NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 1, Jan.-2021

FACTORS AFFECTING USER ADOPTION OF IDENTITY MANAGEMENT SYSTEMS: AN EMPIRICAL STUDY

Ishaq Azhar Mohammed
Sr. Data Scientist & Department of Information Technology, Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT
This paper discusses the application of identity and access management in Blockchain technology. Over the past two decades, a variety of identity and access management systems have been created for a variety of purposes, based on the requirements of businesses. IdMS is a creative new IT artifact, including developing technology and innovative strategies, to build user identity-centered methods, characteristics, authentication factors and Internet security privileges across various websites [1]. IdMS allows the use of identical user data, manages identification information and credential authentication on different websites, reduces the number of identifiers (– for example, passwords) and identities that a user needs to deal with by increasing online identity online. The desire of the specific user to embrace the suggested solution is essential to adopting any solution on the internet-based domain. Scholars in a variety of disciplines are interested in understanding variables that influence the usage of new IT [2]. The main objective of this study is to understand and empirically examine the important factors affecting the user adoption of IdMS.

Keywords: Identity and access management, identity management systems, identity theft, SSO solutions, information technology

INTRODUCTION
Threats in the online environment are also increasing, especially those who are connected to them. Identity theft has a major impact on personal financial choices and presents security concerns to both individuals and businesses. Identity Management (IdM) technologies handle the identity disorder created by the usage of many numerous configurations and promote a strategy that promotes efficiency and security by lowering user management expenses, identity, credentials, and characteristics [2]. Controlling how individuals identify themselves on various websites is a technologically complex problem. Almost every website requires web users to keep numerous and distinct versions of their online identities, login credentials, and personal details. Password research indicates that a usual web user has around 25 login credentials profiles and inputs roughly 8 passwords each day [2]. A variety of identity management systems (IdMS) using Web single sign-on (SSO) solutions have been developed and deployed to solve this issue. IdMS is described as a new IT artifact that includes the process, policy, and emerging technologies in use for managing user identification details and for controlling access to various websites. Applications using IdMS comprise of Microsoft Live Connect, Facebook Connect, OpenID, Information Cards, OpenID, PayPal Access, and Twitter OAuth. As per a study carried out by Blue Research, most internet users (66 percent) consider IdMS, especially SSO platforms, as an alternate and appealing option for the management and accessibility to their site [2,3]. Consequently, the necessity to deploy IdMS properly is more essential. Nevertheless, IdMS acceptance is slow. For instance, the IdMS adoption rate throughout the United States has been less than 5% and in other nations, it is much lower. IdMS should therefore address the requirement to encourage end-user adoption. In addition, the IdMS technology industry is anticipated to expand in the next years. According to Forrester Research, a technological and market research company that analyzes technological trends and their effect on consumers and businesses, the IdMS market is expected to expand from almost $2.6 billion in 2006 to more than $12.3 billion by 2014 [3,4].
In addition, the utility of IdMS is expected to grow in the event of commercial usage of IdMS, as more users embrace it. Earlier studies have shown that today's atmosphere matures for acceptance and usage by new technologies includes technical advancements, greater comprehension of technology, and more tech-savvy customers. The acceptance or refusal of the IdMS artifact is, however, still unclear. It may be possible to improve IdMS user adoption by understanding human identity and researching variables that affect IdMS acceptability. Therefore, it is necessary to create a model that incorporates the important features of IdMS

and variables based on their comprehension, especially from the end-user viewpoint. Through this research, variables that affect user acceptance of identity management systems are determined and explained.

PROBLEM STATEMENT

The main problem that this paper will try to solve is an assessment of the factors that affect the adoption of identity management systems. As a subject in current literature, identity is becoming more prominent, and identity management has been recognized as an emerging discipline and a major study issue for the next few decades. The adoption of IdMS by users may have an impact on an individual's approval of other applications that deploy and exploit the same technologies to their advantage [3]. Because the deployment of new IdMS brings with it a new set of hazards, knowing how the risks associated with new IdMS implemented in online services are viewed and handled may be important to individual usage of online products [4]. However, nothing is understood about how IdMS users view their interactions with the system. To improve the design of IdMS and boost acceptance, it is essential to study how consumers perceive this new technology in various Web-based programs like networking sites and e-commerce.

