomes an ID-powered service, it moves up the user verification stack toward identification, limiting access to paid content or services to legitimate users (people). This includes checking the identity of the user through means like a password, facial recognition, or two-factor authentication able to confirm that the person in question is the person they say they are[172]. Through strict identification procedures, only legitimate rights holders can access premium content or services and protect their intellectual property and revenue streams. It helps improves the platform, making it more secure all while ensures a seamless and trustworthy user experience which in turn would lead to more users subscribing to the platform with confidence to avail paid services as well[173].

4.3.1.4 Age Verification and Access Control

Age restrictions as is the case for alcoohol sale, gambling access, etc… have greatly benefitted from digital identity verification, when digital id is associated a person's legal age. With secure methods of verifying the users age such as date of birth verification, age verification scanning, and age verification services, businesses are able to ensure that minors are not gaining access to services which is otherwise meant to be restricted[174]. This not only supports to comply with

---

[172] Willemyns, I. (2020). Agreement forthcoming? A comparison of EU, US, and Chinese RTAs in times of plurilateral E-Commerce negotiations. *Journal of International Economic Law*, *23*(1), 221-244.

[173] Wang, Y., Lu, Z., Cao, P., Chu, J., Wang, H., & Wattenhofer, R. (2022). How live streaming changes shopping decisions in E-commerce: A study of live streaming commerce. *Computer Supported Cooperative Work (CSCW)*, *31*(4), 701-729.

[174] Vieira, J., Frade, R., Ascenso, R., Prates, I., & Martinho, F. (2020). Generation Z and key-factors on e-commerce: A study on the portuguese tourism sector. *Administrative Sciences*, *10*(4), 103.

governmental regulations but also protects the children from dangerous practices. Age verification measures that are this robust also show a commitment to responsible business practice and can help to earn good favour with both customers and the regulators[175].

4.3.2 Benefits of Digital Identity Verification

4.3.2.1 Enhanced Security

Integration of identity verification features enable businesses to authenticate the identity of their users and minimize the risk of unauthorized access or fraud. They might confirm the identity of folks with the use of two-factor authentication, biometric verification or sometimes that bit of authentication directly into the body. And not only protect the business but also protect the data or assets of their customers[176]. Having robust identity verification mechanisms in place show positive sign for the security and reliability, which builds trust among customers which leads to a good brand value and increasing loyalty of the customer[177].

4.3.2.2 Improved Customer Experience

ID verification is an essential service offering that can not only streamline the customer journey but also simplify the steps the customer takes to obtain a product or service. This allows businesses to ensure that customers can quickly access their accounts or make purchases without being

[175] Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: a framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054.

[176] Tofan, M., & Bostan, I. (2022). Some implications of the development of E-commerce on EU tax regulations. *Laws*, *11*(1), 13.

[177] Tammpuu, P., Masso, A., Ibrahimi, M., & Abaku, T. (2022). Estonian E-Residency And Conceptions Of Platformbased State-Individual Relationship. *Trames: A Journal of the Humanities & Social Sciences*, *26*(1).

encumbered by cumbersome barriers of security[178], and implementing uniformity and convenience in the form of biometric authentication or token-based verification. Implementing this results in a better customer experience and also makes it more secure by making sure the user is who they say they are. This, in turn, makes customers more likely to interact with the business, stay loyal, which will increase customer satisfaction and retention[179].

4.3.2.3 Reduced Fraud and Identity Theft

The detection of fraud is a common use case for many businesses who want to reduce their chances of being subjected to identity theft or other types of fraud. Attackers often exploit weaknesses in these systems, but businesses can combat that by implementing robust fraud detection solutions, like monitoring for unusual account activity[180], verifying that users are who they say they are, and using advanced analytics to detect anomalous patterns in user behavior. This preemptive action additionally serves to reduce financial loss and sustain the business reputation and the consumer confidence. By monitoring fraud detection strategies and changing rapidly, businesses can outpace newly-emerging threats and create a safe operating environment[181].

---

[178] Svobodová, Z., & Rajchlová, J. (2020). Strategic behavior of e-commerce businesses in online industry of electronics from a customer perspective. *Administrative Sciences*, *10*(4), 78.

[179] Sutinen, U. M., Saarijärvi, H., & Yrjölä, M. (2022). Shop at your own risk? Consumer activities in fashion e-commerce. *International Journal of Consumer Studies*, *46*(4), 1299-1318.

[180] Sullivan, C. (2013). Digital identity, privacy and the right to identity in the United States of America. *Computer Law & Security Review*, *29*(4), 348-358.

[181] Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.

