ISSN 2278-3091
Volume 9, No.1.2, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse2391.22020.pdf
https://doi.org/10.30534/ijatcse/2020/2391.22020

Innovation of National Digital Identity: A Review

Noor Azaimy Samion[1], Azlinah Mohamed[2]
[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Shah Alam, Malaysia, n_azaimy@yahoo.com
[2]Advanced Analytics Engineering Centre, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Shah Alam, Malaysia, azlinah@tmsk.uitm.edu.my

ABSTRACT

Malaysian National Digital Identity (NDI) initiatives become a strategic move that leads to the growth and necessary transformation of today`s digital service sector. Digital identity would improve the quality and efficiency of public services provision, especially in e-government services. National Digital Identity is a verifiable trusted system to authenticate Internet identity or person digital identity in the cyber world but not to replace MyKad. The initiatives are mainly to authenticate identities of an individual who accessing, perform transactions and digital signing in e-government services. Massive growth in terms of technology and issues related to digital identity has been observed and the lack of centralizing digital identity would be the main challenges in Malaysian e-government services effectiveness. This paper presents a review of digital identity implementation by reviewing 37 publications to identify and evaluate the issue, challenges, and technology impact on NDI implementation. To support the implementation, an exploratory study has been conducted to analyze the implementation of digital identity including India and Estonia as a case study and will provide a comparative evaluation of these findings. The results of this study highlighted possible improvement areas concerning NDI implementation, and Malaysia can also benefit from India and Estonia's experience to ensure the success of implementation from this comparative approach.

Key words: Blockchain, Digital Identity, e-government, PKI.

1. INTRODUCTION

There have been numerous efforts to ensure that Malaysia can acquire a digital environment and telecommunication infrastructure. According to research conducted by the Malaysian Communication and Multimedia Commission (MCMC), they found that 90% of public services are currently online and e-commerce consumers penetration at 61.6% [1]. Meanwhile, 62% of business organizations have internet subscriptions [1]. The research also found that the broadband breakthrough of 100 Malaysian people is 121.1% and the cellular breakthrough of mobiles is 130.2% [1]. Preparedness in terms of the digital environment and telecommunication facilities are imperative to ensure the effectiveness of the digital services sector, support growth of the digital economy and digital lifestyle amongst the population [1]. To achieve the aspiration, MCMC`s launch one of the latest strategies through the National Fiberasation and Connectivity Plan (NFCP) aiming to provide Internet accessibility to 98% of populated areas on average 30Mbps of speed by 2023[2].

The NDI indirectly supports other projects including government online services 2.0 (GOS 2.0) MAMPU, Central Bank (BNM) Financial Sector Blueprint 2011– 2020, Know-Your-Customer electronic usage and consistent with National E-Commerce Strategic Direction Plan by Ministry of International Trade and Industry (MITI) [2]. Malaysia can explore digital services using secure and safe digital identity ecosystems on a cross-border basis of regional and international [2]. In the meantime, the emerging of information technology is increasing day by day and it reflects the growth of risk exposure to cybercrime especially in identity theft. Cybercrime can be defined as illegal activities the usage of computer by committing a crime that breach certain law including identity theft [5]. Identity theft can be described as identity fraud in which someone or a system pretends to be someone else by acquiring certain personal information such as identification number, phone number and so forth to impersonate the individual for their benefit [6]. The number of cases involving identity theft in Malaysia rose 20% from 371 in 2017 to 446 in 2018, based on Malaysia Computer Emergency Response Team (MyCERT) Incident Statistics 2018[6]. The personal data used for identity theft was probably derived from the many cases of privacy abuse during the past years however only 4% of the data was encrypted [6]. By implementation of National Digital Identity in Malaysia, it seems to be fitted with others government digital initiative and connecting the dots into one centralized identity solution to improve efficiency of government delivery system without ignorance of security, integrity and social benefits.

The main goal of his study is to analyze digital identity implementation and comparative evaluation of finding based on a case study at India and Estonia as a benchmark and to provide a key factor concerning digital identity implementation. The phase of identifying an issue, challenges, and technology impact is critical for the decision making of successful implementation to Malaysian citizens and to mitigate the risk and to avoid abandoned technology or project afterwards. The study also highlighted the lack on previous study which not covered the review of current implementation and local needs in terms of the people, business and the nation.

The rest of the paper is structured into 6 sections that represent each of the key aspects of NDI research. Section 2 is a related study which presents identity type, the issues currently the main concern for digital identity implementation, the challenges and technology impact. Section 3 is a methodology which consists of method selection and approach. Section 4 will discuss the finding which consists of results and analysis. Section 5 represents discussion and future research. Finally, section 6 is the conclusion of the research.

