A STUDY

Next Generation Identity Framework

The proposed Identity Framework is designed primarily to address a number of issues with current identity systems.

Govind Yadav
yadavgovind@hotmail.com
1st October 2023

Contents

Abstract

Globally, identity fraud costs people, businesses, and governments more than USD 1 trillion each year. Our goal is to create a secure physical identity framework that would offer fool proof, multi-purpose physical and real-world identities that may be used as national identity systems for many nations in order to resist this threat. This document's goal is to present the distinctive idea behind the adaptable Next Generation Identity Framework. The impact of identity fraud is thoroughly examined in this study, along with the weaknesses of the physical identity systems that are now in use. Finally, the framework is introduced, along with certain distinctive and ground-breaking characteristics.

Introduction

To establish the scene, let me share a story from my own life. I requested a publicly trusted document signing certificate a while back. Face-to-face verification was necessary, and I had to show my biometric passport as part of identity vetting. The Certifying Authority (CA), which is well known for its rigorous verification processes, thoroughly checked my passport before issuing the digital certificate. However, there was no handheld passport reader, which would have provided considerably more reliable validation of the digital credentials stored inside the chip as utilised by airport border agents. It is not practical for all relying parties to purchase hardware card readers for various forms of identification. Imagine that I had a stolen passport and, using the highest level of accuracy, had replaced the victim's photo with mine. This is definitely a possibility in the modern world. With the victim's information on it and based on a false physical identification, the outcome would be a completely authentic digital certificate (online identity)! Now, a fraudster can perform numerous online scams using such an online persona. There are other comparable government-issued physical identities (such as a driver's licence or voter identification card) that are relatively less secure but serve as KYC foundation for many organizations such as financial institutions, government agencies etc. These identities offer visual identification (in the absence of hardware card readers), and are all vulnerable to such attacks.

What this framework is all about

The proposed Identity Framework is designed primarily to address a number of issues with current identity systems. It also offers a number of additional advantages that are not currently available. Most crucially, this ID system will provide a very high degree of visual identity assurance without the use of a card reader or network access. Both citizens and governments will receive enormous advantages from the system. This framework can be efficiently used by numerous government agencies and private businesses in a nation to authenticate and authorise (A&A) both domestic and foreign residents. The establishment of a secure national ID system, increased surveillance, cyber security aimed at reducing terrorist and anti-social propaganda on social media, improved eGovernance, a highly effective and secure electronic voting system, the control of illegal immigration, an increase in GDP through institutionalised trust etc. would be key benefits to the governments. Features like "User Profiling," which by itself can, minimise significant fraud, financial inclusion, reduced corruption, robust 2FA to protect financial transactions, social media, etc. are all examples of social advantages for citizens.

We will raise the bar for creativity with a special fusion of fresh creations and re-creations and by seamlessly blending cutting-edge technologies.

Defining Terms

Despite the fact that these categories are well defined, I still want to distinguish between "online" and "real world/physical" identities. We have logical access to a variety of online services in the virtual world via websites, apps, servers, etc., and identities are typically formed by usernames, customer IDs, employee IDs, etc. Typical identity authentication involves passwords. There are two-factor authentication methods, including PKI, several types of OTP, secure browsers, mobile push notifications, etc., for enhanced identity authentication. Real-world or physical IDs, such as a passport, driver's licence, voter card, etc., identify a person in the real world where we need physical access to buildings, premises, countries, services, etc.

Additionally, it is important to distinguish between identity theft and identity fraud. Identity theft happens when a victim's identity is stolen or compromised. Access to a victim's personally identifiable information (PII) through other sources is sufficient for identity theft to occur without the need for a fraudster to physically steal the victim's ID card. Identity fraud occurs when a victim's identity is actually used fraudulently to open a bogus bank account, obtain services, claim income or tax benefits, etc. Last but not least, identity fraud does not always require the theft of the victim's personal information; instead, the perpetrators may utilise entities that do not exist at all, such as false names, forged or falsified identification documents, or they may even lie about their own age to conceal their genuine identities.

Please Note:

A) The focus of this concept document is solely on "what" this framework will accomplish, not "how" it will accomplish it. The latter is more concerned with design and specification(s), which are outside the purview of this paper.

B) This is not a standard identity and access management or governance solution for controlling access to user identities across numerous third-party endpoints and target applications.

The impact of identity fraud

Identity fraud can wreak havoc on societies and economies, and this crime is often committed to facilitate other crimes such as age deception, organised crime, credit card or document fraud, money laundering, false insurance claims, employment fraud, illegal health care access, drugs trafficking, bullying, damaging people's reputations, theft of public money, property, or records; embezzlement; false statements in connection with the acquisition of a firearm; fraud and false statements; mail, bank, and wire fraud. Such fraud also contributes towards specified nationality and citizenship, relating to wilfully failing to leave the country after deportation and creating a counterfeit alien registration card, and various other immigration offences like passport and visa violations, obtaining customer information by false pretences, specified terrorism violations, etc. Non-financial loss to individuals occurs due to legal consequences, mental, emotional consequences and learned helplessness consequence. Non-financial costs to businesses due to Reputational damage, loss of customer confidence, disturbing internal operational activities and diminishing productivity and physical health consequences. These frauds affect not only individuals, business and the nation's economy, but they are also a national security threat.

Consider some facts

As per European Commission Study on online identity theft and identity-related crime (Final Report), in the period 2017- 2019, following statistics were observed:

A **148 million** EU citizens reported having been targets or victims of different forms of **phishing**. The total direct losses to citizens as a result of phishing could be an estimated **EUR 27.0 billion**.

B **32 million citizens** experienced or had been a victim of **bank card or online banking fraud**. The total direct losses accruing to EU citizens as a result of bank card/ payment fraud could be estimated between **EUR 882.0 million and EUR 2.4 billion**.

C With 31% of global attacks in 2020 occurring in the European region (up from 21% in 2019), Europe became the top-attacked geographical region in the world in 2020

D Estimated indirect costs/losses to victims (individuals) as a result of identity theft is EUR 31 billion.

E The cost of credential theft is about **EUR 400,000** per company.

F **129 million citizens** were victims of **malware and 49 million citizens** were targets or victims of **hacking**.

G **28 million citizens** experienced **impersonation** and total direct losses are an estimated **EUR 1.0 billion.**

H Data theft attacks detected by the private sector increased by 160% in 2020 compared to 2019.

Note

These are highly conservative figures since the EU survey was limited by a low response rate of national authorities to online surveys and interview requests and difficulties in identifying relevant case law. In 2019, only 28% of victims of identity theft in the European Union (EU) contacted the police, a smaller share than in 2018. If 100% fraud were to be reported, the losses would be in excess of EUR 250 billion! The report states that there is lack of comparable EU-level official statistics, surveys, or private sector data and most significantly this study does not factor cybercrime and it omits many other issues linked to cybercrime, its prevention and investigation.

According to CIFAS, UK in 2022 saw an unprecedented 409,000 cases of fraudulent conduct recorded to the National Fraud Database – the highest volume ever recorded. This is an increase of 14% on 2021. Identity fraud cases have now reached an unprecedented level, accounting for 68% (277,234) of cases in 2022. In 2013, CIFAS reported the overall amount of fraud committed in the UK was expected to be between GBP 52 and 85 billion (USD 87 and 142 billion), and identity-related fraud accounted for 60% of that total (USD 52 to 85 billion). Additionally, out of all identity-related fraud, plastic cards—mostly store and credit cards—were involved in 30% of cases. This fraud can be stopped by creating strong identities and safeguarding users' PII.

According to US Federal Trade Commission Consumer Sentinel February 2023 report:

A There were 2.3 million reports of fraud in 2022. And consumers claimed to have lost close to $8.8 billion to fraud, a rise of approximately $2.6 billion since 2021.

B Identity theft accounted for 21.5% of all fraud.

C Card fraud is the most common type of identity theft reported in 2022.

D Identity theft is one of the top two fraud categories across all US states.

Javelin Strategy and Research's March 2023 report suggested that the total amount of Identity fraud in 2022 in the US was $ 20 Billion and the number of U.S. adult victims stood at 15.4 million.