4.3.3 Challenges and Best Practices

User data security and privacy: Data Security and Privacy are the biggest challenge for digital identity verification. User data must appropriately secure to prevent unauthorized access or data breaches, so organizations should enforce encryption, secure storage, and access controls. On top of that, they need to follow the privacy laws and regulations to ensure the users data is well taken care of[182].

It covers Compliance — meeting the requirements of different regulatory and standards (GDPR, PCI DSS) which is another headache. Identity verification is necessary for organizations, because it creates a legal responsibility on them to secure the data of their users from fraud. Non-compliance of these regulations is punishable by an extensive fine and also a damaging of the organizations public image[183].

Scalability and Interoperability: As enterprises grow and transact more, they require identity service solutions that scale as per demand. Moreover, these solutions should be easy to integrate with existing legacy business systems, — so business runs without a glitch. It means we need to ensure scalability and interoperability which are less likely since it needs the investment of technology infrastructure[184].

---

[182] Sepashvili, E. (2020). Digital chain of contemporary global economy: e-commerce through e-banking and e-signature. *Economia Aziendale Online-*, *11*(3), 239-249.

[183] Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395-410.

[184] Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. *GSC Advanced Research and Reviews*, *18*(3), 066-077.

Best Practices:

1. Enforcement of Strong Authentication:One of the steps to make customer verification power up is to mandate the real-time implementation of multi-factor authentication (MFA) Before letting users access their account MFA demands more than two factors of authentication that make it harder for unauthorized users to gain access to an account[185].

2. Implement Routine Security Patches — Security patches and updates are important to improve the security of systems and software to protect against vulnerabilities with greater ease of maintaining security standards. There are actual security patches which are not installed, which exposes systems and can compromise future hacking and data leaks[186].

3. User Education: By making users aware of the necessity of having a strong password and other security measures in place, the risk of an individual facing identity theft or any kind of fraud is reduced to a great extent. In order to guard user's digital identity, people should use strong, unique passwords and beware of phishing[187].

So, without mince words, digital identity verification has sevral pros for remotely done commerce, however, the organization must overcome the faced challenges that come with it with a good put

[185] Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.

[186] Murdiana, R., & Hajaoui, Z. (2020). E-Commerce marketing strategies in industry 4.0. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *2*(1), 32-43.

[187] Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, *8*(1), 104-110.

in place best practices and security measures to ensure an effective and adversaries safe verifcation ceremony[188].

[188] Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing digital identity goals–the case study of Aadhaar in India. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18* (pp. 489-501). Springer International Publishing.

CHAPTER FIVE

5.1 Conclusion

In this detailed study, we have explored all aspects of digital identity in e-commerce- from its creation and lifecycle management, to the legal consequences and operational consequences of digital data. The key takeaway from the research is that digital identity verification is the first line of defense not only in strengthening security systems, but also in making the customer identify, humanize online transactions and reduce the chances of any fraudulent incidents.

Digital identities undergo a lifecycle in which the identity is created, aspects of it get registered (e.g. collected customer of data), registered and continuously maintained and managed (e.g. data refresh) and de-registered or deleted when it is no longer needed or after the identity has been used. For online stores, digital identity management is absolutely essential, in order for them to secure trust and respect from customers and help ensure their safety. This includes employing strong authentication such as multi-factor authentication at different touchpoints to ensure that users are who they say they are. E-commerce legal implications of digital identity primarily involve compliance with regulations that dictate the use of digital identity, such as General Data Protection Regulation (GDPR) in… It enforces the laws to ensure data protection, privacy and the secure handling of digital identities on a very strong level. Failure to comply carries huge punishments and wrecks a firm's credibility.

Digitally, this affects the quality (efficiency and dependability) of e-commerce. Maintaines the integrity — By allowing only authenticated users to use the services, a business can prevent potentially unauthorized access and malicious fraud. Digital identity verification systems have a vital role to play in this respect as they provide a secure way for customers to affirm their identity and hence, round off the online transaction process, making them more personal. All this, adds

credibility to the customer from the business end and easy the transaction method efficiently. This research underscores the importance of strong digital identity verification systems to enhance security, increase customer confidence and reduce fraud in e-commerce. Businesses can make the online environment safer and more trusted for their customers when they integrate these holistic identity management practices.

5.2 Implications for e-Commerce

This research provides valuable e-commerce insights. It is a stark reminder which confirms the need for more stringent digital identity proofing measures in order to protect financial misconduct and strengthen the entire security system. It also highlights the necessity of protecting user privacy and complying with relevant laws to build trust and establish credibility with customers. We also explore the impact digital IDV has on customer journey improvements and business growth opportunities.