2. RELATED STUDY

A new Malaysian brainchild initiative was introduced in August 2019, the National Digital Identity that is meant to extend the legality and identification of online applications. The goal of making an NDI is the government`s effort to encourage confidence in e-government, digital economy, online business and services in Malaysia.

Meanwhile, the marketplace for numerous services that facilitate the subscription of the telecommunications infrastructure should be met on these aspects of infrastructure availability. In line with [7], a high-quality ICT infrastructure is one amongst the main factors that create government progress in the implementation of e-Government. This study explores from a Malaysian viewpoint regarding the issues, the challenges, and therefore the technological effects of citizens. To ensure citizens can demonstrate their identity online, reliable confidentiality and assured protection, a robust model of authentication system must be established with a secure and trusted network in a digital identity management system. The scope of the study focuses on a review of the current implementation and local needs of the people, business and the nation. The result of this study is concerning the key factor of digital identity implementation supported on a case study in the Republic of Estonia and the Republic of India. The selection of both countries based on the conceptual and practical level of implementation of digital identity. Estonia is known as a pioneer digital governance and leverages its technology in every aspect of governance including the first country in the world embrace an election over the internet. Whereas India, their national digital identity known as Aadhaar (Hindi word translate to 'foundation') was established in 2008 with more than one billion enrolments and considered the largest biometric-linked digital identity system in the world [3].

2.1 Identity

Identity (ID) is the set of all attributes of an entity, whether it's a human, a business or an object and help to differentiate between each other [26]. Identity is a part and parcel of daily life in several components especially in government administrative, social and business transactions [9]. As a result, identity management is very important for the government in creating a good society. However, the government identity system typically not to be dormant and often undergo metamorphose according to time, culture and society.

Physical identity – Mykad

A Frenchman, Roland Moreno was patented smart cards for the first time in 1974, however, the idea was only widely used in the era 80s and 90s. There are a few factors the usage of smart cards ideally acceptance by the world due to smart card patents expired in 1995, fraud case associated with magnetic strip cards drive business to find a secure alternative and technology available in terms of cost-effectiveness and interoperability of equipment [10]. Malaysia is the first country in the world to use photo identification and biometric data on the integrated chip as a national identity card [10]. Apart from identification purposes, it also contains a valid driver's license, a digital certificate and personal keys with Public Key Infrastructure (PKI) protection to allow electronic signature transactions. MyKad may store information about the passport but does not replace the travel document entirely. MyKad was launched as one of the four MSC Malaysian flagship applications and as to improve the system and change the current Identity Card [10].

Electronic Identification (e-ID)

Digital ID or electronic identification (e-ID) is a digital representation of data on a person, organization or object [11][12][27]. It is the computer network that refers to a person or entity's real identity. e-ID consists of information about an individual, organization or system that represents them across computer networks. All information is provided in e-ID can be integrated with driver's licenses and passports. The main purpose of e-ID is to perform a transaction in e-government, job employment, health care, social security and taxation [11].

2.2 Issues of NDI

There are a few issues need to be considered to minimize the risk and significant impact of NDI implementation. Having a technical infrastructure and Cybersecurity is the main concerned in e-government management.

Identity theft

Theft of personal information (identity theft) in e-government threat comes from the misuse of individual personal data which may include individual identification, passwords, social security numbers, information on credit cards and so on. This is usually referred to as identity theft with a huge number of citizens data is gathered, stored, analyzed and revealed during the e-government processes [6][13]. There were many potentials for Malaysia's e-government exposed to the risk of security threat and identity theft such as Department of Registration, taxation, Land Registry Office and other public-facing departments that contain valuable personal data of an individual. When dealing with transactions, NDI can offer an opportunity to improve the security and privacy of personal information. The real applications of NDI would be less likely to be exploited to use them as malicious purposed by using biometrics and related digital authentication and data capture technologies. Mostly the passwords, keys, and cryptograms are included but forging a fingerprint or other biometric information of another person is complex.

Digital Divide

Today we live in a world where digital technologies have invaded everything in our lives, changing the nature of learning through the introduction of new types of information. Because people have little or no access or exposure to digital technology and the Internet in our modern world, their capacity to fully contribute to and benefit from society and the economy is reduced [14][15]. Essential to other members of society these people are disadvantaged [14]. To bridge the gap by applying national and global strategies that share information and knowledge more equally among the rich and poor information, it is important to understand what the digital division constitutes [14]. Most countries seek to pursue new policies to achieve their technical objectives and thus to close down the digital divide between the people. As defined by Economic Co-operation and Development (OECD), the "digital divide" refers to the differences in the use of the internet and the use of the Internet for many activities among people, communities, businesses and geographic areas at various socio-economic levels [28][29].

