The International Journal of Engineering and Science (IJES)
|| Volume || 9 || Issue || 01 || Series II || Pages || PP 84-102| 2020 ||
ISSN (e): 2319-1813 ISSN (p): 23-19-1805

Unicard; National Identity Evolution

Hussam Elbehiery[1], Khaled Elbehiery[2]
[1]*Computer Networks Department, Ahram Canadian University (ACU), Egypt*
[2]*Computer Information Systems Department, DeVry University, USA*
Corresponding Author:Hussam Elbehiery

----------*ABSTRACT*----------
The use of information technology in our daily lives has been on the rise. The ordinary governmental based identity system provides a vital foundation of authoritative sources of trust, but they usually focus on delivering official routine services rather than providing a choice of other services, privacy protection, and interoperability. Looking deep into the current identity system, it is widely known that, the identification, verification, and account creation is time consuming and duplicated across multiple systems, as a result, the future should be working towards identity system that demonstrates portability of trust and the ability for individuals to take control of their identity destiny. We are in a desperate need for a new secure electronic identity for citizens in a form "Unicard", a unique identifier used across multiple services, not only the essential services such as electronic passports, driving licenses, issuing citizens personal certificates such as birth certificates, marriage and divorce certificates, government benefits, schooling, healthcare system but also high security access cards such as credit cards. The unicard should be scalable and flexible to accommodate with other services anytime and anywhere that could be beneficial to the citizen such as bank account, mobile phone, utility bills, etc. or it could be necessary for the national security such as credit card, phone records transactions, and more to assure reducing the fraud, identity theft, and terrorism. Many countries already have taken aggressive and rapid steps toward the transition and transformation to an integrated digital society. The research paper will discuss the important aspects of the proposed unicard, links to governmental services, national identity system, and non-governmental services, how the unicard positively affects the country's economic growth and reduce fraud crimes. The security authentication processes that will be used to save and secure this new proposed unicard will also be covered.

KEYWORDS;-*National Identity, Banking Credit cards, Informal Economy, Money Laundering, Organ and Drug Trafficking, AAA, Formal Data Bases linkage.*

Date of Submission: 20-01-2020 Date of Acceptance: 05-02-2020

I. NATIONAL IDENTITY DOCUMENT ID

1.1 National Identity Evolution

A national identity document ("ID", "ID card", "identity card", "IC", "citizen card" or "passport card") is an identity card with photo, usable as an identity card at least inside the country, and is issued by an official authority [2].

In the absence of a formal identity document, a driver's license may be accepted in many countries for identity verification. Some countries do not accept driver's licenses for identification, often because in those countries they do not expire as documents and can be old or easily forged. Some countries require all people to have an identity document available at any time. Many countries require all foreigners to have a passport or occasionally a national identity card from their home country available at any time if they do not have a residence permit in the country [3].

The identity document is used to connect a person to information about the person is often in a database. The photo and the possession of it is used to connect the person with the document. The connection between the identity document and information database is based on personal information present on the document, such as the bearer's full name, age, birth date, address, an identification number, card number, gender, citizenship and more. A unique national identification number is the most secure way, but some countries lack such numbers or do not mention them on identity documents [4] and [5].

Law enforcement officials claim that identity cards make surveillance and the search for criminals easier and therefore support the universal adoption of identity cards. In USA, the new smart identity card has been introduced on 26 November 2018. Personal data on the smart identity card is fully protected and its security features, card durability as well as chip technology on personal data protection have been enhanced [6].

Arguments against overuse or abuse of identity documents such as that those cards reliant on a centralized database can be used to track anyone's physical movements and private life, thus infringing on

personal freedom and privacy. The management of disparate linked systems across a range of institutions and any number of personnel is alleged to be a security disaster in the making [1].

The fear that a national identify card would compromise an individual's right to privacy could happen and lead to the misuse of governmental power. The U.S. and Canada are among countries where a national identify card has been discussed but, so far, not seriously advocated by the government. A number of so-called third world countries require their citizens to carry some kind of national identity card. Today, airlines and banks require some sort of identity authentication. Typically, a driver's license, passport, or other card with your name and an embedded photo is sufficient [4].

1.2 National ID and the REAL ID Act

National ID cards have long been advocated as a mean to enhance national security, unmask potential terrorists, and guard against illegal immigrants. They are in use in many countries around the world including most European countries, Hong Kong, and southeast Asia. The United States and the United Kingdom have continued to debate the merits of adopting national ID cards. The types of card, their functions, and privacy safeguards vary widely. In response to the tragic events of September 11th, 2001, there has been renewed interest in the creation of national ID cards. The public continues to debate the issue, and there have been many other proposals for the creation of a national identification system, some through the standardization of state driver's licenses. The debate remains in the international spotlight -- several nations are considering implementing such systems though. The United States congress has passed the REAL ID Act of 2005, which mandates federal requirements for driver's licenses. Critics argue that it would make driver's licenses into de facto national IDs, and others have called for the repeal of this ill-conceived national identification law [7].

1.3 National ID Cards

The September 11th, 2001 terrorist attacks changed the world, governments, and many people became more and more concerned about their security. A number of countries have considered or considering again their approach to a form of ID card. Despite the support for ID cards, there are growing fears about the possible loss of privacy, freedom, and that the new technology could increase law enforcement’s power more than it should be. The main idea of this research paper is to look at the main advantages and disadvantages of national ID card, security properties of resident ID cards, possible threat and security features and alternatives as well.

1.3.1 Advantages and Disadvantages

New technologies introduce both positive and negative features and the national identity card is one of the contentious issues areas where opinion is divided. Hence, it is not surprising that some countries have mandatory identity cards, some have voluntary identity cards, whereas the rest do not have resident identity cards at all. The following are some of advantages of the national ID card:

- Deal with illegal working and immigration.
- Combating crime and potential attacks by terrorists.
- Enhancing access to public services.
- Gathering the information in one card.
- Prevent forged identity.
- More convenience.

On the other hand, many people argue the disadvantages of identity cards:

- Expensive to administer.
- Encroachment of privacy.
- Increased threat for fraudsters to acquire people's identities.
- Restricting the freedom and increasing monitoring.
- Potential abuses of identification cards.

1.3.2 Security properties

"Smart" identity cards have great security features as listed below:

- Access control mechanisms (ACM).
- Domain-specific unique identify (UID).
- Selective Disclosure.
- Verify-only mode.
- Biometric templates.
- Availability.

It is questionable whether the introduction of a national ID card scheme is an effective way to tackle terrorism and improve national security. There are also serious considerations with regard to data security and civil liberties, which need to be taken into account. However, a number of countries have been using identity cards for many years and ID cards are continually being developed to make them more secure. Taking all things into account and from what it have been examined, the passport is a suitable document to prove identity and is sufficient for maintaining national and international security [8].

II. BANKING CREDIT CARDS

The credit card is a type of bank-card that lets you borrow money – credit – before paying it back with interest. They work as a type of loan, but instead of getting money in an account, you get credit that you spend via the card, before paying back what you owe each month. There are a number of different types of credit cards designed for different people and purposes, including cards that [9]:

- Offer rewards depending on how you use them.
- Help you build your credit report.
- Let you transfer an existing balance onto a new card with lower or no interest.

As long as you use them properly, credit cards can have a number of advantages over debit cards and cash payments. These include:

- Spreading purchases out.
- Buying now to pay later.
- Having purchase protection.
- Getting an interest free loan.
- Getting benefits and rewards.
- Cutting down your debt.
- Boosting your credit rating.

When you use a credit card, you should be mindful of the following risks:

- The possibility of debt.
- Your credit score.
- Fees and charges.
- Limited usage.

Like other financial tools and services, credit cards come with many advantages and disadvantages. It's critical to understand the details before you sign up for any credit card. Otherwise, you may end up with a card that traps you instead of setting you free. Therefore, here are the advantages of using credit cards [10]:

- Purchasing Power.
- Rewards.
- Convenience.
- Trackability.
- Use during an emergency.
- Builds credit history.