Losses were judged more significant by the Aite Group in its report, U.S. Identity Theft: The Stark Reality, which found that 47% of Americans experienced (financial) identity theft in 2020. Losses from identity theft cases cost USD 502.5 billion in 2019 and increased by 42% to USD 712.4 billion in 2020!

The loss goes beyond money; the 9/11 hijackers enrolled in flight schools and purchased tickets using false identification. The Marseille suspect had seven identities, the Brussels attackers were also suspected of renting a residence using a false name. This is a terrible loss of human life!

A 2007 University of Missouri study of undergraduates from the Midwest was referenced in a BBC News Magazine article. The study indicated that by the end of their second year, 32% of the respondents had obtained a fake ID (often a driver's license). The majority of students who are underage use this to purchase alcohol, according to a report by NIH PA and BBC News Magazine.

As per European Commission's Centre for Strategy, in France (2010), out of total 3572 convictions, 11% cases were identity theft and half of these were related to human trafficking.

It should be mentioned that, according to UK research, just 16% of victims actually report cybercrime to the authorities. Other regions have seen similar patterns as well. Therefore, the numbers predicted in points 1–4 above would be significantly greater.

Measuring the worth of "trust" is one more technique to evaluate the effects of identity fraud. Additionally, trust can be institutionalised or formalised. As a result, more people can conduct business with one another. The only way to increase wealth for people, organisations, and the economy as a whole is to conduct more commerce. According to Steve Knack, a senior economist at the World Bank who has been researching the "Economics of Trust" for more than ten years, trust is worth 99.5% of U.S. economy or GDP!

Background

Securing online identities has become a major focus area for organisations due to the ever-growing cybercrime. Protecting online identities has risen to the top of the priority list for organisations worldwide due to the growth in cybercrime. Small user bases make it easy to manage and keep track of these attacks like phishing 2.0, pharming, MITB etc. but as user bases grow to the hundreds of thousands or millions, difficulties become more serious.

While extensive research has been done to address online identity fraud, "real-world" or "physical" identity fraud has gotten much less attention. However, when the threat landscape changes, the challenges are equally as severe as they are with online identity fraud. In phishing attacks, for instance, it is feasible for hackers to copy or clone physical identities similar to stealing or duplicating a user's online identity. Simple photographic ID cards have been increasingly easy to counterfeit in the past decade thanks to the accessibility of numerous low-cost, high-resolution printers, scanners, and image editing software. Fraud is still a major concern, even with identities that are issued by the governments, like passports (including biometric passports), birth and death certificates, national ID cards, etc.

A summary of the major ID system types and their shortcomings

Let's talk about a fundamental issue before we talk about specific ID schemes. The photograph is the most significant component of any physical ID card. The relying party, such as a security officer (SO) or an individual, determines the identity of the ID holder by manually comparing the ID card's photograph to the subject's face. Visual identification is the term for this. The snapshot is definitely the fraudsters' ultimate aim. They can mimic the victim and use the identity to perpetrate other frauds if they print their picture on top of the victim's picture. Most ID cards incorporate a variety of holograms, colour-shifting printing, watermarks, fine line printing patterns, and other security features that are challenging to reproduce but not impossible. Visual identification has a fundamental issue in that it is very difficult to see ID card irregularities with the unaided eye.

With the use of skilled manipulation techniques, a phoney photograph can be printed with genuine (or virtually genuine) holograms or watermarks that are nearly impossible for the human eye to spot.

The following are a few well-known instances to help with the analogy and further explanation:

A

Without looking at them under UV light, a properly replicated currency bill cannot be identified. From the second half of 2012 to the end of 2015, a total of 2.6 million counterfeit euro banknotes were taken out of circulation. According to the European Central Bank Report, this equates to EUR 126 million when looking at the 2015 denomination percentage breakdown. According to a Times of India report from 2017, the country's banks saw the highest level of fake cash detection in eight years

B

Since a long time ago, people have been forging passports, which are supposed to be secure government-issued IDs. A warning from the EU border agency about the dangers of fake passports is included in the hundreds of cases of passport forgery that are reported each year. Interpol, the French Border Police (Police aux Frontières) and Spanish National Police (Policía Nacional) busted a fake ID racket in 2022. Earlier Police aux Frontières reported 2,774 instances of forged national identification certificates and 3,278 instances of forged passports in 2011.

C

A number of financial payment instruments and documents, including bank checks, demand draft, cash receipts from POS terminals, etc. rely solely on handwritten signatures for validation. If falsified, these signatures are highly challenging for the average person to spot.

To address this issue, most ID cards also have a chip that stores the subject's data in electronic form, and with FIPS/ CC-certified chips, it is very hard to manipulate the image and other information. However, a card reader is necessary to read this data. And that's the issue— not every dependent party has a card reader on hand; due to the expense of the hardware and logistics, some organisations might decide against using card readers. It is ineffective to have an ID system that requires a card reader for high levels of assurance. Other ID systems, with their shortcomings, are as follows:

1 Magnetic Strips

Some forms of identification, including traditional debit and credit cards, cash cards, access cards, etc., have a **magnetic strip** that contains "machine-readable" data, such as a user name, account number, secret identification information, etc. The ability to extract data from magnetic strips and create a perfect duplicate of the original card is known as "cloning." Take ATM card skimming as an example. Another barrier to access for aspiring fraudsters is magnetic strips.

2 RFID

RFID is yet another handy method that is frequently used for physical access; however, like magnetic strips, RFID has privacy concerns and is quite vulnerable to cloning attacks. All varieties of RFID chips, including low-frequency, high-frequency, and UHF chips, are vulnerable to this assault. Another emerging technology is near-field communication (NFC), which is vulnerable to these assaults because it is based on RFID standards (ISO/IEC 14443 and ISO/IEC 18092). The attacker must position the skimming device as close to the ID card as necessary, depending on the frequency.

3 Online Verification

Online verification of ID cards against a main database is another method. Online verification effectively picks up on altered documents or fake IDs because the information on the ID will be incorrect in the database. A straightforward way to ensure that an ID is authentic is to print a special serial number or other identifying information on it and keep it in a centralised database. If the ID checked is fake; either the number on the ID is not registered for the owner or the database does not include the number at all.

Another benefit of online verification is that it makes it simple to revoke documents that have been lost or stolen. Indian Unique Identification Authority (UIDAI)'s Aadhaar is the largest national identity programme on the globe, is a significant example. It is an online verification method that utilises 'pure biometric' credentials kept in a centralised repository. A citizen is given a special identity number that is printed on paper and connected to his or her biometric data that is stored securely in a central database; no smart cards are issued.

While it is excellent at catching fraud, a major drawback is that it requires a biometric reader unit, and the SO must be 'connected' to the backend system. For example, if a SO has to verify the ID while out in the field, he or she must be linked to the server by 5G/4G/3G, SMS, PC, IVR, etc. What happens if the SO doesn't have a biometric reader machine, PC, or laptop? What if they aren't in a mobile network coverage area? What if the mobile network has been shut down[1] or knocked out due to a terrorist attack, espionage, or a natural disaster? A lack of connectivity can have disastrous effects[2]. In order to be effective, an ID system must be able to provide a high level of security even when the SO is 'offline' or without a reader while also providing total 'mobility'.

Furthermore, according to NIST, biometrics are efficient in local network environments but should not be used in remote network environments because biometric data is static by nature and can be abused by fraudsters through replay attacks[3] or even friendly fraud if it is intercepted (or stolen from the repository or victims). A user can only reset their biometric fingerprint 10 times, twice when using an iris scan, and none with facial recognition. Therefore, a credential solely based on biometrics is unquestionably not the ideal option as a first line of defence.