In Malaysia, the digital divide may cause by a few factors such as age, education, wealth, and location, among others. The MCMC is attempting to reduce this gap by addressing practical terms to improve the underprivileged areas. According to MCMC, Internet access is below the national broadband penetration rate, which in 2016 stood at 76.9% or 24.5 million users in Malaysia [4]. The digital divide created a new paradigm for defining society which had a significant impact on the daily activities and living lives, especially in Malaysia. The opportunity to access the Internet in full create disparities and segregation in various fields. Income gaps and education play a key role in narrowing digital gap which indirectly leading to the ethnic and racial disparities in access to technology in homes and workplaces. The implications of this gap are highly perceived in areas of employment, work opportunities, connectivity, politics, businesses, health sectors, community growth and emergency situations.

2.3 Challenges of NDI

Most of the governments in the world believe that e-government implementation will improve their image as modern, credible and efficiency through technology placement. However, there is no perfect or definite guideline for successful implementation but proactive measurement, good planning, identity management, and regulation & law may mitigate the failure dan close the gap of NDI implementation.

Regulation & Law

The Malaysian government gradually introduced a law to promote such e-government initiatives, such as the Computing Crimes Act 1997, the Telemedicine Act 1997, the Digital Signature Act 1997, the Copyright Act 1997, the Communication and Multimedia Act 1998, the Electronic Commerce Act 2006, the Electronic Government Activities Act 2007 and the Personal Data Protection Act 2010[6].

Digital Identity Management

Digital Identity Management (DIM) must be in place to protect a digital identity [16]. Such management is critical for users to be customized, data protection and regulatory compliance [11]. It is quite feasible for an organization to produce the most efficient identity management by evaluating the risk and impact of errors for every single digital authentication element [26]. According National Institute of Standards and Technology Special [26], there a guideline is assisting an administrative to avoid an error:(1) Identity proofing error (i.e., a false claimant alleging a wrong identity), (2) Authentication error (i.e., a fraudulent plaintiff who uses a flawed credential) and (3) Federation error (i.e. the statement of identity is affected). The importance of a DIM approach to public policy issues mostly related to the trust. Trust is a pillar of digital electronic government, electronic commerce and social interactions. The enhancement of trust will accelerate the development of digital government and business services and increase among stakeholders.

2.4 Technology of NDI

Nowadays identity systems and tomorrow's future identity systems generally fall into three types: hierarchical, federated and decentralized. Their fundamental structure distinguishes them, with implications for adoption and trust level [30]. In centralized, the assets of an organization that manages and operates the system are used in this traditional system. The

owner or manager of the device (such as the software provider of a third party acting on behalf of the owner) must register, use and store the personal identity and related data [27][30]. In federated, the system defines where two or more central system holders establish mutual trust, either through the distribution of evidence and trust components or through the proofing of trust and evidence requirements [3][30]. Whereas in decentralized, the systems do not rely on a single system owner or group of system owners for identity recognition and management. Alternatively, it usually consists of a digital device owned and managed by an individual including identity information store [17[[30][32].

Technology availability

Technology is an important factor in determining the direction and effectiveness of the system and thus providing effective service to people in the implementation of digital identity. Several technologies apply to the implementation of digital identity mainly PKI and blockchain. Technology is selected for several reasons, including automation and human-oriented processes, security, governance, privacy and data protection, and cybersecurity.

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) has been developed to support a public key (asymmetric) cryptography. The plaintext message is encrypted using the public key of the sender in this form of cyphertext message, and the receiver is likely the only one to decrypt the ciphertext message into a plain-text message using the private key [18]. The term PKI is used to define procedures, technologies, and practices needed for the delivery of a secured infrastructure [27][31][33][34]. A PKI component consists of the following: Authentication: This can be described as an identifying method. PKI facilitates this via digital certificates. Non-repudiation: All information sent at a later time could be ignored by the sender. This ensures that the information received are trustworthy by ensuring and validating the owner of the digital document. Confidentiality: described as a measure of securing transmission of information through networks and ensuring unauthorized persons do not have access to it. Encryption algorithm used by PKI safeguard confidentiality. Integrity: Data integrity principle means that no changes should be made to information while moving through the network. Data integrity has been secured by cipher-text messages using the hashing algorithm. Access Control: this is defined as to allowing access to information that is permitted only to individuals with the necessary security permissions [31]. The implementation of PKI has been widely used in Malaysia especially involving e-government services such as e-Filing system for citizen income tax return form and Government Public Key Infrastructure (GPKI) for Malaysian government officers. However, the main problems in this algorithm is the low speed of transaction, a substantial increase in cryptogram size compared to the size of original message, and a declining the resistance because of the advancement of mathematical methods. There is emerging technology for public key infrastructure to be explored with a different algorithm namely elliptic curve cryptography (ECC) as an alternative to offer a stronger security and performance [8].