There are also disadvantages of using Credit Cards:

- Overspending.
- Interest and fees.
- Fraud.
- Mounting Debt.

III. INFORMAL ECONOMY

An informal economy (informal sector or grey economy) is the part of any economy that is neither taxed nor monitored by any form of government. Although the informal sector makes up a significant portion of the economies in developing countries, it is sometimes stigmatized as troublesome and unmanageable. Integrating the informal economy into the formal sector is an important policy challenge. Unlike the formal economy, activities of the informal economy are not included in a country's gross national product (GNP) or gross domestic product (GDP). The informal sector can be described as a grey market in labor.

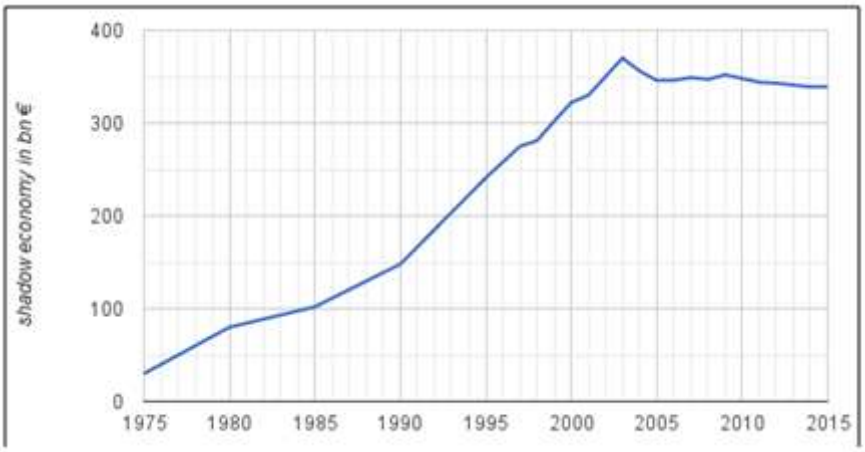

Figure 1. German shadow economy 1975–2015, Friedrich Schneider University Linz

The total EU shadow economy has been growing systematically to approximately 1.9 trillions € in preparation of the EURO driven by the motor of the European shadow economy, Germany, which has been generating approximately 350 bn € per annum since then (see also diagram on the right). Hence, the EU financial economy has developed parallel an efficient tax haven bank system to protect and manage its growing shadow economy. As per the Financial Secrecy Index (FSI 2013), currently Germany and some neighboring countries, range among the world's top tax haven countries.

The diagram below clearly shows that national informal economies per capita vary only moderately in most EU countries. It is because market sectors with high informal part (above 45%) like "building and construction" or "agriculture" are rather homogeneously distributed over the countries, whereas sectors with low informal part (below 30%) like "financial and business" (in Switzerland, Luxembourg), "public and personal services" (in Scandinavian countries) as well as "retail, wholesale and repair" are dominant in countries with extremely high GDP per capita i.e. industrially highly developed countries.

Figure 2. EU shadow economy

The next diagram shows that in absolute numbers the shadow economy per capita is related to the wealth of a society (GDP). Generally spoken, the higher GDP the higher shadow economy, albeit non-proportional. The red scale represents the numbers displayed by the red bars of the diagram on the left [11].

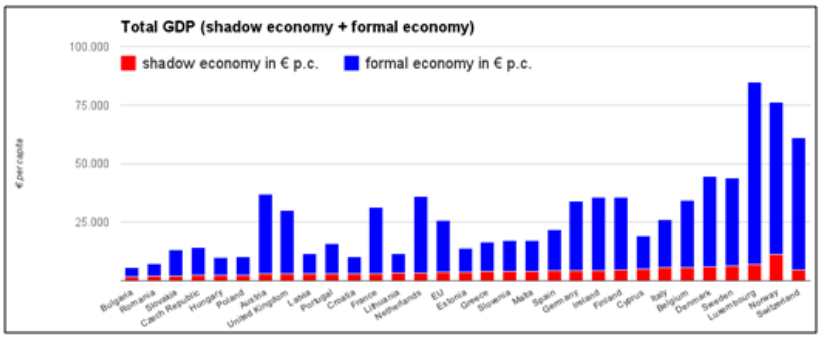

Figure 3. Map of the national shadow economies per capita in EU countries

Therefore, there are five facts about informal economies; First, it is huge, reaching about half of the total in the poorest countries. Second, it has extremely low productivity compared to the formal economy: informal firms are typically small, inefficient, and run by poorly educated entrepreneurs. Third, although avoidance of taxes and regulations is an important reason for informality, the productivity of informal firms is too low for them to thrive in the formal sector. Lowering registration costs neither brings many informal firms into the formal sector, nor unleashes economic growth. Fourth, the informal economy is largely disconnected from the formal economy. Informal firms rarely transition to formality, and continue their existence, often for years or even decades, without much growth or improvement. Fifth, as countries grow and develop, the informal economy eventually shrinks, and the formal economy comes to dominate economic life [12].

3.1 Integration of the Informal Economy into its Formal counterpart

Facing informal projects requires the development of unconventional solutions to encourage this sector to integrate with the formal economy, and deal legally with it. In this regard, many governments in many countries recommended a number of important points to encourage the integration of the informal economy into its formal counterpart, and we review it as follows [36]:

- The governmental trade and industry department and the competent authorities make a comprehensive and complete inventory of all informal economic activities, whether industrial or commercial, and then register their activities in their own control bodies, for example the Industrial Control Authority.
- Encouraging joining the formal sector by giving financing benefits and affiliated loans to everyone who seeks to work legally.
- Examining how this sector can benefit from the experience of setting up incubators for projects that have been created in some countries (these incubators are a complex that the state provides in a place that has a license for a specified period of time ranging between 3 to 5 years and small projects are grouped in it, with a central administration to serve Those projects, and through the incubator after he acquires experience, he can move to his own place).
- Carry out awareness-raising campaigns at the governorate level and places where this informal sector gathered to familiarize workers with the importance and benefits of its entry into the formal sector.
- Giving priority to labor-intensive national projects that absorb various types of employment, whether unqualified or qualified technical, increasing the national private sector's participation in these projects and giving priority to filling the job opportunities provided by these projects to the people of the regions where they are located.
- Activating the monitoring and follow-up on the implementation of these projects, popular, and specialized oversight bodies.

IV. MONEY LAUNDERING

Money laundering is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions. The overall scheme of this process returns the money to the launderer in an obscure and indirect way. One problem of criminal activities is accounting for the proceeds without raising the suspicion of law enforcement agencies. Considerable time and effort may be put into strategies, which enable the safe use of those proceeds without raising unwanted suspicion. Implementing such strategies is generally called money laundering. After money has been laundered, it can be used for legitimate purposes [13].

In another meaning, money laundering is the process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from the criminal activity is considered dirty, and the process "launders" it to make it look clean. Money laundering is itself a crime. Money laundering is essential for criminal organizations that wish to use illegally obtained money effectively. Dealing in large amounts of illegal cash is inefficient and dangerous. Criminals need a way to deposit the money in legitimate financial institutions, yet they can only do so if it appears to come from legitimate sources. Banks are required to report large cash transactions and other suspicious activities that might be signs of money laundering. The process of laundering money typically involves three steps: *placement*, *layering*, and *integration*.

- *Placement* puts the "dirty money" into the legitimate financial system.
- *Layering* conceals the source of the money through a series of transactions and bookkeeping tricks.
- In the final step, *integration*, the now-laundered money is withdrawn from the legitimate account to be used for whatever purposes the criminals have in mind for it.