LITERATURE REVIEW

A. Identity Theft

Identity fraud and identity theft are two of the most serious issues for customers who frequently engage with businesses and brands online. These two words are often used in the same sentence. A variety of crimes involving fake identification, that is, using someone else's identity to get anything, are referred to collectively as identity fraud [4,5]. Identity theft is defined as the use of another individual's private information for one's gain. Identity theft and identity fraud are both criminal offenses that are often perpetrated in conjunction with other breaches of security. When it comes to identity theft, there is an extra dimension of victimization as this type of fraud can have a direct impact on the lives of the victims (whose identities have been stolen) as well as scamming third parties like the providers, consumers, commercial banks, and other organizations.

B. Identity Management

The phrase 'identity management (IdM)' has gained widespread use in academics and industry. The word, on the other hand, does not have a widely recognized definition. This lack of general understanding may be explained by the fact that IdM is a relatively new word whose definition is not yet fully defined in the scientific community. There is a significant correlation between IdM and operations in developing digital environments [4]. Another IdM description called it the framework and system for controlling identification in computers or communications networks. Information and digital identity management (IdM) is the process of representing and identifying entities as digital signatures in web servers. Integrated digital management (IdM) comprises processes, rules, and technology that enable users to gain access and privileges via the use of authentication methods.

C. Identity Management Systems

Users' access to important web applications is controlled and managed via identification and authentication, which protects business dealings data from unauthorized users. Identification is a component of identity management and is carried out through an identification system [5]. The IdMS concept is extensive and multifaceted since there are various needs and viewpoints for each of the parties involved (users, IDPs, and service providers). Furthermore, IdMS may be used in systems with varying levels of security, from high to low [5,6]. Additionally, IdMS are user-controlled systems that are managed by companies or governments. Furthermore, IdMS may be either "anonymously credential-based" or "token-based," which means that some of these systems depend on user-to-service-provider mediation, whereas others allow users to establish their identities using anonymous credentials. Therefore, IdMS has been described in a variety of various ways and with distinct interpretations. Integration of essential personal information from various systems into a single shared and unique identity has been described as Identity Management Systems (IdMS) [6]. IdMS is a system used to handle the authentication of end-users, access and limitations rights, accounts, and other characteristics that provide a person greater control over identity information. Processes, rules, and

technological innovations are used to manage user identification and regulate access to online resources [6]. IdMS aim to increase efficiency and security while simultaneously reducing the expenses associated with maintaining users and their identities, credentials, and characteristics (also known as credentials management).