1. Tamil Nadu government suspends internet & To ensure fair exam, Rajasthan cuts mobile internet links for 2 days
2. Supreme Court's directive to UIDAI
3. AADHAAR biometric compromise reports; 1, 2, 3, 4

As a second line of defence, UIDAI has the Fraud Risk Management (FRM) module, which faces two difficulties:

a) Because they are ultimately 'probability' (score) based prediction solutions, they are prone to false-positive. In other words, they are never 'certainty-based', and by design, they only alert fraudulent transactions when the amount of fraud reaches a certain threshold. For instance, UIDAI announced its first fraud ever in February 2017 after discovering that the biometric credentials of one victim had been exploited concurrently 194 times by three distinct organisations. Now the fraudsters would always avoid being discovered if they kept the transactions below the threshold level! The end result is a national identity system with an unreliable first line of defence (biometrics) and a second line of defence based on probability! Realizing this flaw, UIDAI allowed users to disable their biometric authentication by browsing the UIDAI portal and receiving an OTP by SMS on the registered phone.

This strategy also has some fundamental faults, including:

- the potential for fraud when linking an Aadhaar card to a mobile number via phone porting or SIM swap; and
- the ability to deceive unsuspecting victims into unlocking their biometric authentication in a manner similar to a conventional phishing attack.

b) The Indian government instructed telcos to make sure that their retailers or agents do not engage in fraudulent activities related to unauthorised authentication and has requested that the operators have 'sufficient supervision' in this regard. Imagine the security of a solution that depends on the government urging thousands of operators and agents to adhere to best practises! When this was unable to close the gaps, the idea of a virtual ID[4] was established. Users can generate virtual ID numbers at the UIDAI portal and share them with dependent parties in place of their true, permanent Aadhaar numbers.

4. UIDAI introduces concept of 'Virtual ID' to address privacy concerns

Once again, this strategy has several flaws:

- similar to phishing, victims can be duped into creating a virtual ID and sharing it with the hackers;
- they can still be tricked into sharing their true Aadhaar number; and
- access to the UID site itself can be compromised via phishing or pharming attacks, as was previously discussed.

In September 2018, the Supreme Court issued a significant decision that invalidated Section 57 of the Aadhaar Act, which effectively prohibited all private organisations from using biometric authentication. Over the years, all these loopholes led to 50,000 agents being suspended for breaking the rules, 210 data leaks, 30 police FIR reports filed for violations of the Aadhaar Act, etc. As soon as UIDAI demanded that private enterprises delink their Aadhaar numbers, these organisations began to fight against this decision, citing growing KYC costs, declining trust in the system, and eventually greater transaction costs—classic examples of a lack of "institutionalised trust." UID finally offered offline authentication using QR codes and eKYC in response to criticism from the private sector (which accounts for around 80% of GDP) and concerns about monitoring, privacy invasion, and data farming. Again, QR codes are useful for a variety of purposes, such as product tracking and identification, document management, general marketing, facilitating quick URL access, etc.

However, using QR codes for end-user authentication is unwise because

- Aadhaar QR codes are static in nature, and unwary victims may fall victim to phishing attacks where they may end up clicking and giving the QR code picture to fraudsters. The weaknesses that plague static grid cards also affect QR codes and

- after being taken at a legitimate-looking agency, dishonest agents can sell or misuse the QR codes, just as happened with biometric data in February 2017.

eKYC requires the end user exchanging a zipped file and the password with the relying party to authenticate. This file has the demographic data. eKYC is obviously subject to the same risks as QR codes. Such a fraud will be made easier by the authentication mechanisms' very offline nature. After about 6 years, the Government eventually allowed private organizations to leverage the authentication scheme. I'd like to sum this up by noting that, since it's started a decade and a half ago, UID's Aadhaar has come full circle. Ironically, despite being initially created to address the issue of weak authenticators, it eventually provided one!

Another example of online verification is the Social Security Number (SSN) in the US, which is used to trace people for Social Security purposes. Being an online verification system, it is also prone to fraud. Aadhaar Card identity numbers continue to be reported as stolen[5], and 25% of fraud victims in 2014 reported having their SSNs taken.

4 PKI Smart Cards

These credential containers are the strongest ones available right now. These smart cards contain a built-in crypto processor and an impenetrable design that guards against skimming and key cloning of the credentials (the private key). Unfortunately, the majority of PKI setups have flaws. Here are a few well-known PKI smart card deployments and the problems they have:

A Biometric passports

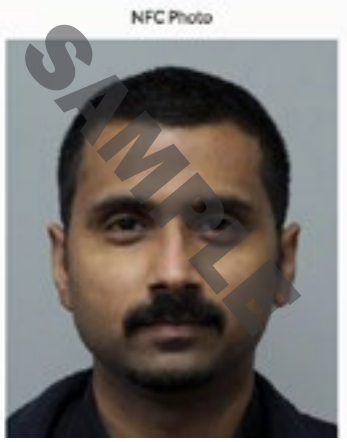
5. Times Of India Reports on compromise of Aadhaar ID No 1, 2

Digital signatures are leveraged in biometric passports to verify that the subject's data is not altered inside the chip (Passive Authentication). This method works flawlessly and serves the purposes of 'data integrity' and 'non-repudiation'. However, a smart card reader is needed, which reads the data and validates the digital signature, to verify that the electronic data is not altered. In the absence of the reader, the passport only provides rudimentary 'visual identification' and has the same restrictions and shortcomings as previously indicated. To illustrate, below are 3 sample photos from my passport.

a) Actual scan of document front photo

b) OCR Photo – zoomed-in scan view

c) NFC Photo – stored in the chip, read by the smart card reader and displayed on screen.



As stated earlier and clearly evident here, holograms, water marks etc., effectively do not offer much help. Over the years, the OCR photo has become quite cluttered and on contrary to assisting in photo tamper detection, these actually impede the verification process. Notice that the scar next to my right eye is not visible at all in OCR photo. Hence, it is the NFC photo, which is leveraged by the SO and ultimately requires a card reader.

Additionally, there are a few other flaws in the biometric passport system:

a) The subject's picture is the most significant feature of any Photo ID card. The difficulty for unassisted eyes to identify ID irregularities is one fundamental issue with visual identification. With the use of skilled editing methods, a phoney photo can be printed with actual (or almost real) holograms or watermarks that are nearly impossible for the human eye to see. For greater deterrence, several countries employ multiple images. The most recent British passports have four printed photos on them.

b) A basic access control concern is that PII data can be read or skimmed via RFID even while the passport cover is closed. To combat this, some nations have developed a very thin metal mesh that functions as a shield when the passport cover is closed.

c) Because our PII is printed on the passports, it is an inescapable problem if we have to present a photocopy of our passports as identification, such as when checking into a hotel or opening a bank account, etc. Our PII could be misused by anyone who has access to the scanned document! A similar concern, with UID Aadhaar, has been raised by Government of India.

d) One of the problems with extended access control is that passports employ JPEG2000 images that can be exploited by toolkits like Metasploit[6].There are few other vulnerabilities highlighted.

e) Lastly, I'll give a personal story from a few years ago regarding problems with facial recognition to draw attention to yet another downside. I got my passport issued with a French cut, eventually grew a beard, and went on an international trip. Because of my beard, the immigration officer at an EU transit airport took around 10 minutes to let me through. He was unsure if I was a legitimate passport holder. This was repeated in Hong Kong as well. Similar to this, bad actors can compromise security by using "look-alike" fraud. Facial recognition-based biometric passports, as adopted by ICAO, is vulnerable since it lacks different biometric credentials. Combining facial recognition, finger prints, and a PIN would be an improved approach.

6. Issues with Biometric Passports No 1 & 2

B US Department of Defense

The US Department of Defense Common Access Card (CAC) employs PKI smart cards for both logical and physical access. For logical access, CAC uses PKI-based authentication, which necessitates a card reader and functions securely like other PKI smart card-based systems. For physical access, however, it is "Visual Identification," which is just as excellent (or awful) as that of a typical PKI smart card-based solution - it's only the printed photo that counts in both circumstances. What if a fraudster prints his image over the image of the victim on a CAC card that has been stolen? There is a chance that he or she will at least get physical access to some secure facilities. Fraud is possible.