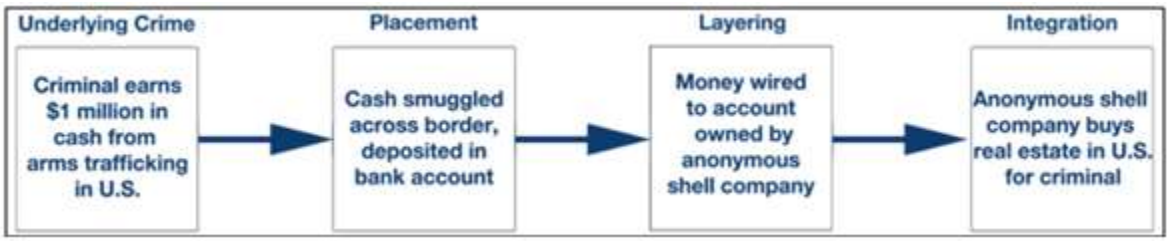

Figure 4. Global Financial Integrity

4.1 Electronic Money Laundering

The Internet has put a new spin on the old crime. The rise of online banking institutions, anonymous online payment services and peer-to-peer (P2P) transfers with mobile phones have made detecting the illegal transfer of money even more difficult. Moreover, the use of proxy servers and anonymizing software makes the third component of money laundering, integration, almost impossible to detect—money can be transferred or withdrawn leaving little or no trace of an IP address. Money can also be laundered through online auctions and sales, gambling websites, and virtual gaming sites, where ill-gotten money is converted into gaming currency, then back into real, usable, and untraceable "clean" money. The newest frontier of money laundering involves cryptocurrencies, such as Bitcoin. While not totally anonymous, they are increasingly being used in blackmail schemes, the drug trade, and other criminal activities due to their relative anonymity compared with more conventional forms of currency. Anti-money-laundering laws (AML) have been slow to catch up to these types of cybercrimes, since most of the laws are still based on detecting dirty money as it passes through traditional banking institutions [14], and [15].

4.2 Money laundering committed offence

Money laundering offences have similar characteristics globally. There are two key elements to a money laundering offence:

- The necessary act of laundering itself i.e. the provision of financial services; and
- A requisite degree of knowledge or suspicion (either subjective or objective) relating to the source of the funds or the conduct of a client.

The act of laundering is committed in circumstances where a person is engaged in an arrangement (i.e. by providing a service or product) and that arrangement involves the proceeds of crime. These arrangements include a wide variety of business relationships e.g. banking, fiduciary and investment management. The requisite degree of knowledge or suspicion will depend upon the specific offence but will usually be present where the person providing the arrangement, service or product knows suspects or has reasonable grounds to suspect that the property involved in the arrangement represents the proceeds of crime. In some cases, the offence may also be committed where a person knows or suspects that the person with whom he or she is dealing is engaged in or has benefited from criminal conduct [16].

V. ORGAN AND DRUG TRAFFICKING

Organ trafficking is possibly one of the most covert forms of human trafficking. A global shortage of organs has driven the industry, relying on poor populations to be donors and wealthy foreigners to be recipients. This section discusses the prevalence of organ trafficking will be explored, especially in relation to transplant tourism. Suggestions to stop trafficking will also be explored. There is no reliable data on organ trafficking, but the World Health Organization (WHO) (2004) believed it to be steadily on the increase, with brokers charging wealthy recipients $100,000+ and giving impoverished donors as little as $1,000, both amounts in U.S. dollars. It is also estimated that 10% of the organ transplants done globally are completed using black market organs (Negri, 2016; United Nations, 2018). Cultural and religious customs ban or discourage some individuals from donating organs willingly or receiving post-mortem organ donations (World Health Organization, 2004). Illegal organ harvesting generally is not harvesting organs from willing donors going against cultural laws for the sake of philanthropy, but harvesting from unwilling or uninformed donors through exploitation of impoverished, indebted, homeless, uneducated, and refugee people (United Nations, 2018). It is difficult to know exactly how many people have been victims or recipients of illegally harvested organs because of the complex nature of organ trafficking, like human trafficking in general, which leads to unreliable statistics and underreporting (Yousaf & Purkayastha, 2016) [17].

Drug trafficking is a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws. UNODC is continuously monitoring and researching global illicit drug markets in order to gain a more comprehensive understanding of their dynamics. Drug

trafficking is a key part of this research. Further information can be found in the yearly world drug report. The Balkan and northern routes are the main heroin trafficking corridors linking Afghanistan to the huge markets of the Russian Federation and Western Europe. The Balkan route traverses Iran (often via Pakistan), Turkey, Greece and Bulgaria across South-East Europe to the Western European market, with an annual market value of some $20 billion. The northern route runs mainly through Tajikistan and Kyrgyzstan (or Uzbekistan or Turkmenistan) to Kazakhstan and the Russian Federation. The size of that market is estimated to total $13 billion per year [18].

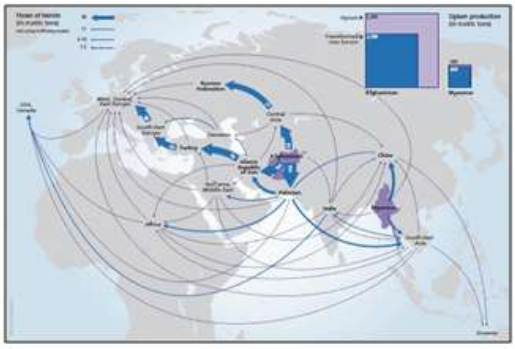

Figure 5. Global heroin flows from Asian points of origin

The United Nations Office on Drugs and Crime's World Drug Report 2005 estimates the size of the global illicit drug market at US$321.6 billion in 2003 alone. With a world GDP of US$36 trillion in the same year, the illegal drug trade may be estimated as nearly 1% of total global trade. Consumption of illegal drugs is widespread globally and it remains very difficult for local authorities to thwart its popularity.

Figure 6. Major Trafficking

VI. TRADE FINANCE DOCUMENT PROCESSING

While international trade has existed for centuries, today's trade finance practices facilitate its growth and success. Banks play an important role of acting as the intermediary for international trade finance to take place. While there are various ways in which trade finance is practiced in banking, trade finance documents remain a constant in these processes. From letters of credit to bills of lading, trade finance document processing is always challenging due to the wide variety of document types and operational requirements in place. TIS document processing solutions for trade finance automate and streamline these processes in three focus areas: *Data Extraction*, *Data Validation*, and *Document Screening* [19].

Figure 7. Trade Finance Validations

Data without validation can rarely be guaranteed of integrity. Benefits of document screening for trade finance documents:

- Incorporation of semi-automation in non-structured operational requirements
- Intelligent extraction with data integrity check
- Fuzzy matching that mimics the way that humans read documents
- Full document sanction screening, alleviating the user's need to perform the mundane, low-value tasks

6.1 Improving Processes for Trade Finance

Today, financial institutions play a critical role in ensuring that their customers are not engaged in money laundering or other criminal or terrorist activities. However, "Know Your Customer" (KYC) and related processes can be time-consuming, costly, and frustrating. Worse, they can interfere with an international business getting the trade finance it needs. In addition, beyond trade finance, it can delay or prevent financial institutions and customers from establishing a wide array of productive financial relationships. Some are looking to Blockchain technology to help.

KYC rules require banks to verify a new customer's identity and the legitimacy of its funds, understand the context of its transactions, and evaluate its money laundering risks. However, KYC-related due diligence and investigation can take months, especially in international environments, and the delays may be worsening. According to one recent survey, 89% of corporate customers have had an unsatisfactory KYC experience, and 13% actually changed their financial relationships as a result.

Further, since each financial institution has its own KYC processes, customers may have to repeatedly jump through similar (but not identical) hoops for trade finance, other lending and banking relationships, securities broker-dealer accounts, currency exchange and money transfer services, insurance services, and more.

6.2 Blockchain and KYC

Recalling how Blockchain works may help make clear why it might be valuable in KYC and related processes. Blockchain establishes a digital ledger of transactions that can be shared across large, decentralized networks of computers. Cryptographic techniques enable each participant in a Blockchain to add new transactions that are verified by other computers on the network using specialized algorithms. Once these transactions are verified and recorded, they become extremely difficult to change or remove. A Blockchain network has no central point of control, and participant computers must reach consensus on verifying new entries. Therefore, advocates argue, Blockchain might resist cyberattacks that can compromise centralized information systems.