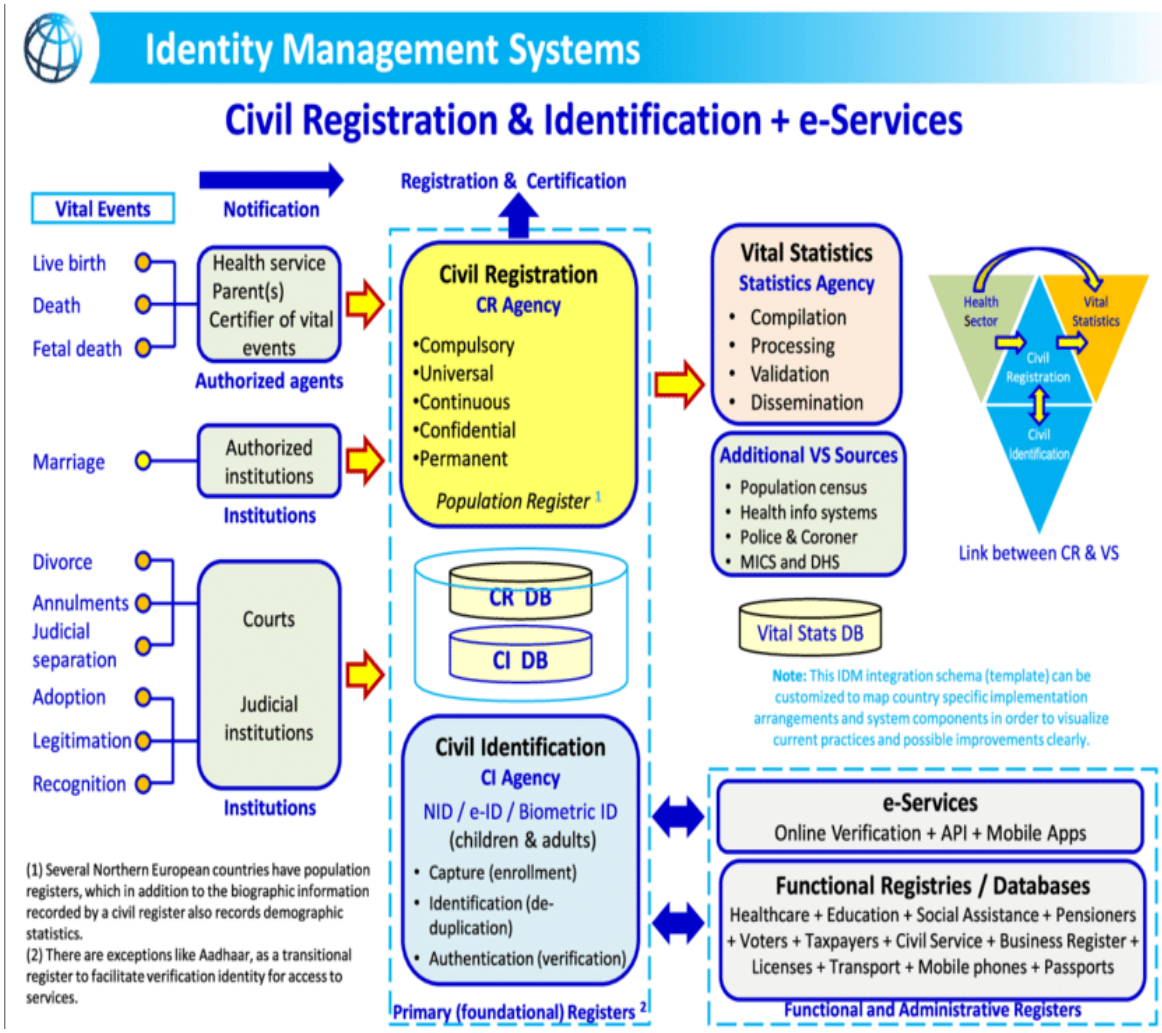

Fig i: Identity management systems

D. Adoption of Identity Management Systems by End-Users

In information system (IS) theory and practice, the adoption and acceptability of information technology (IT) have continued to be a critical issue. The keywords 'adoption' and 'acceptance' have been used to undertake a literature search for these subjects. As a result, the two terms are often used interchangeably [8]. User adoption of information and communications technology (ICT) has preoccupied information and communications technology (ICT) academics to the point that IS/IT adoption and dissemination research is currently regarded as the most mature field of study within the IS discipline [8]. Furthermore, user acceptance of new technology is a continuous management issue that must be addressed. The variables that influence the rejection or acceptance of a new information technology artifact such as IdMS have long been of interest to information systems experts, but they remain a mystery. The study of technology adoption has led to the development of many theoretical models.