C EMV Chip and PIN cards

At ATMs, POS terminals, online and telephone-based payment systems, bank cards act as identification. They rely on PINs and printed card information for authentication. Card skimming can be stopped thanks to the introduction of EMV chip and PIN cards. However, a victim may still give the card information to a fraudster who calls pretending to be from the bank (a practise known as vishing) or be tricked into sending money to someone else. This may occur if a phishing or SMS attack is perpetrated online (smishing). These attacks take advantage of the fact that a printed card number and PIN are all that are required to complete a transaction, making them vulnerable to serious fraud. Additionally, there are vulnerabilities with the chip and PIN cards for example PIN bypass attack etc. An excellent report released by the University of Cambridge reveals security protocol flaws with EMV chip and PIN cards.

Note: For a higher level of assurance, ID cards 1 through 4 above require a hardware card reader.

An in-depth analysis of numerous ID systems reveals, without a doubt, that the age-old fundamental challenge of securely identifying a person in a vast population base has still not been overcome. This is mainly because no physical ID system can guarantee a high level of assurance without a card reader.

Authorization: A Common Issue with Most ID Systems

I want to draw attention to a problem with authorization that affects the majority of ID systems. Identity verification is typically the only thing that ID systems themselves offer. The management of authorization occurs mostly independently. In general, the majority of the ID systems discussed above do not save permission information on the ID card. Let's look at an instance: A foreign national enters a nation with a valid visa and remains there after the visa expires. Until the subject appears at immigration or leaves the country via human trafficking, how would the authorities know that this person is remaining illegally? There are several other potential fraud scenarios as well.

If we examine the underlying causes of such serious security holes, we find that

- the existence of several ID systems that operate in silos — fraudsters utilise alternative IDs to elude law enforcement — and
- the fact that the majority of current identity systems do not support authorization checks are the key causes.

The two most important benefits of having authorization data securely stored inside the smart card are that

1. authorization may be checked even if the SO or relying party is offline, and
2. we don't have to rely on or incorporate separate authentication and authorization systems.

The proposed framework

This suggested framework has been conceptualised to address the aforementioned problems in a way that would close numerous security gaps in existing identity management systems while also providing a number of additional advantages. This framework will offer all elements necessary to support end-to-end identity lifecycle activities, such as identity proofing, de-duplication, registration, secure card issuance, card usage (authentication and authorization), real-time alerts to ID holders and authorities, reporting, and identity revocation, suspension, and renewal.

Importance of the Framework

A Novel and distinguishing features

1 Robust Visual Identification

For the first time, this identity system will include cutting-edge and distinctive technology that will make use of characteristics that people naturally use to identify one another. Since holograms and watermarks are of little use in identifying people in real life, they will not be used on ID cards. The average person will be better able to spot fraud if complicated holograms, etc., are absent. We will achieve a **very high level of visual identification assurance without the need for any hardware card readers** by combining biometrics and advanced printing techniques based on 2D image registration using the radon transform. This makes it an ideal solution for authentication that can be implemented for a large number of users. With the help of this technology, ID cards will have tamper-resistant photos that are also securely saved inside the chip and digitally signed as an extra security measure.

2 Automated photo tamper detection

Since effective security is constantly layered, a card reader would be the next line of defence after visual identification. This add-on hardware card reader will provide automated photo tamper detection in addition to reading authorization data from the chip (details below). As previously said, the upcoming generation of innovative picture printing techniques will fully automate the detection of even the smallest alteration in the photo.

3 Renewable Identities

In US, Executive Order 13402 established the President's Identity Theft Task Force in the US in May 2006, and among its many recommendations is that victims of identity theft should be able to obtain a different form of identification. It can be expensive and time-consuming to provide new ID cards, making ID card renewal a logistical nightmare. Think about the likely event of a bank reissuing your bank card if it has been compromised.

What if the ID holder can reset their identifying details without having to get a new physical card? It seems inconceivable. Correct? Well, the suggested identity framework will present this ground-breaking capability. The fact that the bad guys won't be able to tell when the ID holder has updated the identification information means that this feature alone can stop the majority of identity theft.

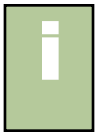
This feature is not offered by any ID system today! An indirect result of this feature will be that relying parties will be required to verify the identification information frequently (as required), significantly lowering the likelihood of off-line fraud. Returning to comparison with AADHAAR, this capability will assist in preventing ID number leaks, for which UIDAI has introduced temporary locking systems and a "virtual ID" system[7]. However, both of these systems[7] are ineffective, and fraudsters can deceive unwary victims into unlocking their biometric credentials and sharing virtual IDs in a manner akin to conventional phishing attacks! With the use of this functionality, it will be possible to prevent vulnerabilities when relying parties validate identity checks just by the fraudster submitting the victim's identity number, as is typical with SSN and Aadhaar[8].

4 Cyber Security

Authentication, in my opinion, is the single most crucial aspect of an organisation's overall information security story. The most straightforward example could be how we secure our homes. We want anybody who has the right key to be able to enter. As was already said, there are a number of online authentication methods that are inefficient and have historically resulted in numerous, significant information security breaches. By far the most efficient 2FA method—better than pure biometric-based ones—is hardware crypto smart cards. We've already talked about why biometrics are undesirable for any scenario involving online authentication. Smart cards, however, provide a significant logistical difficulty for huge user bases, which is one of the main reasons why they were never widely used as an online authenticator.

7. Aadhaar's temporary biometric locking system and Virtual ID concept
8. How your identity documents can be misused & FIR filed in Aadhaar data leak case; all info safe, says UIDAI

Now when this Framework will be in place, crypto smart cards will already be distributed and used for establishing physical identities, it makes perfect sense to employ them to secure online transactions and data as well - better ROI! Additionally, the framework will offer a special Machine Identity Protection (MIP) technology for generating unique crypto keys based on the functionality of digital systems (a combination of software and hardware configurations), using properties or features derived from their own construction and behaviour, capable of guaranteeing both their authenticity and freedom from attack. The foundation for provisioning soft smart cards will be hardware smart cards. Both forms of smart cards will be able to defend against all known attacks linked to authentication, including malware device takeover. The system will offer following cyber security advantages:



Emails are used to launch 75% of all malware security attacks, including ransomware. Email links and attachments are almost equally common. When unsuspecting victims click on these links, trojans and malware are finally installed, which is when the actual damage is done. Hackers can execute sophisticated malware by breaching weak email account credentials (passwords) and utilising these to send out a customised spear phishing email to known victims, in addition to using fake emails to initiate such attacks. Smart malware now makes use of artificial intelligence to learn the sender's wording and mimic the length and style of emails. It's quite sophisticated! The advantages of this framework can be greatly utilised by web mail service providers (such as Gmail, Yahoo, etc.) and corporate email users (such as Office 365, Google Suite, etc.).

Email digital signatures may be enforced to attach the identity of the sender to the email, as these physical IDs will be provided for all users and their email IDs will be verified. Over time, if all relying parties only permitted signed emails, imagine the amount of fraud that could be controlled! Although the majority of email clients today support digital signatures, end-user verification and the logistics of using smart cards still proves to be the biggest obstacle. With this framework, the issue will be resolved because all ID holders would be verified and smart cards will be widely used. There is no danger of key compromise because the private key for the digital signature will be generated and stored within a PIN-protected FIPS 140-2/3 smart card that is designed to avoid key skimming. As a result, non-repudiation may be properly enforced. If an email is later determined to include malware, the sender's digital ID can be permanently disabled, other service providers can be informed, and the bad guys are prevented from opening new email accounts anywhere else. Additionally, the ID card can grant 2FA-based access to the email account itself, further preventing sophisticated malware attacks.

This eliminates all attack vectors. As a result, cyberattacks will drastically decline, and trust in digital media will rise. For convenience, the credentials can optionally be saved locally on the device and secured using the MIP as indicated in A.4 above. The service provider will be able to decide whether keys held on a smart card or in a device will be trusted for transactions based on the level of security.