We have previously discussed potential Blockchain financial applications in payment processing as well as trade finance, as well as addressing Blockchain's role in enabling cryptocurrencies such as Bitcoin, the application it was created for. In contrast, KYC processes are primarily about verifying information, and only indirectly about transactions. However, Blockchain can verify information in much the same way it verifies transactions.

Typically, Blockchain based KYC services establish a digital identity linked to a customer, and give that customer control of the document exchanges involved in KYC processes. For example, in start-up KYC-Chain's system, the customer owns a private wallet secured by private keys, and can give permission to financial institutions to immediately view the information they need to see, rather than forwarding it manually in paper or electronic format. KYC-Chain's software also enables a customer to confirm identity through a "zero-knowledge based proof" that shares only as much information as is necessary, rather than entire documents.

Conventional KYC processes may involve a financial institution compliance employee phoning or emailing a new customer to access information such as location of incorporation, ownership structure, regulatory status, outstanding legal proceedings, and types of financial transactions anticipated. Deloitte's proof-of-concept KYC start service envisions moving these tasks to regulated KYC added-value service providers. They would be authorized to perform a customer's KYC checking for all the financial institutions it wants to use, and veracity checks already performed by others in the network would be available to streamline future on-boarding. Again, the customers themselves would control who sees their information. Moreover, they would be able to track authorizations via Blockchain based smart contracts [20].

6.3 Linking KYC and Anti-Money Laundering in the Blockchain

As IBM Blockchain expert Nitin Gaur notes, an integrated Blockchain system that encompasses KYC at the customer onboarding stage and Anti Money Laundering (AML) analysis afterwards would have obvious advantages. It could offer a unified source of reliable data and chained transactions where all participants could access audit data and logs, including regulators. In order to share data in a trusted distributed ledger, financial institutions would be required to provide more useful data for analysis by participants throughout the network. With access to linked transaction information from many institutions, AML specialists – potentially including

regulators – could gain powerful tools for identifying patterns of money laundering between banks in real- or near-real-time [20].

6.4 Trade Confirmation and Affirmation

Trade affirmation/confirmation is generally an OTC concept, as OTC transactions are mostly bilateral in nature and therefore they need to be confirmed by both the counter-parties (legally). Affirmation mostly relates to alleging the trade which means agreeing on the trade economics by both the counter-parties and once the trade is affirmed, trade confirmations are exchanged (which could be a paper confirm exchanged over email/fax or it could be electronic confirm exchanged over 3rd party platforms like Mark it) which act as a trade evidence or legal contract and specifies all the terms of the trade. Once both the counter-parties match the trade terms as specified in the trade confirmations the trade is then called as "Confirmed" and in case there is mismatch on any of the trade terms then the trade is called as "Disputed" until discrepancies are resolved. The confirmation/affirmation process refers to the transmission of messages among broker-dealers, institutional investors, and custodian banks regarding the terms of a trade executed for the institutional investor. Because the trades of institutional investors involve larger sums of money, larger amounts of securities, more parties, and more steps between order entry and final settlement, institutional trades are usually more complex than retail transactions [21].

6.4.1 Confirmation Using the ID System

The typical components of the "customer-side" settlement of an institutional trade under the current SRO confirmation rules are illustrated in Figure 8.

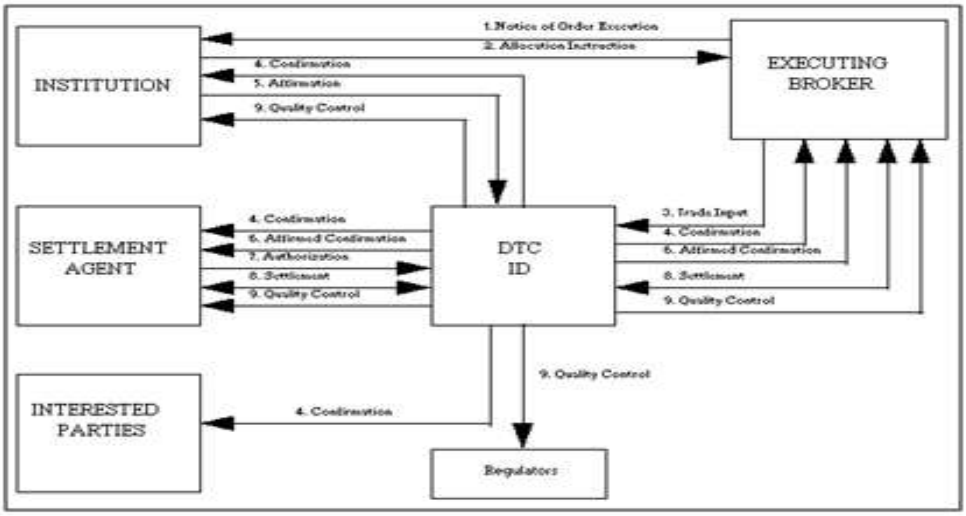

Figure 8. Current ID System

Typically, an institutional trade will begin with the institution's investment manager placing an order with the broker-dealer. After the broker-dealer executes the trade, the broker-dealer will advise the institution of the execution details. This is commonly referred to as giving notice of execution (step 1 of Figure 8). The institution then advises the broker-dealer as to how the trade should be allocated among its accounts (step 2 of Figure 8). The broker-dealer then submits the trade data to DTC (step 3 of Figure 8).

Next, DTC adds the transaction to the ID system's trade database, assigns an ID control number, and forwards an electronic confirmation to the institution, the broker-dealer, the institution's settlement agent, and other interested parties (e.g., trustees, plan administrators, or correspondent banks) (step 4 of Figure 8). The institution reviews the confirmation for accuracy. If accurate, the institution or its designated affirming agent affirms the trade through the ID system (step 5 of Figure 8). DTC then generates an affirmed confirmation and sends it to the broker-dealer and to the institution's settlement agent (step 6 of Figure 8).

At this point, the trade is sent into DTC's settlement system (i.e., the ID system is not a settlement system in that no money or securities move through it) and must be authorized by the party obligated to deliver the securities (i.e., the selling party) institution or the settlement agent before settlement occurs (steps 7 and 8 of Figure 8). "Quality Control" involves DTC's monitoring and production of various reports for regulators and ID system users which show such things as when a confirmation was sent and the affirmation was received (step 9 of Figure 8).

VII.AAA (AUTHENTICATION – AUTHORIZATION – ACCOUNTING)

The administrator can take an access to a router or a device through console but it is very inconvenient if he is sitting far from the place of that device.Therefore, eventually he has to take remote access to that device. However, as the remote access will be available by using an IP address therefore it is possible that an unauthorized user can take access using that same IP address therefore for security measures, we have to put authentication. In addition, the packets exchange between the device should be encrypted so that any other person should not be able to capture that sensitive information. Therefore, a framework called AAA is used to provide that extra level of security. AAA is a standard based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization) and capture the actions performed while accessing the network (through accounting) [24].

- **Authentication**

Process by which it can be identified that the user, which want to access the network resources, valid or not by asking some credentials such as username and password. Common methods are to put authentication on console port, AUX port or vty lines. As a network administrator, we can control how a user is authenticated if someone wants to access the network. Some of these methods include using the local database of that device (router) or sending authentication request to an external server like ACS server. To specify the method to be used for authentication, default or customized authentication method list are used.

- **Authorization**

It provide capabilities to enforce policies on network resources after the user has gain access to the network resources through authentication. After the authentication is successful, authorization can be used to determine that what resources is the user allowed to access and the operations that can be performed. For example, if a junior network engineer (who should not access all the resources) wants to access the device then the administrator can create a view which will allow particular commands only to be executed by the user (the commands that are allowed in the method list). The administrator can use authorization method list to specify how the user is authorized to network resources i.e through local database per ACS server.

- **Accounting**

It provide means of monitoring and capturing the events done by the user while accessing the network resources. It even monitors how long the user has an access to the network. The administrator can create an accounting method list to specify what should be accounted and to whom the accounting records should be send.