However, only a little amount of study has been done on the user adoption of IdMS [8]. During the last decade, many studies have been conducted to determine the variables that affect the adoption of information technology goods or Internet activities like Internet e-commerce and online shopping. Although the demand for Web 2.0 technologies and new Online services such as IdMS is increasing, research is lacking to investigate the adoption patterns of such technologies [9]. Our research has shown that no studies have been conducted that have looked specifically at the deployment of IdMS to incorporate positive or negative

variables at the interpersonal level [10]. As a general rule, this problem connected with the adoption of IdMS has received limited attention in the scientific literature [10]. The unique character of IdMS, as well as the continuing adoption process, served as the impetus for performing an innovation–adoption research on IdMS, which was completed in 2012. As such, the primary goal of most studies is to increase awareness of the significance of impact variables on user acceptance of IdMS. IT is used because it provides real value. As a result, it has been extensively researched, and a variety of concepts have been used to investigate IS/IT adoption and usage in a variety of settings. In the published studies on system integration of information technologies, theoretical models of technology adoption are used, such as the technology acceptance model (TAM) and the innovation diffusion theory (IDT). While many have attempted to capture the unique characteristics of IdMS, few, if any, have contributed novel components that have been experimentally established and verified. Technology adoption theories would benefit from a strong theoretical basis for studying user adoption of IdMS, which would in turn aid in the creation of empirical studies on IdMS's acceptability by users [10].

E. Identity Management System Challenges

Our digital identities are critical to our ability to connect with others on the internet. Digital identity management systems (IDMS) that manage and govern digital IDs, on the other hand, confront many difficulties. Secure identification solutions that are widely implemented and readily understood are needed to address the challenges associated with using the Internet [10,11]. Ongoing research in IdMS is confronted with a slew of difficulties in striking a balance between usability, privacy, and security [12]. End-user liability incentives are required as a result of appropriate frameworks that bring these sometimes-separate elements together with technological solutions that offer liability incentives to end-users. There has yet to be suggested and created a workable method for mutual authentication in which both users and providers are needed to submit credentials, and in which the providers are authenticated to the users and vice versa. Several significant obstacles to IdMS have been highlighted in the literature, with the majority of them being related to design, usability, integration, privacy, security, trust, cost, and acceptance [13].

People, consumers, end-users, and service providers all have a difficulty in determining the desired results and expectations for their respective situations. As a result, further research may reveal what has to be negotiated between users and service providers to properly capture the expectations that are required for the creation of effective identity management systems [13]. A causal model may be created and evaluated to better understand the problems and requirements of IdMS from the viewpoint of its users.

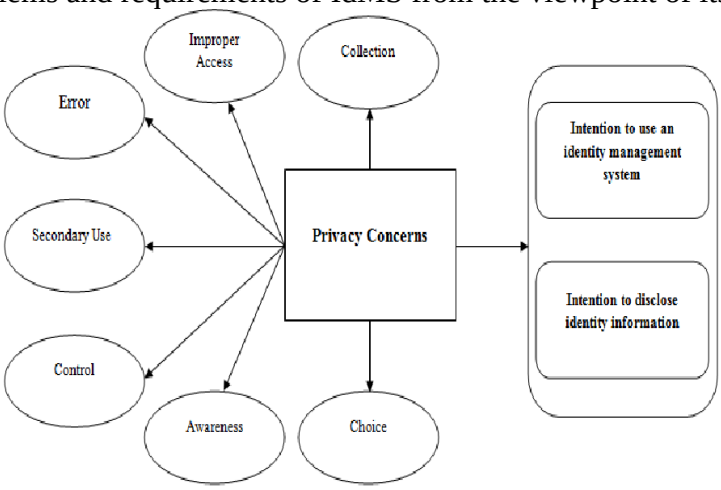

Fig ii: Privacy concerns in User adoption of IdMs

FUTURE IN THE U.S

Given its varied economic, demographic, and political settings, identification systems are a critical part of sustainable development strategies in the United States. Comprehensive identification systems showing significance can provide a wide range of benefits for corporations and companies, especially when they are automated [14,15]. These include making it easier for people to gain access to benefits and rights and to receive services, as well as enhancing the efficiency of public management, strategizing, and delivery of

services [15]. Furthermore, early data indicates that identification systems may help the government save money by reducing fraud and loss in transfer programs, enhancing administrative efficiency, boosting tax collection, and creating new income streams [16]. Because of this, the adoption of strong and inclusive identification systems at the national scale has the potential to provide significant financial benefits for private sector businesses. However, much like with the public sector, determining the direct economic impact of identification systems on private sector companies may be difficult to determine.