5.3 Recommendations for Future Research

Future researchResearch frameworks may be based upon emerging theoretical insights, providing a number of interesting directions to extend the findings of this study. It would also be useful to go further and investigate the effectiveness of digital identity verification methodologies and technology and to what extent they may or may not improve security and fight against frauds. Similarly, as part of e-commerce, user should analyze e-commerce customer trust & loyalty in a digital ID compliant electronic world. In addition, research efforts might explore how scalable,

interoperable digital identity solutions can keep pace with the growing requirements of the e-commerce industry.

5.4 Final Thoughts

The link between the findings and how crucial digital identity verification is to e-commerce concludes that it is almost beneficial for the e-commerce industry and consumers on a wide scale. Adopting a holistic concept around digital ID and leveraging best approached to validate its legitimacy could be instrumental in providing additional security whilst promoting customer satisfaction for the businesses and enabling growth in the digital domain for the longer term.

REFERENCES

References

Achmad, W. (2023). MSMEs Empowerment through Digital Innovation: The Key to Success of E-Commerce in Indonesia. *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 469-475.

Ahmad, A. Y. B., Gongada, T. N., Shrivastava, G., Gabbi, R. S., Islam, S., & Nagaraju, K. (2023). E-commerce trend analysis and management for Industry 5.0 using user data analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(11s), 135-150.

Al Mashalah, H., Hassini, E., Gunasekaran, A., & Bhatt, D. (2022). The impact of digital transformation on supply chains through e-commerce: Literature review and a conceptual framework. *Transportation Research Part E: Logistics and Transportation Review*, *165*, 102837.

Alsubari, S. N., Deshmukh, S. N., Al-Adhaileh, M. H., Alsaade, F. W., & Aldhyani, T. H. (2021). [Retracted] Development of Integrated Neural Network Model for Identification of Fake Reviews in E-Commerce Using Multidomain Datasets. *Applied Bionics and Biomechanics*, *2021*(1), 5522574.

Bădîrcea, R. M., Manta, A. G., Florea, N. M., Popescu, J., Manta, F. L., & Puiu, S. (2021). E-commerce and the Factors Affecting its Development in the Age of Digital Technology: Empirical Evidence at EU–27 level. *Sustainability*, *14*(1), 101.

Ballerini, J., Yahiaoui, D., Giovando, G., & Ferraris, A. (2024). E-commerce channel management on the manufacturers' side: ongoing debates and future research pathways. *Review of Managerial Science*, *18*(2), 413-447.

Boysen, A. (2021). Decentralized, self-sovereign, consortium: The future of digital identity in canada. *Frontiers in Blockchain*, *4*, 624258.

Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

Chin, S. H., Lu, C., Ho, P. T., Shiao, Y. F., & Wu, T. J. (2021). Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things. *Computer Standards & Interfaces*, *76*, 103504.

de Andrade, N. N. G. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, *28*(2), 153-162.

Din, A. U., Han, H., Ariza-Montes, A., Vega-Muñoz, A., Raposo, A., & Mohapatra, S. (2022). The impact of COVID-19 on the food supply chain and the role of e-commerce for food purchasing. *Sustainability*, *14*(5), 3074.

Esmeli, R., Bader-El-Den, M., & Abdullahi, H. (2022). An analyses of the effect of using contextual and loyalty features on early purchase prediction of shoppers in e-commerce domain. *Journal of Business Research*, *147*, 420-434.

Feher, K. (2021). Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. *Journal of information science*, *47*(2), 192-205.

Geng, R., Wang, S., Chen, X., Song, D., & Yu, J. (2020). Content marketing in e-commerce platforms in the internet celebrity economy. *Industrial Management & Data Systems*, *120*(3), 464-485.

Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. *computers*, *9*(3), 66.

Hongmei, Z. (2021). A cross-border e-commerce approach based on blockchain technology. *Mobile Information Systems*, *2021*, 1-10.

Jain, G., Kamble, S. S., Ndubisi, N. O., Shrivastava, A., Belhadi, A., & Venkatesh, M. (2022). Antecedents of Blockchain-Enabled E-commerce Platforms (BEEP) adoption by customers–A study of second-hand small and medium apparel retailers. *Journal of Business Research*, *149*, 576-588.

Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825.

Khrais, L. T., Zorgui, M., & Aboalsamh, H. M. (2023). Harvesting the digital green: A deeper look at the sustainable revolution brought by next-generation IoT in E-Commerce. *Periodicals of Engineering and Natural Sciences*, *11*(6), 5-13.

Kiba-Janiak, M., Marcinkowski, J., Jagoda, A., & Skowrońska, A. (2021). Sustainable last mile delivery on e-commerce market in cities from the perspective of various stakeholders. Literature review. *Sustainable Cities and Society*, *71*, 102984.

Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673-1685.

Kleisiari, C., Duquenne, M. N., & Vlontzos, G. (2021). E-Commerce in the Retail Chain Store Market: An Alternative or a Main Trend?. *Sustainability*, *13*(8), 4392.

Landim, A. R. D. B., Pereira, A. M., Vieira, T., de B. Costa, E., Moura, J. A. B., Wanick, V., & Bazaki, E. (2022). Chatbot design approaches for fashion E-commerce: an interdisciplinary

review. *International Journal of Fashion Design, Technology and Education*, *15*(2), 200-210.

Lee, C. S. (2022). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13-14), 2529-2553.

Li, H., Hu, Q., Zhao, G., & Li, B. (2022). The co-evolution of knowledge management and business model transformation in the post-COVID-19 era: insights based on Chinese e-commerce companies. *Journal of Knowledge Management*, *26*(5), 1113-1123.

Li, M., Shao, S., Ye, Q., Xu, G., & Huang, G. Q. (2020). Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. *Robotics and Computer-Integrated Manufacturing*, *65*, 101962.

Lucas, G. A., Lunardi, G. L., & Dolci, D. B. (2023). From e-commerce to m-commerce: An analysis of the user's experience with different access platforms. *Electronic Commerce Research and Applications*, *58*, 101240.

Luo, N., Wang, Y., Zhang, M., Niu, T., & Tu, J. (2020). Integrating community and e-commerce to build a trusted online second-hand platform: Based on the perspective of social capital. *Technological Forecasting and Social Change*, *153*, 119913.

Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing digital identity goals–the case study of Aadhaar in India. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18* (pp. 489-501). Springer International Publishing.

Mohammed, I. A. (2021). Factors affecting user adoption of identity management systems: An empirical study. *International Journal of Innovations in Engineering Research and Technology*, *8*(1), 104-110.

Murdiana, R., & Hajaoui, Z. (2020). E-Commerce marketing strategies in industry 4.0. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *2*(1), 32-43.

Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.

Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. *GSC Advanced Research and Reviews*, *18*(3), 066-077.

Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395-410.

Sepashvili, E. (2020). Digital chain of contemporary global economy: e-commerce through e-banking and e-signature. *Economia Aziendale Online-*, *11*(3), 239-249.

Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.

Sullivan, C. (2013). Digital identity, privacy and the right to identity in the United States of America. *Computer Law & Security Review*, *29*(4), 348-358.

Sutinen, U. M., Saarijärvi, H., & Yrjölä, M. (2022). Shop at your own risk? Consumer activities in fashion e-commerce. *International Journal of Consumer Studies*, *46*(4), 1299-1318.

Svobodová, Z., & Rajchlová, J. (2020). Strategic behavior of e-commerce businesses in online industry of electronics from a customer perspective. *Administrative Sciences*, *10*(4), 78.

Tammpuu, P., Masso, A., Ibrahimi, M., & Abaku, T. (2022). Estonian E-Residency And Conceptions Of Platformbased State-Individual Relationship. *Trames: A Journal of the Humanities & Social Sciences*, *26*(1).

Tofan, M., & Bostan, I. (2022). Some implications of the development of E-commerce on EU tax regulations. *Laws*, *11*(1), 13.

Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: a framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054.

Vieira, J., Frade, R., Ascenso, R., Prates, I., & Martinho, F. (2020). Generation Z and key-factors on e-commerce: A study on the portuguese tourism sector. *Administrative Sciences*, *10*(4), 103.

Wang, Y., Lu, Z., Cao, P., Chu, J., Wang, H., & Wattenhofer, R. (2022). How live streaming changes shopping decisions in E-commerce: A study of live streaming commerce. *Computer Supported Cooperative Work (CSCW)*, *31*(4), 701-729.

Willemyns, I. (2020). Agreement forthcoming? A comparison of EU, US, and Chinese RTAs in times of plurilateral E-Commerce negotiations. *Journal of International Economic Law*, *23*(1), 221-244.

Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, *5*(2), 206-221.

Xiong, X., Yuan, F., Huang, M., Cao, M., & Xiong, X. (2020). Comparative evaluation of web page and label presentation for imported seafood products sold on Chinese e-commerce

platform and molecular identification using DNA barcoding. *Journal of food protection*, *83*(2), 256-265.

Yuan, C., Moon, H., Wang, S., Yu, X., & Kim, K. H. (2021). Study on the influencing of B2B parasocial relationship on repeat purchase intention in the online purchasing environment: an empirical study of B2B E-commerce platform. *Industrial Marketing Management*, *92*, 101-110.

Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational inclusion: Getting older adults ready to own safe online identities. *Education Sciences*, *12*(10), 715.