AAA can be implemented by using the local database of the device or by using an external ACS server.

- **local database**

If we want to use the local running configuration of the router or switch to implement AAA, we should create users first for authentication and provide privilege levels to user for Authorization.

- **ACS server**

This is the common method used. An external ACS server is used (can be ACS device or software installed on Vmware) for AAA on which configuration on both router and ACS required. The configuration include creating user, separate customized method list for authentication, Authorization and Accounting. The client or Network Access Server (NAS) sends authentication request to ACS server and the server takes the decision to allow the user to access the network resource or not according to the credentials provided by the user.

7.1 Benefits of using AAA security

AAA security enables mobile and dynamic security. Without AAA security, a network must be statically configured in order to control access. IP addresses must be fixed, systems cannot move, and connectivity options must be well defined. The proliferation of mobile devices and the diverse network of consumers with their varied network access methods generates a great demand for AAA security.

AAA security is designed to enable you to dynamically configure the type of authorization and authentication you want by creating a method list for specific services and interfaces. AAA security means increased flexibility and control over access configuration and scalability, access to standardized authentication methods such as RADIUS, TACACS+, and Kerberos, and use of multiple backup systems. The increase of security breaches such as identity theft, indicate that it is crucial to have sound practices in place for authenticating authorized users in order to mitigate network and software security threats [25].

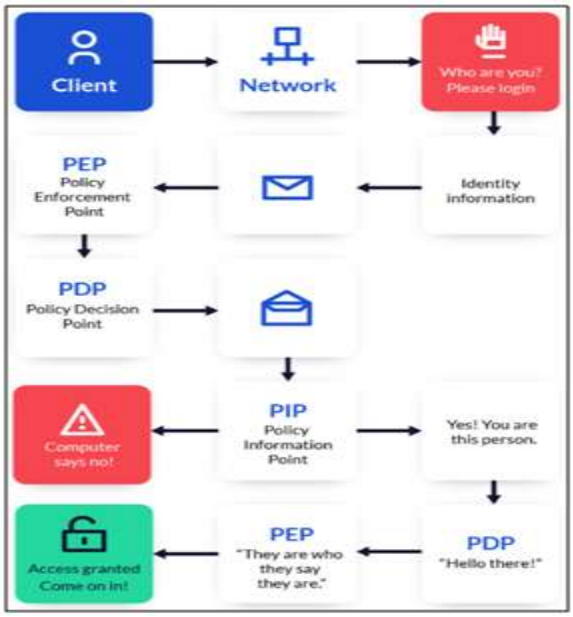

Figure 9. AAA security in action

VIII. DUAL AUTHENTICATION

8.1 Multi-factor authentication

Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are. A good example of two-factor authentication is the withdrawing of money from an ATM; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out. Two other examples are to supplement a user-controlled password with a one-time password (OTP) or code generated or received by an authenticator (e.g. a security token or smartphone) that only the user possesses.

Two-step verification or two-step authentication is a method of confirming a user's claimed identity by utilizing something they know (password) and a second factor other than something they have or something they are. An example of a second step is the user repeating back something that was sent to them through an out-of-band mechanism. On the other hand, the second step might be a six-digit number generated by an app that is common to the user and the authentication system [22].

8.2 Two-Factor Authentication(2FA)

Two-factor authentication (2FA) is a second layer of security to protect an account or system. Users must go through two layers of security before being granted access to an account or system. 2FA increases the safety of online accounts by requiring two types of information from the user, such as a password or PIN, an email account, an ATM card or fingerprint, before the user can log in. The first factor is the password; the second factor is the additional item.

2FA is designed to prevent unauthorized users from gaining access to an account with nothing more than a stolen password. Users may be at greater risk of compromised passwords than they realize, particularly if they use the same password on more than one website. Downloading software and clicking on links in emails can also expose an individual to password theft.

Despite the slight inconvenience of a longer log-in process, security experts recommend enabling 2FA wherever possible: email accounts, password managers, social media applications, cloud storage services, financial services, blogging platforms and more. Apple account holders, for example, can use 2FA to ensure that accounts can only be accessed from trusted devices. If a user tries to log in to their iCloud account from a

different computer, the user will need the password, but also a multi-digit code that Apple will send to one of the user's devices, such as their iPhone.

2FA is not just applied to online contexts. 2FA is also at work when a consumer is required to enter their zip code before using their credit card at a gas pump or when a user is required to enter an authentication code from an RSA SecurID key fob to log in remotely to an employer's system.

While 2FA does improve security, it is not foolproof. Hackers who acquire the authentication factors can still gain unauthorized access to accounts. Common ways to do so include phishing attacks, account recovery procedures and malware. Hackers can also intercept text messages used in 2FA. Critics argue that text messages are not a true form of 2FA since they are not something the user already has but rather something the user is sent, and the sending process is vulnerable. Instead, the critics argue that this process should be called two-step verification. Some companies, such as Google, use this term. Still, even two-step verification is more secure than password protection alone. Even stronger is multi-factor authentication, which requires more than two factors before account access will be granted [23].

IX. BIOMETRIC AUTHENTICATION

Biometric authentication is a form of security that measures and matches biometric features of a user to verify that a person trying to access a particular device is authorized to do so. Biometric features are physical and biological characteristics that are unique to an individual person and can be easily compared to authorized features saved in a database. If the biometric features of a user trying to access a device match the features of an approved user, access to the device is granted. Biometric authentication can also be installed in physical environments, controlling access points like doors and gates. Common types of biometric authentication are increasingly being built into consumer devices, especially computers and smartphone. Biometric authentication technologies are also being used by governments and private corporations in secure areas, including at military bases, in airports, and at ports of entry when crossing national borders [26].

9.1 Common Types of Biometric Authentication

- **Fingerprint Scanners**

Fingerprint scanners, the digital version of old-fashioned ink and paper fingerprinting, rely on recording the unique patterns of swirls and ridges that make up an individual's fingerprints. Fingerprint scanners are one of the most common and accessible modes of biometric authentication, though consumer-grade versions, such as those found on smart phones, still have the potential for false positives. Newer versions of fingerprint scanning move beyond fingerprint ridges and below the skin to assess the vascular patterns in people's fingers, and may prove more reliable. Despite their occasional inaccuracy, fingerprint scanners are among the most popular and utilized biometric technologies for everyday consumers.

- **Facial Recognition**

Facial recognition technology relies on matching dozens of different measurements from an approved face to the face of a user trying to gain access, creating what are called faceprints. Similar to fingerprint scanners, if a sufficient number of measurements from a user match the approved face, access is granted. Facial recognition has been added to a number of smart phones and other popular devices, though it can be inconsistent at comparing faces when viewed from different angles, or when trying to distinguish between people who look similar, such as close relatives.

- **Voice Identification**

Vocal recognition technologies measure vocal characteristics to distinguish between individuals. Like facial scanners, they combine a number of data points and create a voiceprint profile to compare to a database. Rather than "listening" to a voice, voice identification technologies focus on measuring and examining a speaker's mouth and throat for the formation of particular shapes and sound qualities. This process avoids the security issues that could be caused by attempts to disguise or imitate a voice, or by common conditions such as sickness or time of day that might change the audial qualities of a voice to a human ear. The words a user speaks to access a voice-protected device may also be somewhat standardized, serving as a sort of password and making the comparison of approved voiceprints to a user's unique voiceprint easier, as well as foiling particular ways to bypass voiceprint comparison, such as recording an authorized user saying something unrelated.

- **Eye Scanners**

Several types of eye scanners are commercially available, including retina scanners and iris recognition. Retina scanners work by projecting a bright light towards the eye that makes visible blood vessel patterns, which can then be read by the scanner and compared to approved information saved in a database. Iris scanners operate similarly, this time looking for unique patterns in the colored ring around the pupil of the eye. Both types of eye

scanners are useful as hands-free verification options, but can still suffer inaccuracies if subjects wear contact lenses or eye glasses. Photographs have also been used to trick eye scanners, though this method is likely to become less viable as scanners become more sophisticated and incorporate factors like eye movement into their verification schemes.