Blockchain

Blockchains can be described as tamper-evident, tamper-resistant electronic ledgers that are applied in a decentralized manner and typically not implemented by a central authority of a country [19]. For a basic understanding, any transaction by a group of users requires to be registered in a shared ledger in the community so that no transaction can be altered once the blockchain network is released. The idea of blockchain technology merging seamlessly with computing concepts and other innovations emerged as a modern cryptocurrency in 2008. The modern cryptocurrencies knowns as bitcoin are digital cash secured by cryptographic mechanisms as an alternative of a central repository or authority [26]. Bitcoin are described in the paper [19][20][21] and bitcoin cryptocurrency network was established a year later in 2009. The Nakamoto paper has included a prototype following the most modern blockchain-monetary schemes. Bitcoin was considered the first of several blockchain implementations [19]. Blockchain components consist of the following: Ledger: The platform that uses a ledger to record a detailed history of transactions and value in the blockchain not able to override [19]. Secure: The data in the ledger is not manipulated and the data can be verified [19]. Shared: The ledger of blockchain using decentralized concept and guarantee accountability across the blockchain network nodes [19]. Distributed: Blockchain able to distribute to allow blockchain networks to be more robust to attack from bad actors by scaling up the number of nodes [19]. Trusted digital identification is one of the main challenges faced by the Internet since it has been created and neither of the conventional, offline methods of checking that anyone whom they think their identification is being used. In addition, digital identity will raise questions about critical failure factors and management purposes if these IDs are produced, processed, and controlled by a central agency and contrast with blockchain distributed technology.

2.5 Case Study: Republic of Estonia

Estonia is a relatively small country in the Baltic region of Northern Europe. The country formed after independence from the Union of Soviet Socialist Republics (USSR) in 1992. It is estimated to be the least-populous member of the European Union with a population of 1.3 million [24].

Estonia grasps innovation in every field of governance up to the next generation [30]. Since Estonia was implemented digital identity, their e-government transforms into a fully transparent administration, a very high degree of freedom, rule of law, a simple flat-rate, low indirect taxation system and openness to foreign investment and so on are the key indicators that show Estonia's solid position [22]. Estonia is the first nation to embrace internet elections and provide e-residency. Another step in the direction of e-government is the Estonian identity card. The ID card is an enforced identity document for Estonian people just like in many other countries. It serves the dual purpose of providing proof of identification and specifically setting up an individual's identity in the electronic environment, including serving as an individual's digital signature [3]. The ID program is leveraged in three ways under the Estonia Digital Identity Program which is 1) ID card: The general parts of the photo ID are included in this card. Apart from the legitimate photo ID sections, a card chip holds embedded files and can be used as decisive proof of identity in the digital world using 2048-bit public key encryption [27]. 2) Mobile ID: Mobile ID enables people using mobile device a protected digital identification. Same purpose like an ID card, mobile ID meant for e-services or online businesses to access and signing documents digitally without the need for a card reader through a Mobile-ID SIM card provided by telco operators for citizen usage [23][27].3) Smart-ID: Smart-ID servers as a mobile app identification solution and therefore does not require a SIM card on a smart mobile device.

There are a few areas that deliver a positives impact on Estonia. ICT is one of the areas affected while digital identity was implemented and the growth of internet usage from 28.6% in 2000 to 84.2% in 2014 and on the other hand the percentage rate of an individual was not IT savvy was dropped only 10% in 2015 from over 32% in 2006[22]. Another area concerned was the economic growth and global competitiveness was raised. Estonia considered among EU countries has the fastest growing real Gross Domestic Product (GDP) and among the lowest unemployment rate in EU countries [22]. Estonia demonstrates one of the most advanced digital identity implementations and discovers the scale of an impact once a restriction can be recognized, even though a population is technically experienced. In general, even though Estonia has a small population and a highly developed infrastructure, significant risk management steps are required. The effect would likely have been significantly greater in developing countries with weak infrastructure and populated [3].