Access management will continue to increase in extent and breadth in the USA, influencing trends in identity management from the next generation. The future of IAM will be further reshaped by the continuing adoption of innovations like IoT, Cloud Solutions, and artificial intelligence [16]. Safeguarding digital identities is becoming more essential as digital identities grow more prevalent. To remain competitive, businesses must adapt to changing demands [16,17]. This involves adopting identity management systems that are compatible with their present business requirements while also allowing them to adapt to future developments.

ECONOMIC BENEFITS TO THE U.S

The continued growth of the Internet economy in the United States is dependent on the proper management of online identification information. When it comes to identity management, it is essential in a variety of settings, including the enterprise, e-commerce, and government, since it underpins corporate operations and services, as well as enabling digital interactions and transactions from the viewpoint of the consumer. Identity and identity management systems (IdMS) are a major research subject in the identity and identity management fields [17]. Expanded income levels and revenue-generating possibilities for privately-held businesses across sectors may be facilitated by robust, widely utilized identification systems, which can do this via the following means: An increased identifiable customer base When it comes to accessing public and commercial services that need evidence of identity, the absence of identification papers is a significant impediment [18]. As a result, expanding the reach of strong identification systems has the potential to expand the client base of businesses across a wide range of sectors.

Digital, interoperable, and queriable identity systems may assist to minimize customer attrition by lowering the transaction costs that customers incur while confirming or authenticating their identities [19]. Furthermore, when such systems assist businesses in more accurately assessing risk, they not only aid in the prevention of fraud, but they also help to reduce the number of false positives (low-risk customers who are mistakenly allotted a high-risk score) and turned down transactions as a result of inaccuracy in the verification process [20]. For example, in the United States online retail sector, businesses lose $118 billion in revenue in a given year as a result of unjustified transaction cancellations, relative to a loss of $9 billion due to actual fraud.

Due to the increasing importance of digital identity in the online world, identity management systems (IDMS) have become critical components for the product development and advancement of secure, reliable, and user-friendly IdMS, which is essential in establishing trust in applications such as e-commerce. The introduction of IdMS has, as a result, brought about fundamental changes to electronic transactions; as a result of this, academics recommend that further study into IdMS studies should cover the interactions between people and systems. The importance of digital identity systems in the commercial sector is almost as significant as in the public sector. Many businesses, including those that provide banking services, telecom providers, online business platforms, aviation services, and others, must validate and confirm the identifications of their users at different points throughout the customer lifecycle to transact with them and provide services. In many cases, a government-issued or recognized credential, such as a national identification card, passport, or another document, serves as the source of legitimacy for a customer's identity. In areas where authoritative evidence of identification is difficult to come by, businesses are more likely to have smaller accessible client pools, higher administrative costs, and more fraud risks than in other areas.

CONCLUSION

The main aims of this research were to determine and empirically analyze the factors that influence IdMS user adoption. The results of the research indicate that IdMS will be an alternative and appealing option for

managing and preserving online identities on the Internet in the future, as predicted. But the overall adoption and user acceptability of the IdMS artifact will be driven by end-users' ideas, perceptions, and requirements as well as the impact of these on users' behavioral intentions towards IdMS. In this research, we discovered many significant variables that influence peoples' behavioral intentions to use IdMS. These factors include usefulness, simplicity of use, task–technology fit, trusting attitudes, confidence in the Internet (including information sharing), privacy concerns, and cost. In this reonrd, the IdMS user adoption model will be critical in improving user acceptance rates, assessing technical areas, ensuring effective implementation, and developing security and privacy regulations. In addition, this study serves as a springboard for future investigation and offers a helpful lens through which to examine people's ideas and perceptions in the context of the adoption of IdMS and developing technological innovations at an early stage of adoption, respectively.