Biometric authentication methods may also serve as a form of two-factor authentication (2FA) or multi-factor authentication (MFA), either by combining multiple biometric patterns or in conjunction with a traditional password or secondary device that supplements the biometric verification. Biometrics do still face some obstacles to widespread consumer adoption. Certain biometric technologies are very complicated to program, install, and use, and may require educating consumers to assure they are used correctly. Security updates are critical to ensure that biometric data and functions continue to work properly. Error rates are still a problem with some biometric measures as well, and frustration with errors may make consumers less likely to adopt biometrics into everyday usage patterns. Despite these risks, biometric authentication is increasingly gaining acceptance across a number of industries that rely on security, and are likely to continue becoming more common in consumer-grade devices and applications [26].

9.2 Biometrics Authentication pros and cons

It seems like biometrics are everywhere in Identity and Access Management (IAM): fingerprints, facial recognition, voice recognition, and more. Nevertheless, are biometrics really the cure for secure authentication? Like all technologies, this one has pros and cons. In this topic, we will examine the good, the bad, and the ugly side of biometrics for authentication [27].

- **Biometrics Pros**

There is a reason biometrics are increasingly popular in identity management: they are harder to fake. Authentication has evolved. It started with what you know, a username and password, for instance. However, it is easy to steal or trick people into giving up the information they know. So, authentication techniques moved to what you have: a cell phone in hand or a card key. This, combined with what you know, made users more secure.

However, biometric authentication might not be secure enough. Cyber criminals could still obtain or fake the devices users had. What you are, demonstrated through biometrics, is the next stage for authentication. And it's true, it's much harder to fake someone's voice, fingerprint, iris, etc. On top of that, biometric authentication is often easier for users: you carry you around everywhere. Putting a finger over a keypad or looking into an eye scanner is not tough to do. Some systems, such as facial recognition, can even authenticate without the user consciously making a gesture. Simply move into a room or sit in front of your computer and you're authenticated via facial recognition, for instance. Best of all, users are not going to forget their fingers or eyes like they do passwords or physical keys. You will not have all those password reset tickets piling up at your help desk with biometrics.

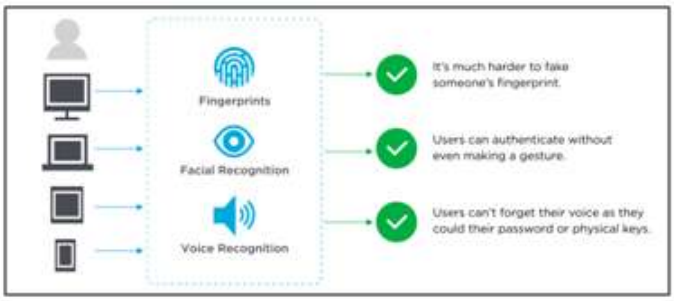

Figure 10. The good part about biometrics for security

- **Biometrics Cons**

So, what is the downside? First, while biometrics are generally more secure, they are not foolproof. For example, smartphone fingerprint scanners often rely on partial matches, and researchers have found that it is possible to create "master prints" that match partials well enough to give access to a large number of user accounts. Researchers have also demonstrated the ability to create fake fingerprints from high quality prints left behind. Others have found ways to use photos or 3D prints to trick iris scanners or facial recognition systems. Sometimes the issue is that the system can be hacked as much as that it too often fails to recognize a valid user: someone wearing different makeup or new glasses, the voice of a user who is sick or has just woken up.

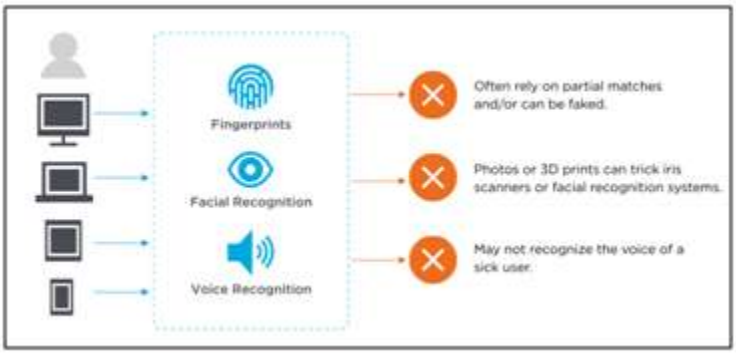

Figure 11. The bad part about biometrics for authentication

So, it's no surprise then that quality biometric solutions cost more. In fact, 67% of IT professionals cite cost as the biggest reason for not adopting biometric authentication. There are hidden costs, too, with 47% of those surveyed reporting a need to upgrade systems in order to support a shift to biometrics. This is why many companies considering adoption of biometrics are focused on using it as only one component of multi-factor authentication (MFA). MFA can require a biometric factor and a non-biometric one. If one authentication factor is hacked, the user's account is still secured by the other. In addition, with tools like risk-based authentication, MFA can adapt to challenge users when the probability of cybercrime is high and reduce the barriers to entry when it is low.

If you have been following developments in biometrics, you are probably aware of the ethical concerns surrounding many forms of biometrics. One of them involves bias. Facial recognition systems may not recognize POC or non-CIS gender people as accurately. In addition, learning systems for biometrics have too often been based primarily on white or white male photos, creating a clear bias that results in difficulty recognizing people in the broader population. Additionally, there are fears about how biometric data could be used. Who has access to images used for facial recognition, fingerprints, or voice patterns? Is it acceptable for companies to sell or provide their biometric data to others, such as law enforcement, immigration enforcement, or repressive foreign governments? For businesses, another ugly side of biometric data is the storage issue. Where biometric data is stored, it must be stored securely. Because if it has hacked, there is no going back—a person cannot change their fingerprint or their iris. That means losing your biometric data presents a permanent risk of hacking for the rest of your life.

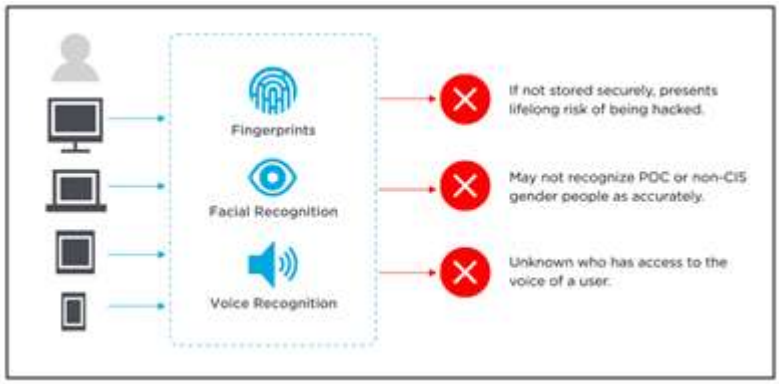

Figure 12. The ugly side of biometrics

Companies that choose to store employees' or customers' biometric data are taking on a big financial and ethical responsibility. This is one reason to consider on device storage: where the biometric data is stored on the device that authenticates the user, like the user's smartphone or computer. This gives the user control over the data and it also restricts its location to a local device, reducing the likelihood of a cyber-criminal gaining access to large sets of biometric data through a single breach. While there are many sides to the biometric debate, one thing is for certain: the technology is here to stay. Despite the bad and the ugly side of biometrics, the good side is outweighing them, enough that companies are expected to continue adopting biometrics for authentication [27].

XI. FORMAL DATABASES LINKAGE

A government database collects information for various reasons, including climate monitoring, securities law compliance, geological surveys, patent applications and grants, surveillance, national security, border control, law enforcement, public health, voter registration, vehicle registration, social security, and statistics [28].

10.1 Open Government Data

Open Government Data (OGD) is a philosophy- and increasingly a set of policies - that promotes transparency, accountability and value creation by making government data available to all. Public bodies produce and commission huge quantities of data and information. By making their datasets available, public institutions become more transparent and accountable to citizens. By encouraging the use, reuse and free distribution of datasets, governments promote business creation and innovative, citizen-centric services [29].