2.6 Case Study: Republic of India

The National Unique ID Program (UID) of India was introduced in 2008. It is now known as 'Aadhaar' (a Hindi word means foundation). It is a specific 12- digit count, given with biometric and demographic data of each Indian citizens. It is reported to have the largest biometric-linked national ID system with over one billion claimed registrations in India [30]. When established, the program aimed at reducing social benefit fraud, waste and abuse by ensuring that benefits are given to the right person and increase the efficiency of the welfare delivery system. Now the project has expanded to cover various daily aspects in India, for example, bank transactions and the use of mobile phones [35]. India had major difficulties in identifying social program beneficiaries. A large proportion of residents lacked formal credentials, and many who had credentials are limited to recognized locally. Inadequate recognition and confirmation procedures meant that public authorities often provided social welfare services to the same citizens on several occasions or to persons without qualifications. Before Aadhaar, 58% of the food grains subsidized and 38% of kerosene subsidized government programs were estimated not to reach their desired beneficiaries. The result led to a massive waste of resources. These concerns have impacted the other social programs including scholarships, education, pensions, and family subsidies. The programs were seen as an opportunity to provide an ID to people who had not previously had or did not have a single ID or as an opportunity to create a super identity which is more durable, traceable, minimal or no risk of misuse or identity theft. After a year of implementation of the programs, billions of Indian citizens have a nationally recognized identity and a variety of government and private sectors have been unlocked. There were over 12 billion US dollars in financial transactions and over 1 billion banks and mobile telephones were connected to Aadhaar [35][36]. The program also has saved the government an estimated USD 10 billion by reducing fraud and abuse.

According to [17], Aadhaar facilitated financial inclusion and equality between men and women. The Centre for Global Development conducted a survey of Aadhaar users in the state of Rajasthan found out that almost every household has now a minimum bank account and a significant proportion of it holds women. Before the Aadhaar, only 44% of women had bank accounts and now risen to 90% [17]. It also found that most women are doing banking transactions for their families. This is significant to the bank industries where Aadhaar helps increasing the trust in customers and the possibilities growths their loan services facilities. Based on case this case study, Aadhaar emphasizes that the development of digital infrastructure could benefit directly from social and financial transactions. This significance of identity means to those who have been previously exclusion are now included in many social security programs. The direct value to improve government employee performance or absenteeism are still uncertain. To realize its full potential as an instrument for changing games that can enhance

transparency, Aadhaar needs to become progressively open and important to urban and rural populations and the rich and poor.

3. METHODOLOGY

The purpose of this study will be involving a few methods that consist of content analysis of past reviews to acquire necessary information. This research goal will be identifying and evaluating the issue, challenges, and technology impact on NDI implementation by reviewing secondary data as a source. The research is exploratorily utilizing a semi-structured qualitative method for gathering information and grounded a model to analyze information. The information has been arranged by pattern or topics and composed to analyze important data and keyword. The study focused on more than a various research paper, technology and computer journals, and books.

The study of the NDI areas has been reviewed to comprehend the circumstance and area of the research. The research input keywords and combination from the area of research; Digital identity, PKI, Blockchain, identity management, digital divide and e-government. About 48 papers were selected and analyzed topic pertinent to the research.

3.1 Approach

In this research, the inductive approach has been used to collect information from different sources. The visual model in Table 1 explains an overview of the process.

Table 1 : The process in an inductive analysis by Creswell [37]

Initial read through text data	Identity specific segment of information	Label the segments of information to create categories	Reduce overlap and redundancy among the categories	Create a model incorporating the most important categories
Broad reading	Segmentation of the text	Categorizing up to 30-40 labels	Categorizing up to 15-20 labels	Categorizing up to 3-5 labels

The purpose of the approach is to create three to five categories of possible improvement areas concerning NDI implementation and summaries that focusing the key aspects of the issues, challenge and technology impact into consideration in the raw data which will be evaluated to be the main themes in the research goals [25].

The approach starts by reading the text thoroughly and consider a mixture meaning was found in the text. The identification of text segments that contain a form of meaning and creates a new category label for the text segment. The category where it is applicable will be added with additional text segment. The initial description of each category was developed to analyse the research relevancy such as text association, link and implication [25].

Table 2: Research Identification Segment of Information

Segment	Scope
Main Segments	Digital Identity
Sub-segments	Issues pertinent to digital identity
	Challenges of digital identity implementation
	Technology underpinning digital identity
	National type of identity
	The critical success factor for digital identity

The main segment of research has been pinpointed to the sub-segment so that the required information can be analysed with more detail to achieve the research aims as per Table 2. Upon listing all the information concerned, the classification of the labels is conducted in the creation of new categories where they are linked to the sub-segment. All of this information may create duplication because the information will be too broad and complex. Therefore, the process in Table 3 was carried out in the formulation of the inductive analysis of quality information.