Complete accountability, audibility, and decentralised control are among blockchain technology's most coveted qualities, according to recent EU research on the subject. Not all use cases, however, call for complete anonymity. For instance, I know BlockChain is a trustworthy system when I transfer money using digital currencies or disclose sensitive information. What about the person sitting on the opposite side of the network, though? I want to be sure that the individual is who they say they are. This is when a robust, vetted identity system like this one comes into play. Attacks on cryptocurrency launches have already demonstrated the devastating impact[9] of total anonymity. Blockchain is powered by asymmetric (private) keys that represent each user's actual identity and are used to digitally sign transactions. The private key in a cryptocurrency wallet must obviously be protected; if it gets compromised through a malware attack, the victim's identity is lost, and all the coins linked to the key become the hacker's assets. Because cryptocurrencies are completely anonymous, a key pair is not linked to a digital certificate; there is no identity connected to the key (and hence related coins), and as a result, there is no recourse at all. The W32M Caligula virus, which was developed more than 25 years ago, was intended to infect the victim's computer, search for PGP key rings (which contained the private key), and then discreetly upload them to the hackers. In a world rife with malware[10], you can envision the threat scenario. A few such carefully crafted acts of espionage might undermine public trust and cause the system to fall apart.

9. CoinDash Hack, Ether ICO hacked, North Korea suspected of hacking into bitcoin exchanges
10. Hackers swipe over $64mn in bitcoin from cryptocurrency marketplace Nicehash | What's the expected loss when Bitcoin is under cyberattack? A fractal process analysis

To protect passwords, encryption keys and various secrets, 3rd party security vendors rely heavily on underlying native security offered by OS, device and microprocessor providers. A majority of these main stream providers have been successfully attacked multiple times for example Pegasus attack against WhatsApp encryption keys (iOS & Android), Jeff Bezos iPhone hack, Meltdown & Spectre (Intel, ARM, AMD, Linux/ Windows etc.) and SGAxe and CrossTalk targeting Intel H/W. Without the protection of asymmetric keys, which is the basis of this concept, none of the blockchain implementations, including smart contracts, digital rights management, patent protection, e-voting, supply chain management, etc., would be successful. The best comparison I can make is to attacks that frequently occur due to many people using weak credentials (passwords). Blockchain is a PKI implementation and will inevitably follow suit if not implemented with best practises (effective protection of private keys). The credentials can alternatively be saved locally on the end-user devices and secured using the MIP as indicated in A.4 above for convenience. Keys held on a device or a smart card may be trusted for transactions, depending on the security level, at the discretion of the service provider.

By specifically tying end user accounts to this ID, social media services can greatly benefit from preventing fraudulent and duplicate accounts, which are frequently the source of fake news, are quickly emerging as a major concern for social media service providers, governments and can have an enormous negative political influence. Without a strong physical identity tied to the account, there is nothing to stop the perpetrators from

opening a duplicate account, connecting back to the network of people, and continuing the threat. It will aid government authorities in tracking and blocking suspected fake accounts linked to terrorist propaganda[11], anti-social behaviour[12], blackmail or ransom, bullying, etc. Social media platforms can also use robust 2-factor authentication to safeguard against humiliating password leaks[13] and prevent bogus 'Like Factories' preserving the real worth of "Likes" in the process. Likewise, internet retail sites can benefit from using this architecture to stop conmen from duping unwary victims. Relying once more on such an ID system, social media service providers can efficiently coordinate with one another and prevent such accounts and attacks globally. The credentials can optionally be saved locally on end-user devices for convenience and secured using the MIP as indicated in A.4 above. The service provider will be able to decide whether keys held on a smart card or in a device will be trusted for transactions based on the level of security.

iv Comprehensive PKI capabilities that, in addition to certificate-based authentication, will also provide encryption and digital signature (non-repudiation) services that are recognised by most IT Acts and legislation around the world, such as the Indian IT Act, 2008, the EU's eIDAS regulation on digital signature, etc.

v Banks and other financial organisations have become targets of cyberattacks at an astounding rate in recent years. Threats are getting worse for both public and private organisations. The majority of attack vectors, including some 2FA technologies, SIM swap attack, target weak login credentials, including phishing, pharming,

11. Manchester Arena blast prediction on Twitter | TOI report on ISIS Propaganda
12. Tamil Nadu government suspends internet to stop spread of 'rumours'
13. LinkedIn Breach | & Yahoo Attack

cross-site scripting, malware, MITM, and social engineering. The suggested smart card-based system will feature dual identities secured by triple factor authentication (described below) and will offer the strongest authentication available for online services like net banking, e-government services, etc. in multiple countries.

vi

This framework will serve as the foundation for the issuance of alternative online identities, such as publicly trusted S/MIME certificates for email accounts. This will save certifying authorities money and time since every ID bearer will undergo a rigorous vetting process. Certificates for private trust client authentication will also be supported.

vii

The broad identity federation, authentication, and authorization features of this framework can be adapted for use by a variety of network devices, applications, databases, etc. This will significantly minimize cyber-attack vectors.

viii

viii) This identity framework can be expanded to help secure IOT/OT ecosystems and devices in addition to more traditional use cases. We are currently seeing the emergence of a number of such use cases, including keyless home and car locks, wireless access to household appliances like thermostats, air conditioners, refrigerators, music systems, etc., and exterior devices like various sensors, CCTV cameras, smart street lights, etc. More crucially, the MIP (A.4 above) will assist in robustly authenticating the IOT devices to backend systems as well. The ID cards generated by this system can be used to securely login directly into the device or to the IOT-connected systems

5 Anonymous authentication - Ease of Use and enhanced trust

a Anonymous physical authentication.

The Framework is designed to allow anyone to verify a person in a secure manner without disclosing subjects' PII. ID cards could potentially be used to validate a subject's identification extremely rapidly by both SOs and regular citizens alike! For instance, if you are away from home and a contractor, mechanic, salesperson, etc. needs to come by, you frequently worry about the safety of your family members, especially women, or if you are a woman and need to board a bus or cab, especially in somewhat unfamiliar areas at odd hours. With this method, the subject's identification can be recorded in real time at a central server that is by simply taping the subject's ID card to a mobile phone. Authorities are able to act quickly in the event of an unfavourable situation, giving the general public a great sense of security and reducing crime and ordinary fraud. Think of another risky circumstance where this gadget will be useful. There were 37,500 cases of mail tampering reported in the UK in 2014 where fraudulent identities were used to obtain postal deliveries. This fraud could be eradicated if postal delivery staff required the recipient to swipe their ID card. Fraudsters will be unable to use victims' current addresses to set up mail intercepts.

b Anonymous online authentication

In this situation, neither party will be aware of the other's ID number. Instead, after authentication, the system will generate a code that may be communicated with the other party;

this code will contain the subject's partial ID number and be useful for a variety of purposes. User profiling is discussed in point #12 below. It will help tackle certain fraud scenarios.

6 Single ID Card

Today, several government agencies, financial institutions, and other private institutions offer unique IDs to end users, including driver's licences, national identification cards, voter IDs, debit and credit cards, passports, and employee IDs. With the help of this framework, each of these entities will be able to issue a single ID card with all of their unique credentials on it and, when necessary, revoke those credentials without affecting those provided by other entities. Certificates that are qualified could be an illustration. One somewhat unusual characteristic is that citizens would only need to carry one ID card instead of several.

7 Dual Identities

In addition to 'renewable' identity number displayed on the ID card, the system will offer a 'static' identity number as well. The ID number on the card will be used for SO based authentication scenarios even in the absence of a smart card reader. The static ID number is not displayed on the ID card, instead will be stored in the chip and is better suited for secure B-2-B communication and would require a card reader. This idea of dual identities will assist various relying parties in

A. selecting an appropriate authentication technique and
B. thwarting any phishing-related attacks.

8 Triple Factor Authentication

The use of several levels of protection for such an identity makes a lot of sense. In order to accomplish identity authentication, the ID card will support three factors. The first factor is what you know (PIN), the second is what you have (a smart card), and the third is who you are (biometrics). In addition to PIN, biometrics will only be used locally to unlock the PKI credential at the smart card level, which will then be used to authenticate the ID bearer to a remote server. Therefore, in accordance with NIST's best practise advice, biometrics will not be utilised to verify the identity of the ID holder with a remote server. Having said that, the identity system will save the biometric information of ID holders in a secure database solely for the purposes of

A. efficient de-duplication,
B. identifying people even when they don't have the ID card (for example, a lost ID card, a fraudster pretending to not carry his ID card, etc.), and
C. assisting forensics in the identification and tracking of criminals. Both facial recognition and fingerprints will be supported.