REFERENCES

1) A. Alkhalifah, "Understanding the Effect of Privacy Concerns on User Adoption of Identity Management Systems", Journal of Computers, pp. 174-182, 2017.
2) P. Cheney, R. Mann and D. Amoroso, "Organizational Factors Affecting the Success of End-User Computing", Journal of Management Information Systems, vol. 3, no. 1, pp. 65-80, 1986.
3) U. Gl¨asser and M. Vajihollahi, "Identity management architecture," in IEEE International Conference on Intelligence and Security Informatics,June 2008, pp. 137–144.
4) A. Hannoon, "Assessing the role of factors affecting the adoption of VAT-compliant accounting systems", Management Science Letters, pp. 1439-1450, 2019.
5) ICPP, "Identity management systems (IMS): identification and compari-son study," Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG), Tech. Rep., September 2003.
6) P. Coelho, A. Zúquete and H. Gomes, "Federation of Attribute Providers for User Self-Sovereign Identity", Journal of Information Systems Engineering & Management, vol. 3, no. 4, 2018.
7) H. Jang, "Political Identity and Adoption of a New Management Practice", Academy of Management Proceedings, vol. 2012, no. 1, p. 18048, 2012.
8) G. Alp´ar, J. Hoepman, and J. Siljee, "The identity crisis security, privacy and usability issues in identity management," Identity Management on Mobile Devices, January 2011.
9) A. Arabo, Q. Shi, and M. Merabti, "Context-aware identity management in pervasive ad-hoc environments," IJAPUC, vol. 1, no. 4, pp. 29–42, 2009.
10) E. MacLennan and J. Van Belle, "Factors affecting the organizational adoption of service-oriented architecture (SOA)", Information Systems and e-Business Management, vol. 12, no. 1, pp. 71-100, 2013.
11) Y. Cao and L. Yang, "A survey of identity management technology," in Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on, December 2010, pp. 287 –293.
12) T. Zhou, "The impact of privacy concern on user adoption of location-based services", Industrial Management & Data Systems, vol. 111, no. 2, pp. 212-226, 2011.
13) E. Androulaki, M. Johnson, B. Vo, and S. Bellovin, "Cybersecurity through an identity management system," in Engaging Data Forum, MIT, October 2009.
14) D. Sommer, M. C. Mont, and S. Pearson, "PRIME Architecture V3,"PRIME Consortium, Tech. Rep., May 2008.
15) S. G´orniak, J. Elliott, M. Ford, D. Birch, R. Tirtea, and D. Ikonomou, "Managing multiple electronic identities," ENISA - European Network and Information Security Agency, Tech. Rep., 2011.
16) A. Pashalidis and C. Mitchell, "Privacy in identity and access management systems," in Digital Identity and Access Management: Technologies and Frameworks, February 2011.
17) R. Aguiar, D. Bijwaard, B. A. Farschian, A. Jonas, and A. Sarma, "Pervasive services for next generation heterogeneous networks," in Proc. World Telecommunications Congress 2006: Emerging Telecom Opportunities, May 2006.
18) N. K. Taylor, P. Robertson, B. A. Farshchian, K. Doolin, I. G. Roussaki, L. Marshall, R. Mullins, S. Druesedow, and K. Dolinar, "Pervasive computing in Daidalos," IEEE Pervasive Computing, vol. 10, pp. 74–81, January-March 2011.

19) M. Barisch, E. Torroglosa, M. Lischka, R. Marques, R. Marx, A. Matos, A. Perez, and D. Scheuermann, "Security and privacy enablers for future identity management systems," in Future Network and Mobile Summit, Florence, Italy, June 2010.
20) R. Morgan, S. Cantor, S. Carmody, W. Hoehn, and K. Klingenstein,"Federated security: the Shibboleth approach," EDUCAUSE Quarterly,vol. 27, no. 4, pp. 12–17, January 2004.