Table 3 : Findings Selection Process in Sequence

Process	Explanation
1) The preparation of raw data is for data filtering	Format all raw data in the same format as font size, margin, question or important data, if necessary. Every data needs to be backed up. [37]
2) Detailed text reading	Once the data has been prepared, it is necessary to analyse the data by comprehending each context and reaching the theme in great detail.[37]
3) Creation of categories	At this stage, the researcher will identify and define categories or themes. More general categories will come from the research aim. More specific categories will result from repeated data readings. Categories are generated from a meaning unit or by the actual phrases in specific segments.[37]
4) Overlapping coding and un-coded text	In general, qualitative coding has rules that must be concurred with. 1) The text may be classified in various categories 2) there may be text that is not categorized or that does not meet with objective research.[37]
5) Continuing revision and refinement of the category system	The researcher will always have new insights into each category and sub-topic. Selecting quotes that are similar to a theme or significant data. Categories may be combined or linked into superordinate categories if the meanings are equivalent.[37]

4. FINDINGS & DISCUSSION

The results of this study were collected through 37 out of 48 research articles using the inductive approach based on the criteria set out in Table 2 and Table 3. Based on the research objective focusing on the implementation of digital identity and the comparative study, the model produced with main consideration of the good elements of digital identity as shown in Table 4. To further strengthen the results of the research, two case studies were reviewed, namely CS1-Republic of India (Aadhaar) and CS2-Republic of Estonia (e-Identity).

The finding of good elements of digital identity is considered to fall under three pillars. First, Governance in which reported in India case study, several scholars and analysts observed that the introduction of such NDI initiatives excluded people from social welfare and public services (Accessnow, 2018) and to address these issues elements fall under governance such as accuracy, uniqueness, sustainability, scalability, equal opportunity and fair treatment should be considered for NDI implementation. Second, Privacy and Data Protection: NDI services are massive of information, both during registration and during transactions. It raises major privacy and information security issues [3]. Finally, Cybersecurity: Strong architecture and cybersecurity infrastructure will support the effective policy framework for Malaysia NDI. Securing data transactions should be addressed by proper encryption during authentication [3].

Table 4 : Finding of Good Digital Identity Elements

Element	Key factors	Case Study
Acceptable (Governance)	**Accuracy** - Identity-related data **Uniqueness** – Every single person assumed to be different **Sustainability**-system must be robust and future proof **Scalability** – Expand for a growing demand	CS1 - Republic of India CS2 - Republic of Estonia
Thorough (Governance)	**Equal opportunity** – Accessible and authenticated **Fairness treatment**: Inclusion of every single person	CS1 - Republic of India CS2 - Republic of Estonia
Utilitarian (Privacy and Data Protection)	**Utility** – Offer meaningful service **Convenience** – Seamless ecosystem **Ease of use** - Process **Interoperability and portability** – Wider usage and privacy concern	CS1 - Republic of India CS2 - Republic of Estonia
User Preferences (Privacy and Data Protection)	**Transparency** – Log data and tracking **Privacy**-Privacy right and access control **Data protection** – Safeguard from breaches **User control**-Freedom to manage digital identity	CS1 - Republic of India CS2 - Republic of Estonia
Cybersecurity (Protected)	**Protection** – Cybersecurity best practices **Data integrity** – System upholds data integrity **Accountability** – Framework include audit trail and legal protection	CS1 - Republic of India CS2 - Republic of Estonia

Figure 1 visualizes the element of good digital identity that being evaluated and considered on implementation. The sequence of significant elements is Protected with 34 articles, User preferences with 32 articles, Utilitarian with 31 articles, Acceptable with 27 articles and lastly Thorough with 8 articles.

Based on the findings, it can be concluded that the implementation of digital identity is not a matter of technology alone, but the human touch and human intervention prove to have a more significant impact. Technology is not a determining factor of efficiency in digital identity solutions, but they need to take into account the needs of citizen freedom and data privacy. These are the key factors that need to be emphasized by the government.

In Malaysia perspective, NDI concern areas on identity theft issue that are a prerequisite for policymakers to find correct solutions especially involving user authentication. The use of biometrics that difficult to forge can be an additional requirement for the introduction of NDI. According to MCMC, statistics show that Internet access in Malaysia is 67.69% or 24.5 million users. The gap can be reduced by current government initiatives, Fiberasation and Connectivity Plan (NFCP) which aims to provide 98% of the population with an average speed of 30Mbps to the Internet by 2023.