9 FIPS 140-2 Compliance

The entirety of the system will comply with FIPS 140-2 Levels 2/3/4. This will apply to all key containers, smart cards, smart card provisioning devices, application servers, connectors, database encryption, file server encryption, etc.

The FIPS 140-2-compliant crypto smart cards will support biometric capabilities, which will

A. bind the user's identity to the smart card and
B. ensure that the identity cannot be duplicated.

These characteristics are currently absent from the majority of identification systems. And those who do face additional restrictions.

10 Mobility

The suggested technology will be able to provide unprecedented mobility. Along with regular connectivity via PC smart card readers, detachable micro-card readers for remote authentication will support the majority of mobile phone operating systems and work with a mobile app. Manufacturers of cell phones could eventually offer built-in card readers.

11 Telecom Handset and Network Level Authentication

Calls can be routed to the ID number rather than the phone number when there is an integrated card reader. Two significant benefits will result from this.

A. The phone number itself is PII and can be used to identify a person. Users just need to share their ID number with others in order for calls to be forwarded to their phones, and they can alter their landline and mobile numbers at any time. Consequently, this system will aid in protecting PII and
B. With such widespread ID card reading technology, it may

also be possible to conduct identity checks during phone calls in order to prevent telephone-based terrorism such as bomb threats, fraud, prank calls, swatting, ransom calls, etc.

In other words, the handset will authenticate the user prior to placing the call, and the telecom operator will only let calls go through if authentication is successful—this is security at both the handset and telecom network level! Of course, this calls for more investigation into novel communication protocols.

12 User Profiling

This system will offer the vital function of logging citizens' profiles (especially those related to crime, anti-social behaviour, and fraud) in their respective nations and provinces and assigning a dynamic score. Authorities and citizens can register a complaint if they are aware of the subject's specific ID number. The score is determined by the quantity and quality of complaints. If a relatively minor offence—like breaching traffic laws, for example—is not repeated within a given time frame, the system will automatically improve the citizen's profile score. False complaints stemming from personal grievances will just be one instance, so they won't have much of an effect. Additionally, authorities may change the score and tweak algorithm for calculating the score with the proper approvals in place.

The primary benefit of such a concept is that it can instantly tell a relying party whether or not to believe a subject. Think about certain situations. Simply tapping the subject's ID card on your mobile device or punching the ID number into our

portal or app will provide you with the score if you are dealing with someone who is selling to you, engaging in business with you, promising a job, making friends with you on social media or other online communication, etc., and you are unsure of whether this person is trustworthy. Access to the subject's profile score will, obviously, first require the relying party to authenticate itself to this proposed system and would require the subject to authorise score access. In the case of anonymous authentication, the system will produce a code that may be shared with a third party and contains the subject's partial ID number and profile score. Since residents will be aware that their criminal record or financial fraud can always be tracked and have an influence on their work, business, visa applications, mortgage etc., regardless of where they relocate, this will naturally help reduce crime. Similar to police approvals required for tracing and listening to phone calls etc., accessing subjects' profiles outside of this route would require appropriate degrees of government clearance. In addition to reporting concerns, we may also highlight good behaviour, which raises the subject's profile rating and rewards the individuals accordingly for example tax rebate etc.

This feature goes beyond being "nice to have." Statistically speaking, according to the US Federal Trade Commission Consumer Sentinel February 2023 report, a startling 46% of all complaints received in 2022 were related to fraud- these were categorised by type as follows: Credit card fraud, bank fraud, loan or lease fraud, employment or tax-related fraud, government documents or benefits fraud, and other identity theft. User profiling alone, in my opinion, can stop a significant amount of identity fraud! – Citizens will be greatly relieved, and institutionalised trust will improve for the benefit of the economy.

13 User Data Privacy

According to the FTC Identity Theft Survey and a Utica College report, between 12% and 27% of identity theft incidents may be caused by data breaches, which can occur at smart card level or at central repositories. Although there isn't a lot of research linking physical identity theft with data breaches, it is possible that they are the cause of some of these incidents. This framework has been designed in a way that ensures users' personally identifiable information (PII) will always be encrypted, including when it is issued, saved on a smart card, or accessed by dependent parties such as government agencies. The ID cards and card readers will be made so that only authorised parties, like the subject's department or the government, would be able to see the identifying information of the ID holder. Smart cards will be able to identify real card readers and the servers they are connecting with, thwarting any MITM attacks. Users will greatly profit from this strategy since they will always be notified in real time via emails, web portals, mobile app push notifications, and SMS whenever a relying party needs to authenticate them. The ID holder can then accept or reject these requests by logging into their account via their smart card. The relying parties may have access to their PII with their consent. By doing so, service providers' abuse and fraud will decrease. Identifying and reporting fraud at an early stage will be made easier by this. Additionally, users may view fresh recognitions and complaints (and respond appropriately) on the dashboard, check their current profile score, send and receive encrypted messages, and view which agencies and organisations have accessed their personally identifiable information.

14 Graduated Authentication

This system will handle several progressive authentication levels as specified in FIPS PUB 201-3. As a result, it will be possible to choose the optimum level of identity authentication for various use cases, achieving the ideal balance between security and user comfort.

15 Surveillance, Crime and Fraud Prevention

Governments can use this framework as an extra layer on top of CCTV surveillance, telephone tracking, internet traffic monitoring, and other methods to keep an eye on problematic individuals. Alerts will be issued to the appropriate authorities each time a suspected person's ID card is examined (contact-based and contactless procedures are supported). The surveillance will become even more effective if the framework is extended to new departments, organisations, stores, transportation networks, etc. For instance, governments might coordinate and keep tab on residents who reside or work abroad and return home solely to file for benefits. The technology will have biometric capabilities, making it a powerful tool for identifying and tracking criminals using forensic evidence.

16 Unique Identities

ID systems typically lack the ability to prevent residents from reapplying for IDs after they have been cancelled. For instance, if a citizen's driving privileges are suspended,

in some nations he or she can travel to another city, county, or province and apply for a new licence under a different identity! This type of fraud can be avoided if the ID system has a strong central de-duplication mechanism to prevent citizens' identities from being fraudulently issued to them again after they have had their identities cancelled. This suggested solution will make sure that each user's identification is distinct. This framework will execute biometrics de-duplication checks on its complete database on a national and global level for every new identification to weed out scammers! In 2004, the United Nations (UN) Economic and Social Council (ECOSOC) adopted Resolution 2004/26 on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. The UN adopted Convention against Transnational Organised Crime (UNTOC) specifically addresses identity theft, albeit solely in the context of the fight against organised crime and in relation to offline identity theft.

17 NIST FIPS 201 augmentation

The framework will improve on a few FIPS criteria, even though we intend to incorporate the best practises from FIPS 201 PIV. For instance, FIPS 201 does not connect the ID card's photo with the digital credentials kept in the chip; this problem will be fixed. FIPS 201 was created with a specific group of users in mind; however, this framework will be used by a much larger population, changing the use cases significantly. As another illustration, under FIPS 201, the agency code is the first character of the unique identity number (FASC-N), but we also require the country or province code.

FIPS 201 GUID refers to IPv6-based identity, which is extremely unpredictable and insufficient for our needs.

18 Interoperable Identities

Relying parties from one country, province, or department can trust the identities issued by another country, province, or department for all "A&A" purposes since identity issuing will be completely standardised. In other words, anyone can verify an ID card that was issued somewhere else. According to CIFAS, cross-sector fraud prevention is most successful because 63% of fraud discovered by CIFAS systems was found by comparing data from several industries. In 2022, CIFAS members prevented more than £1.3 billion of fraud losses through the use of the National Fraud Database. A fraudster working while claiming Jobseeker's Allowance could be one example; different employers and governments can link-up and stop such fraud. Beyond cross-sector cooperation, nations can work together on de-duplication, a uniform reporting interface, and a unified reporting structure. This could ultimately develop into a "global" physical identity framework. This will address the lack of harmonized national laws, international standardisation of evidence requirements, and the timely collection, preservation, and sharing of digital evidence between countries that could impede investigations of identity theft and identity-related crime.