10.2 OECD Open Government Data project

OGD can pose some tricky questions for governments, such as who will pay for the collection and processing of public data if it is made freely available? What are the incentives for government bodies to maintain and update their data? In addition, what data sets should be prioritized for release in order to maximize public value? Steps are therefore needed to develop a framework for cost and benefit analysis, to collect data, and to prepare case studies demonstrating the concrete benefits - economic, social, and policy - of opening government data. The OECD Open Government Data project aims to progress international efforts on OGD impact assessment. The mapping of practices across countries will help establish a knowledge base on OGD policies, strategies and initiatives and support the development of a methodology to assess the impact and creation of economic, social and good governance value through OGD initiatives [29].

10.2.1 Methodology

The methodology was first put forward in the Working Paper *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*, and is being validated in collaboration with government representatives from OECD countries as well as non-government stakeholders [29].

10.2.2 OECD OGD analysis

- Business Information.
- Registers.
- Patent and Trademark Information.
- Public Tender Databases.
- Geographic Information.
- Legal Information.
- Meteorological Information.
- Social Data.
- Transport Information.

10.3 Linked Open Data in Government benefits

Linked Open Data makes the most sense in tough economic times. She states, "Back in April 2011, I wrote about the US Environmental Protection Agency's efforts to publish facilities data that was locked up in a proprietary database and made available in as Web service via the Facilities Registry System. EPA like many agencies provides a tremendous amount of content via Web services to their respective Web sites. But the information they provide is often: (1) hard to find; (2) difficult to navigate; and (3) one cannot get hold of the raw data." [30]

The semantic web and linked data technologies show great promise for organizing and integrating information on the Web. As custodians of bibliographic information, libraries are ideally placed to play a leading role by providing authoritative information in this domain. The semantic web and linked data have been hyped as the solution for everything from integrating legacy data sets and improving search through to working with big data problems. However, the vision of the semantic web is a long way from being realized. This paper explores how linked data is being used in libraries and related institutions in Australia and globally. Examples are given of linked data in practice and what makes some projects more successful than others [31].

10.3.1 Implications for best practice

- Exposing linked data for collections can enhance search results and make resources easier to find.
- Linked data can be incorporated into online content relatively easily using well-known vocabularies.
- Linked data projects work best within a defined community of users.
- Many linked data tools are difficult to use and are not ready for widespread adoption, but this is changing.

- Linked data show great promise and will be an integral part of the information landscape in the years to come.

10.3.2 Linked data: current usage

Despite linked data and the semantic web having garnered much publicity and discussion, there are still relatively few concrete examples that demonstrate how implementing linked data can benefit an institution. In some respects, there is a chicken-and-egg problem with linked data. One of the main promises of linked data is the increased value that the links between entities can provide; however, if there are few other data sets with which the data can link, then this benefit is not realized. Other barriers to adopting linked data include technological complexity, risk aversion, economic constraints, politics or system constraints (Martin 2012). Even so, the projects that have implemented linked data give a glimpse into what might be possible when a critical mass of data is reached [31].

10.4 Linkage Data

The Web is evolving from a "Web of linked documents" into a "Web of linked data". However, in many cases, data is still locked in information systems and databases and is represented using different, usually not aligned, vocabularies and schemas. In Europe, access to government data, and the possibility to freely use it, In Europe, access to government data, and the possibility to freely use it, is seen as an enabler for Open Government and a goldmine of unrealized economic potential. Open Data usually refers to public records (e.g. on transport, infrastructure, education, and environment) that can be freely used and redistributed by anyone - either for free or at marginal cost. But opening-up data, e.g. in Open Data portals, often happens in an adhoc manner, and in many cases thousands of datasets is published without adhering to commonly-agreed data and metadata standards and without reusing common identifiers.

Hence, a fragmented data-scape is created, where finding, reusing, integrating and making sense of data from different sources is a real challenge. Linked Data can respond to these challenges and can be an enabler of eGovernment transformation, leading to smarter and more efficient government services and applications, and fostering creativity and innovation in the digital economy [32].

"Linked data is a set of design principles for sharing machine-readable data on the Web for use by public administrations, business and citizens." The four design principles of Linked Data put forward by Tim Berners-Lee in 2006.

- Use Uniform Resource Identifiers (URIs) to uniquely identify things (data entities).
- Use HTTP URLs, corresponding to these URIs, so that information can be retrieved.
- Provide metadata using open standards such as RDF.
- Include links to related URIs, so that people can discover more things.

10.5 Looking at the Future of the Linkage Data

At present most information, systems store data in relational databases and make its exchange possible according to well-defined structures, usually using XML schemas. Sharing data according to some sort of schema has been the technological paradigm of the last decades because it enables computer programmes to process data efficiently. However, when these schemas evolve, information systems using them (as data providers or data consumers) need to be adapted accordingly. Over time maintaining these schemas requires significant effort and can be quite inflexible – especially schemas requires significant effort and can be quite inflexible – especially when the pace of change is high.

This is a key reason for the emergence of a new paradigm for data exchange centered around the Resource Description Framework (RDF). According to its publisher, W3C, "RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed". In RDF, data is organized in graphs around subject-predicate-object statements and can be queried using SPARQL. These and other related standards are the foundations of Linked Data. The ISA programme of the European Commission is attentive to this paradigm shift and is running an action on semantic interoperability. This action is putting these standards and technologies together for improving eGovernment, at EU-wide level. The results of this action will then be re-used by public administrations in the member states to implement open data policies, to open up their base registries and to ease data exchange across borders [32].

10.6 REAL ID Act; ID Future

The REAL ID Act establishes minimum-security standards for license issuance and production and prohibits Federal agencies from accepting for certain purposes driver's licenses and identification cards from states not meeting the Act's minimum standards. The purposes covered by the Act are accessing Federal facilities, entering nuclear power plants, and, boarding federally regulated commercial aircraft. The Department of

Homeland Security (DHS) announced on December 20, 2013 a phased enforcement plan for the REAL ID Act (the Act), as passed by Congress, that will implement the Act in a measured, fair, and responsible way.
Secure driver's licenses and identification documents are a vital component of our national security framework. The REAL ID Act, passed by Congress in 2005, enacted the 9/11 Commission's recommendation that the Federal Government "set standards for the issuance of sources of identification, such as driver's licenses." The Act established minimum-security standards for license issuance and production and prohibits Federal agencies from accepting for certain purposes driver's licenses and identification cards from states not meeting the Act's minimum standards. The purposes covered by the Act are accessing Federal facilities, entering nuclear power plants, and, no sooner than 2016, boarding federally regulated commercial aircraft.
DHS is committed to enforcing the REAL ID Act in accordance with the phased enforcement schedule and regulatory timeframes and is not inclined to grant additional extensions to any states that are not both committed to achieving full compliance and making substantial and documented progress in satisfying any unmet requirements. It has been 12 years since the REAL ID Act was passed and half of all the states have already met the REAL ID minimum standards. It is time that the remaining jurisdictions turn their commitments to secure identification into action [33].

10.6.1 REAL ID Enforcement

Almost all USA's states are compliant with the REAL ID Act. Federal agencies can accept driver's license and identification cards from the state. Secure driver's license and identification documents are a vital component of a holistic national security strategy. Law enforcement must be able to rely on government-issued identification documents and know that the bearer of such a document is who he or she claims to be. REAL ID is a coordinated effort by the states and the Federal government to improve the reliability and accuracy of state-issued identification documents, which should inhibit terrorists' ability to evade detection by using fraudulent identification [34].

XII. CONCLUSION

Securing electronic identity for citizens improves public service such as electronic passports, national electronic election cards, social security cards, electronic driving licenses. The high security access cards and records must be protected as well such as credentials and medical health records, banking debit and credit cards and its related transactions. This research paper has provided a study on the application of national electronic identity cards "Unicard" which is a transformation and migration from paper-based identity cards to electronic national IDs, from silo to fully integrated system among different services. Unicard system is coming from the need for increased security, the need to get access to eServices in a secure way, the need to reduce administration costs. It will decrease identity theft, improve administrative efficiency and better control illegal immigration, and terrorism. It will also allow citizens to have access to eServices in a convenient way and to have a stronger protection of their identity in the internet [35].