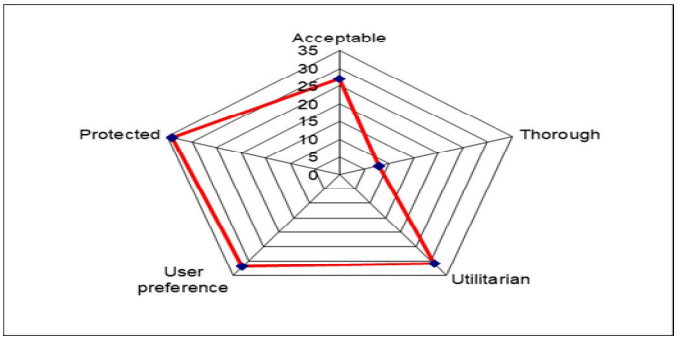

Figure 1 : Research Articles of Good Digital Identity Elements

Such initiatives will boost an impact on ethnic and

racial inequalities in access to technology, especially for a rural group. Referring to the challenges of NDI, the research found Malaysia has a legal framework for holistic digital identity and ready for the implementation of NDI. The design and implementation of NDI must include digital rights for users to sufficiently safeguard them. Failure to contemplate or build in these safeguards should force the shutdown of NDI deployment. For technology impact, the use of PKI technology in Malaysia is not new in a certain government system and the use of this technology was implemented in India. However, the future of Blockchain technology is still in doubt in Malaysia as the legislative framework is not yet established to support NDI initiative.

This research is based on experience in designing and implementing NDI programs around the world. The Indian case study discussed in this article highlights the full range of digital identity systems that need to be tackled to meet the required targets and safeguard human rights [3]. The Estonian experience showed that their NDI system despite its highly sophisticated implementation presents significant risks and is safer using PKI cryptography than the use of biometrics. The advancement of technology like blockchain demonstrates that there are alternatives for the current push for hierarchical NDI systems linked to biometrics [3].

5. CONCLUSION

This paper presents National Digital Identity (NDI) keys areas for establish a good framework for implementation strategy. The study is based on reviewing articles on current implementation and perform comparatives case study in the area of massive implementation and innovative approach. The goal of the digital government is to provide quality rich information and providing efficiency of services to citizens at the same time reducing the cost from the current implementation. As a new transformation initiative by the government of Malaysia, National Digital Identity (NDI) would become an indispensable tool for the government to boost internal and external digital processes that would spillover effect into society, economy, education and wealth of citizens of Malaysia. Although the planning and the approach might sound remarkable, there is no guarantee that the approach will succeed. The ability to identify an individual in the digital world has never been easier because technology becomes more global and complex at the same time. Having said this, the study may benefit to mitigate the risk and identify the gap between theoretical and practical when implementing NDI. Future research will look at the recommendation on how to build a conceptual framework of e-society and the relationship between technological change and economic growth in NDI implementation.

6. ACKNOWLEDGEMENTS

We would like to express our thanks to the Faculty of Computer and Mathematical Sciences, UiTM for the support rendered thus far, Institute of Graduate Study, UiTM for funding and to anonymous reviewers for their useful suggestions.

REFERENCES

[1] Nuraffiza Ahmad, **National Digital Identity Initiatives**,2019 available at https://www.malaysia.gov.my/portal/content/30592.

[2] Hasim bin Zainal Abidin, **The National Fiberisation and Connectivity Plan (NFCP) 2019-2023, 2019** available at https://www.malaysia.gov.my/portal/content/30736,.

[3] Accessnow, **"National Digital Identity Programmes : What ' S Next ? National Digital Identity Programmes",** no. May, 2018 available at https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

[4] Dzof Azmi**, "TELCO DEEP DIVE 2018 : DIGITAL DIVIDE IN MALAYSIA LEAVES MUCH MORE WORK TO BE,"** pp. 1–6, 2019 available at https://www.digitalnewsasia.com/digital-economy/telco-deep-dive-2018-digital-divide-malaysia-leaves-much-more-work-be-done

[5] Reem K. Alqurashi et al, **"Cyber Attacks and Impacts: A Case Study in Saudi Arabia",** p.217, 2020. https://doi.org/10.30534/ijatcse/2020/33912020

[6] S. Zulhuda and A. Ibrahim, "**The State of E-Government Security in Malaysia : Reassessing the Legal and Regulatory Framework on the Threat of Information Theft**", pp. 812–817, 2011.

[7] R. M. Ramli, "**Malaysian E-government : Issues and Challenges in Public Administration**", vol. 44, no. 0, pp. 19–23, 2012.

[8] Kuryazov D.M. **"Algorithm for ensuring message confidentiality using elliptic curves",** p.295 2020. https://doi.org/10.30534/ijatcse/2020/44912020

[9] B. Khan, M. K. Khan, and K. S. Alghathbar, "**Biometrics and identity management for homeland security applications in Saudi Arabia**", vol. 4, no. 15, pp. 3296–3306, 2010.

[10] P. H. P. Yeow and F. Miller, "**The Attitude of Malaysian Towards MYKAD**", no. January, 2005.

[11] M. N. O. Sadiku, A. E. Shadare, and S. M. Musa, "**Digital Identity**", no., 2017. https://doi.org/10.23956/ijarcsse.v7i7.111

[12] R. Darvin, "**Language and identity in the digital age**," no. Norton 2013, pp. 523–540, 2015.