19 Authorization

Most of the ID schemes mentioned above merely offer authentication. This system will combine and automate "A&A," which is currently done by separate authentication and authorization systems that typically require manual approvals. One extremely important application, for instance, may be blocking terrorists or suspected criminals from entering high-security locations, such as airports, aircraft, defence and nuclear sites, power grids, etc. El Al Airlines is renowned for its meticulous inspection procedure; they cross-reference all passenger identities with data from the FBI, CSIS, Scotland Yard, Shin Bet, and Interpol databases. Effective surveillance would result from government agencies being notified right away whenever a suspect attempts to enter an airport or purchases a ticket. When the return trip is due, if the fraudster jumps VISA and does not show up, the appropriate authorities can automatically and right away send out a warning to all other authorities with the subject's ID number pushed onto all SO mobile card readers, ensuring that they are apprehended wherever the ID card is swiped. For the first time, a system will provide a reliable means to catch offenders based on their current location and not their physical address, which can be helpful in controlling variety of other crimes as well. With far less expense and much greater user ease, the suggested system may offer an equivalent degree of security to all airports, public transportation systems, and other institutions. Secure electronic VISA issuance to travellers going overseas might be another use case. The system will handle both near-real-time authorization notifications being transmitted to SO handheld readers and the storage of authorization data inside smart cards.

20 Electronic and online voting

Governments can use this technology as a tool to replace the traditional ballot box method of conducting elections, which necessitates tremendous logistical effort and high costs. It will have advantages like paperless voting, real-time vote counting, reduced forgery related to voter ID cards, ballot papers, and polling stations, elimination of poll-related violence[14], and prevention of abuse and hostile force interference that have affected some very important elections in the past. The majority of the present electronic voting methods call for a specific electronic voting machine (EVM) and do not ensure that a voter casts a single ballot. This framework will permit the use of standard voting equipment (card readers, mobile devices, etc.) and will end voter fraud such as multiple voting. Voting would be available to citizens even if they were not in their city at the time of the election, which would ensure greater participation. Other security-related issues with traditional EVMs are:

A. being susceptible to interception attacks. For instance, EVMs in India are deliberately designed to be stand-alone machines to prevent certain attacks. The proposed system will have robust cryptographic capabilities and will not be prone to such attacks.
B. EVMs require the security of the voting machine itself since they can be tampered with[15]. As mentioned earlier, this proposed system will be FIPS 140-2 Level 3 compliant and hence tamper-resistant. Conventional EVMs are relatively larger in size, so transportation and security introduce additional logistical overheads. The proposed solution will have much smaller devices, thereby overcoming this issue.

14. Elections related violence in Mexico| & West Bengal
15. Times of India Report - How safe is the EVM| DEF CON Voting Village

C. Even with EMVs, menaces like booth capturing are still possible. The “mobility” of this framework will enable voters to cast ballots using their mobile devices, making it possible to conduct such a nationwide vote with the best possible balance of cost, security, and convenience for the first time in history! Blockchain technology could potentially be used to power the electronic voting itself, bringing with it total audibility and decentralised control. This technique is also applicable to referendums and plebiscites. Even with non-democratic forms of government and enterprises, this technique can be utilised to get the opinions of the populace, promoting inclusiveness and state stability.

21 Financial Implications

These ID cards will provide a number of advantages and can be linked to the cardholder’s bank account(s).

A. **Debit and Credit Cards:** The principle behind the proposed framework is such that banks can use the ID cards issued by this system as debit, credit, or cash cards at ATMs, POS terminals, and kiosks. This would significantly aid in the eradication of phishing, vishing, and smishing frauds in the banking industry, preventing the loss of billions of dollars in fraudulent transactions and capital expenditures for re-provisioning bank cards.
B. **Card Present (CP) Transactions**: Through POS machines, retailers take advantage of cashless CP transactions; customers simply swipe their cards to make a purchase. The third-party money transfer feature of internet banking is another alternative for cashless transactions. What if you want to pay someone on the spot with cashless but you

don't have access to net banking, or you have but you can't log in? This proposed system will assist in achieving this goal:

- One can link this ID card with their net banking (one-time effort);
- Launch this framework's mobile app and authenticate with the ID card; and
- With knowledge of the recipient's ID number, they can pay the recipient via CP transactions without having to go to ATMs or net banking, thus indirectly reducing online identity fraud like phishing, vishing, smishing, etc.

The effect on micropayments will be significant. 3rd party payment service providers can leverage strong 2FA offered by the platform.

C. **Cash-less Economies**: With the use of the aforementioned bullet points A and B, it will be possible to significantly decrease "cash"-based transactions, eliminating frauds including forgeries of currency bills, money laundering, the use of black money, cash theft at banks and ATMs, saving billions of dollars for the world's economies. India's black economy was reported to have totalled USD 460 billion in 2016. With points A, B and C, ATMs can be a thing of past!

D. **Instant Payment System:** Peer-to-peer (P2P), person-to-merchant (P2M), and digital wallet-based payment systems are increasingly taking over the financial world. With 8.9 billion transactions per month totalling more than USD 17 billion (April '23), India's UPI is undoubtedly the largest digital payment system in the world and is endorsed by more than 50 countries. The presence of a physical SIM card, which forms the basis of device binding and forbids the use of emulators, is just one of several important security measures offered by UPI-compliant mobile apps. Having said that, the security analysis 'Unified Payments Interface and Payment Apps in India' conducted by the

University of Michigan clearly outlined all UPI 1.0 vulnerabilities. All of these flaws are possible because banks rely on

A. mobile numbers as the basis for device identification and binding,
B. SMS/OPT at 2FA, and
C. a lack of robust machine identity protection (MIP), which makes it possible for passcode-skimming malware to infect end-user devices, particularly Android devices.

There is a through list of Threat Mitigation. These flaws are reportedly present in UPI 2.0 as well. There are additional attack vectors as well, and the NPCI warns the users to be cautions of these. Such limitations are technical in nature and may be circumvented with a strong bank 2FA and MIP, both of which are provided by the proposed framework, along with support for smart card-based mobile payment app authentication akin to Apple Pay, Samsung Pay, and other similar services. Threats from reverse engineering and App repackaging are another area of emphasis in this research. This problem will be resolved by the cutting-edge MIP provided by the framework.

22 Other Miscellaneous Features

Although smart cards will support NFC, the NFC tag won't include users' PII and won't be vulnerable to cloning attempts because of this. In order to combat situations like friendly fraud, this framework will be supported by a real-time fraud risk management module. This module will operate as a supplementary layer for strong identities. An ID system like this can make a significant contribution to reducing the billion-dollar software licencing fraud.

This system will serve as a global repository for digital certificates, allowing anyone to access the recipient's digital certificates and deliver encrypted data with the recipient's ID number. This framework can potentially offer a Post-Quantum solution via robust MIP. A concept document is available here.

B Commercial benefits

This solution will enable annual savings of millions of dollars on the production, provisioning, and logistics of numerous ID cards by replacing them with a single all-purpose ID card.

Governments all around the world invest an enormous amount of money in setting up national ID systems. For instance, the AADHAAR project in India is expected to cost more than $1.5 billion, and as of March 2018, the predicted savings and benefits since the programme's launch were more than USD 109 billion! The Identity Cards Act 2006, which created the UK's National Identity Cards, was projected to have cost £5.612 billion ($8.8 billion)[16]. Several governments can use this framework at a fraction of the cost.

16. British Identity Cards Act 2006| British National Identity Card

C Social benefits

Knowing that their identities cannot be impersonated and that the PII stored on their smart cards and in the repository is safe and impenetrable, would provide them with a physiological sense of security.

This framework will significantly aid in the eradication of corruption in rural and distant areas of developing nations, where middlemen and brokers prevent poor and underprivileged populations from fully taking advantage of government initiatives. Direct money transfers into their bank accounts will be used to accomplish this.