ACKNOWLEDGMENT

The authors would like to thank ***AhramCanadianUniversity(ACU)***, ***Egypt*** and ***DeVryUniversity***, ***USA*** for their support to introduce this research paper in a suitable view and as a useful material for researchers. The authors also would like to thank their colleagues who provided insight and expertise that greatly assisted the research.

REFERENCES

[1]. Hussam Elbehiery, Khaled Elbehiery, "National Identity Evolution" IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 10, pp.1-12, India, ISSN: 2348 – 7968, October 2019.
[2]. Serene S Koh, "National Identity and Young Children: A Comparative Study of 4th and 5th Graders in Singapore and the United States," A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Education) in the University of Michigan, 2010.
[3]. "Why is national identity important," Palo Alto Networks, Prisma™ Public Cloud. End cloud security anxiety, Quora Inc. © 2019, May 12, 2018. [Online] Available: https://www.quora.com/Why-is-national-identity-important
[4]. Margaret Rouse, "National identity card," TechTarget, Copyright 2000 - 2019. [Online] Available: https://searchsecurity.techtarget.com/definition/national-identity-card
[5]. "Appointment Booking (Territory-wide Identity Card Replacement Exercise)," Immigration Department, The Government of the Hong Kong Special Administrative Region. [Online] Available: https://www.smartid.gov.hk/en/
[6]. "Personal Data Protection," Immigration Department, The Government of the Hong Kong Special Administrative Region. [Online] Available: https://www.smartid.gov.hk/en/Persona-Data-Protection/index.html
[7]. Electronic Privacy Information Center (epic.org): Real ID Implementation Review: Few Benefits, Staggering Costs, Washington, D.C., USA, May 2008.
[8]. Yazeed Alkhurayyif, "National ID Cards," International Journal of Computing Science and Information Technology, 2013, Vol.1 (02) 44 – 48, ISSN: 2278-9669, April 2013 (http://ijcsit.org)
[9]. Mehdi Punjwani, "Pros and cons of using credit cards," Moneysupermarket.com Ltd 2020, 15 March 2019. [Online] Available: https://www.moneysupermarket.com/credit-cards/advantages-and-disadvantages/

[10]. OppLoans.com, "Meet Your Credit Character," The OppLoans Guide to Understanding Your Credit, Credit Report and Credit Score. [Online] Available: https://www.opploans.com/content/credit-ebook/part-credit-concept/offers-credit-cards/advantages-disadvantages-credit-cards/

[11]. Informal economy. [Online] Available: https://en.wikipedia.org/wiki/Informal_economy

[12]. Rafael La Porta and Andrei Shleifer, "Five facts about informal economies," Chris Blattman, International development, economics, politics, and policy, 9 June 2014. [Online] Available: https://chrisblattman.com/2014/06/09/five-facts-informal-economies/

[13]. Money laundering. [Online] Available: https://en.wikipedia.org/wiki/Money_laundering

[14]. James Chen, "Money Laundering," Investopedia, Laws & Regulations, Crime & Fraud, Jun 25, 2019.[Online] Available: https://www.investopedia.com/terms/m/moneylaundering.asp

[15]. Will Kenton, "Anti Money Laundering (AML)," Investopedia, Laws & Regulations, SEC & Regulatory Bodies, Sep 10, 2019.[Online] Available: https://www.investopedia.com/terms/a/aml.asp

[16]. International Compliance Association (ICA), "What is money laundering?," 18 January 2020, UK.[Online] Available: https://www.int-comp.org/careers/your-career-in-aml/what-is-money-laundering/

[17]. Jacquelyn C.A. Meshelemiah and Raven E. Lynch, "The Cause and Consequence of Human Trafficking: Human Rights Violations," Creative Commons Attribution-NonCommercial 4.0 International License, COLUMBUS, PB PRESSBOOKS, Montreal, Quebec, Canada. December 2019. [Online] Available: https://ohiostate.pressbooks.pub/humantrafficking/

[18]. United Nations Office on Drugs and Crime (UNODC), "Drug trafficking," Copyright©2020 UNODC, All Rights Reserved, Legal Notice. [Online] Available: https://www.unodc.org/unodc/en/drug-trafficking/index.html

[19]. Top Image Systems (TIS), "Trade Finance," August 10, 2016. [Online] Available: https://www.topimagesystems.com/solutions/banking-process-automation/trade-finance-document-processing/

[20]. Bill Camarda, "Improving "Know Your Customer" Processes for Trade Finance and Other Purposes," © 2019 American Express Company, USA, January 2020. [Online] Available: https://www.americanexpress.com/us/foreign-exchange/articles/kyc-processes-for-trade-finance/

[21]. Quora Blog, "What is the difference between trade confirmation and affirmation." [Online] Available: https://www.quora.com/What-is-the-difference-between-trade-confirmation-and-affirmation

[22]. Multi-factor authentication. [Online] Available:https://en.wikipedia.org/wiki/Multi-factor_authentication

[23]. Will Kenton, "Two-Factor Authentication (2FA)," Investopedia, Laws & Regulations, Cybersecurity, May 9, 2019. [Online] Available: https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp

[24]. GeeksforGeeks, "Computer Network | AAA (Authentication, Authorization and Accounting)." [Online] Available:https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/

[25]. Serena Reece, "What is AAA security? An introduction to authentication, authorization and accounting," Codebots Blog, Nov 27th, 2018. [Online] Available:https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting

[26]. Iovation Inc., A TransUnion Company, "Biometric Authentication." [Online] Available: https://www.iovation.com/topics/biometric-authentication

[27]. OneLogin, Inc., "Biometric authentication, the good, the bad, and the ugly." [Online] Available: https://www.onelogin.com/learn/biometric-authentication

[28]. Government database. [Online] Available:https://en.wikipedia.org/wiki/Government_database

[29]. Organisation for Economic Co-operation and Development (OECD), "Open Government Data," Directorate for Public Governance, Digital government. [Online] Available:https://www.oecd.org/gov/digital-government/open-government-data.htm

[30]. A.R. Guess, "Benefits of Linked Open Data in Gov and Beyond," January 31, 2012. [Online] Available:https://www.dataversity.net/benefits-of-linked-open-data-in-gov-and-beyond/#

[31]. Peter Neish, "Linked data: what is it and why should you care?," The Australian Library Journal , Volume 64, Issue 1, Pages 3-10, 2015. Published online: https://doi.org/10.1080/00049670.2014.974004

[32]. European Commission, "How Linked Data is transforming eGovernment," 12 December 2011. [Online] Available:https://ec.europa.eu/commission/presscorner/detail/en/IP_11_1524

[33]. Homeland Security, "Real ID," USA, Last Published Date: July 5, 2019. [Online] Available:https://www.dhs.gov/real-id

[34]. Homeland Security, "REAL ID Enforcement: Colorado," USA, Last Published Date: September 5, 2019. [Online] Available:https://www.dhs.gov/real-id/colorado

[35]. Elwatannews, ""The common card of the citizen".. A civilizational transition that takes 15 years," Sunday 15th April 2018. [Online] Available:https://www.elwatannews.com/news/details/3275731

[36]. Youm7 News, "6 parliamentary recommendations for the speedy integration of the informal economy," Thursday 9th January 2020. [Online] Available: https://www.youm7.com/story/2020/1/9/

[37]. Egypt Today News, "20 e-government services to be provided in 2019," Wed, Dec. 26, 2018. [Online] Available: https://www.egypttoday.com/Article/2/62599/20-e-government-services-to-be-provided-in-2019

Hussam Elbehiery"Unicard; National Identity Evolution " *The International Journal of Engineering and Science (IJES)*, 9(01) (2020): 84-101.