[13] R. Bhatia, "**International Journal of Advanced Research in Biometrics and Face Recognition Techniques,"** vol. 3, no. 5, pp. 93–99, 2013.

[14] D. D. Cycle, **"The Digital Divide,"** no. 2000, pp. 8–9, 2019.

[15] J. Goode, **"The digital identity divide: how technology knowledge impacts college students,"** 2010. https://doi.org/10.1177/1461444809343560

[16] I. Indu, P. M. R. Anand, and V. Bhaskar, **"Engineering Science and Technology, an International Journal Identity and access management in cloud environment: Mechanisms and challenges,"** *Eng. Sci. Technol. an Int. J.*, vol. 21, no. 4, pp. 574–588, 2018. https://doi.org/10.1016/j.jestch.2018.05.010

[17] A. Gelb and J. Clark, "**Performance Lessons from India ' s Universal Identification Program CGD Policy Paper 020 May 2013,"** no. May, 2013.

[18] A. Albarqi, E. Alzaid, F. Al Ghamdi, and S. Asiri, **"Public Key Infrastructure : A Survey,"** no. January, pp. 31–37, 2015. https://doi.org/10.4236/jis.2015.61004

[19] D. Yaga, P. Mell, N. Roby, and K. Scarfone, **"Blockchain Technology Overview Blockchain Technology Overview,"** p. 66, 2018. https://doi.org/10.6028/NIST.IR.8202

[20] S. Nakamoto, **"Bitcoin : A Peer-to-Peer Electronic Cash System,"** pp. 1–9, 2008.

[21] O. Terbu, S. Vogl, and S. Zehetbauer, **"One mobile ID to secure physical and digital Identity,"** pp. 43–54, 2016.

[22] A. A. Sai and P. O. Boadi, **"A Bundled Approach to Explaining Technological Change : The Case of e- A Bundled Approach to Explaining Technological Change : The Case of E-estonia,"** no. October, 2017.

[23] A. M. Al-khouri, **"Identity and Mobility in a Digital World,"** vol. 2013, no. February, pp. 7–12, 2013. https://doi.org/10.4236/ti.2013.41002

[24] H. Margetts and A. Naumann, "**Government As A Platform: What Can Estonia Show The World,"** 2017.

[25] D. R. Thomas, **"A general inductive approach for qualitative data analysis,"** 2003

[26] M. E. Garcia and J. L. Fenton, **"Digital Identity Guidelines"**, 2018.

[27] T. H. E. D. Revolution, **"Digital Identity : The Essential Guide"**, 2018

[28] OECD (2009-06-11), "**The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers"**, OECD Digital Economy Papers, No. 160, OECD Publishing, Paris, 11 June 2009 available at http://dx.doi.org/10.1787/222134375767.

[29] Misra, P. 2019. **Lesson from Aadhaar: Analog aspects of digital governance shouldn't be overlooked**. Pathways for Prosperity Commission Background Paper Series; no. 19. Oxford, United Kingdom 2019 available at www.pathwayscommission.bsg.ox.ac.uk

[30] World Economic Forum, **"Identity in a Digital World A new chapter in the social contract,"** no. September, 2018 available at https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract

[31] M. Dewan, **"An Idiots Guide to Public Key Infrastructure,"** 2002 available at https://www.giac.org/paper/gsec/2171/idiots-guide-public-key-infrastructure/103692

[32] Ernst & Young, **"Implementing blockchains and distributed infrastructure."** 2016 available at https://www.ey.com/Publication/vwLUAssets/EY-implementing-blockchains-and-distributed-infrastructure/$FILE/EY-implementing-blockchains-and-distributed-infrastructure.pdf

[33] de Andrada and Enrique Caceres, "**Biometric PKI Authentication**" U.S. Patent Application No. USOO96926.03B2 issued Jun 27,2017 available at https://patents.google.com/patent/US9692603B2/en

[34] Jordi et al, **"Procedure for generating a Digital Identity of a user of a mobile device, Digital Identity of the user, and authentication procedure using said Digital Identity of the user"** U.S Patent Application No. US 20160360403A1 issues Dec 8, 2016 available at https://patents.google.com/patent/US20160360403

[35] OECD, "**Embracing Innovation in Government, Global Trends 2018, India Aadhaar Case study,"** no. November, pp. 27–32, 2018 available at https://www.oecd.org/gov/innovative-government/embracing-innovation-in-government-2018.pdf

[36] Shweta Banerjee **"Digital Dividends Aadhaar : Digital Inclusion and Public Services in India."** 2016 available at http://pubdocs.worldbank.org/en/655801461250682317/WDR16-BP-Aadhaar-Paper-Banerjee.pdf

[37] John W. Creswell, **"Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research,".** Published by Pearson, 2012.