Using this framework, a single source of identity is possible. The difficulty of having to present numerous supporting identity documents each time a citizen wants to use a service, such as opening a bank account or applying for a passport or driver's licence, would be eliminated. Additionally, managing various ID cards, such as different loyalty programme cards, is a burden.

Use Cases

1. User profiling will make it easier and faster for the governments to undertake thorough background checks on citizens, which is currently challenging and time-consuming. With people from other countries, it is even harder for the government to undertake thorough background checks. Employers, landlords, and other parties besides government agencies, with due authorization, will be able to do these checks with just the click of a button!

2. Strong online authentication will enable a variety of financial institutions, government agencies, private organisations, etc. to take advantage of this cutting-edge technology and avoid spending separately on authentication systems that are seldom deployed with best practises. This will help save the billions of dollars lost annually due to cyberattacks and online fraud. With online authentication, anyone can get FIPS 140-2 Level 2/3 smart cards with military-grade security

3. Corruption can be minimised by automating ID issuance, reporting fraud detection linked to issuance by users or government personnel etc.

4. 'Alerts', 'Authentication and Authorization', 'Single ID Card', and 'Surveillance' are all combined into one system. When a passenger travel is approved, for instance, the airline ticketing system can check government databases, issue an authorization alert with the passenger's ID number, and send it to all handheld card readers at the specified airports. Passengers authenticate themselves at a card reader at the airport, and since the authorization data is already there, they are allowed to proceed. The airport will not let anyone through with a bogus ticket. Security personnel at the entrance gates can easily authenticate and authorise the subject in commercial, industrial, and residential complexes where people can grant visitors permission by keying in their ID number on a mobile app or portal.

Qualifying Questions

Before we come to a conclusion, it might be wise to summarise the advantages of the suggested system via the lens of competitive analysis. In order to determine whether any other identity system provides the capabilities listed, one could investigate the following important qualifying questions:

Is the Identity system or ID card secure in terms of:

1. Can the ID card's photo be altered in any way?
2. Does it provide high visual identity assurance without card reader?
3. Does it provide strong identity assurance without network connectivity?
4. Can the subject be authorised and authenticated by the system while offline?
5. Is the ID card holder's PII protected?
6. Does it employ three-factor authentication to unlock the credentials on a smart card?
7. Does it offer more than one identity technology with ID card?
8. Is it feasible to dynamically reset the identity data on the card?
9. Does it protect against phishing and other known identity authentication attacks?

Broad-spectrum in terms of use cases. Does it:

1. Provide safe online voting?
2. Support user profiling?
3. Does it support PKI to address use cases like block-chain?
4. Support the use of ID cards as bank cards?
5. Support use cases where end users can log the identities of anyone else and authenticate them to help catch fraud or crime suspects.
6. Offer a strong defence for numerous cyber-security use cases?

All these features and capabilities will be available through the Secure Physical Identity Framework that is suggested in this study.

Conclusion

The European Commission (Report) has identified a total of 181 existing national regulatory and non-regulatory measures across 27 EU Member States to prevent and combat online identity theft, mitigate the risks for consumers and provide victims with support and assistance. Most of the practical measures supported by public institutions are in the form of awareness raising campaigns (38), followed by training programmes (17) and IT tools (14), funding mechanisms (5), public authority systems (5) and Public Private Partnership (4). This Study concludes with recommendations in three areas: victim protection, ID theft prevention and crime investigation and prosecution. EU measures aim either at harmonising various offences that are linked to ID-theft, or at increasing Member States' capacity to prevent and combat this issue. While it is impossible to establish whether such a policy would be an effective deterrent to identity theft perpetrators beyond the predicted minimal implications, it would make dealing with the repercussions easier. These goals, at best, either serve as a deterrent, raise awareness, or provide a resource for victims after the scam has occurred.

Not just this study, but many other comparable reports discussed in this paper and elsewhere fail to address "how" to stop the crime from happening in the first place. Therefore, merely relying on legislative and non-legislative measures is insufficient to combat identity fraud. To serve as a first line of defence and to provide both the government and the populace with new hope, we need a creative, strong, and broad-spectrum identity framework. Last but not least, a tool like this can genuinely be a godsend for most countries, considering the significant impact institutionalised trust can have on the GDP of any country. Apart from directly reducing identity fraud, which costs more than $1 trillion annually, this identity framework can also indirectly support global economies, which are worth many trillions of dollars.

Appendix A: Terms

Phishing is an assault that aims to acquire usernames and passwords from a large number of individuals so that fraudsters can use them. In contrast to phishing, which uses a phoney website to entice victims, phishing 2.0 (also known as advanced phishing) uses an MITM proxy to redirect victim and server communications, compromising users' credentials in the process. Spear phishing attacks are well thought out and more likely to be successful because they target specific people.

Card-present transactions are any financial transactions that require a debit or credit card to be physically present in order to complete the transaction, such as withdrawing cash from an ATM or swiping a card at a POS terminal while visiting a retailer.

Pharming in contrast to phishing, the victim is not targeted via email and given a URL to a bogus website. Even though the victim enters the right URL, malicious DNS servers or corrupted cache files on the user's computer cause a redirect to a phoney (pharming) website. The user ultimately gives the fraudster their login information on the pharming website.

Man-in-the-Browser, or MITB, is an acronym. It is a Trojan-initiated attack that leverages a session that has been authenticated. The Trojan patiently awaits the victim's request to send money to a third party. These Trojans alter the destination account number and potentially the money before the transaction details are sent.

A **digital signature** is executed electronically using the sender's private key and a digital certificate. Usually, well-known certifying authorities provide digital certificates. The sender's public key, which is visible to others, is used by the recipient to verify the signature after the sender's private key digitally signs the data. Data integrity, which ensures that data hasn't been altered after being signed, non-repudiation, which prevents the sender or signer from subsequently denying that they carried out the signature, and certificate-based authentication are all features of digital signatures.

Look-alike fraud occurs when a fraudster impersonates the victim by using a legal ID card that is not their own. For instance, it looks to be more difficult to enter the Netherlands using forged documents given the advancements in the detection of passport fraud. As a result, the Dutch police have observed an upsurge in passport-related look-alike fraud.

Federal Information Processing Standard 140-2 is referred to as FIPS 140-2. The National Institute of Standards and Technology (NIST), a US standards body, is responsible for issuing these certificates. All US federal agencies that deploy cryptographic-based security methods to safeguard sensitive data in computer and telecommunications networks (including voice services) must adhere to this standard. The secure design, implementation, operation, and disposal of a cryptographic module are all covered by the security standards.

A phone porting attack refers to a strategy where a hacker leverages the portability of mobile numbers for improper purposes and obtains the victim's mobile number. This is typically started by creating a false identity for the victim and

contacting his or her telecom operator to request that the services be blocked and switched to a different carrier, allowing access to all texts and calls.

With **SIM swapping**, the fraudster first identifies the intended victim, collects his or her information, and then contacts the victim's mobile service provider. The fraudster will use social engineering strategies to persuade the phone company to port the victim's phone number to the fraudster's SIM service provider. The fraudster will use social engineering strategies to persuade the phone company to port the victim's phone number to the fraudster's SIM. For instance, by pretending to be the victim and saying they have lost their phone, you can access texts and voicemails.

Appendix B: Acronyms

PKI	Public Key Infrastructure
MITB	Man-in-the-Browser
MITM	Man-in-the-Middle
SO	Security officer
ATM	Automatic teller machine
SMS	Short messaging service
GPRS	Global packet radio service
IVR	Interactive voice response
FRM	Fraud risk management
KYC	Know your customer
FIPS 140-2	Federal Information Processing Standard 140-2
FIPS 201	Federal Information Processing Standard 201
FIPS PUB 201-2	FIPS Publication series 201-2
SP 300-73-3	FIPS Special publication 300-73-3
EMV	Europay, Mastercard, VISA
FASC-N	Federal Agency Smart Credential Number
GUID	Global unique identification number
IPv6	Internet protocol version 6
FTC	US federal trade commission
FBI	Federal Bureau of Investigation
CSIS	Canadian Security Intelligence Service
POS	Point of sale
IOT	Internet of things