

Security Risks In Authentication With Electronic ID Cards

CMP7200 Individual Masters Project



Student ID:

Student Name:

Supervisor Name:

Table of Contents

[Table of Figures 1](#_Toc79508645)

[Abstract 2](#_Toc79508646)

[Introduction 2](#_Toc79508647)

[Aim and objectives 5](#_Toc79508648)

[Review of Literature 6](#_Toc79508649)

[Password-Based Systems 6](#_Toc79508650)

[Biometric Confirmation 8](#_Toc79508651)

[Smart-Card-Based Systems 10](#_Toc79508652)

[Non-governmental Identity Providers 12](#_Toc79508653)

[Post Offices 12](#_Toc79508654)

[Bank Credentials 12](#_Toc79508655)

[Hybrid Systems 13](#_Toc79508656)

[Research Methodology 14](#_Toc79508657)

[Data Collection Method 14](#_Toc79508658)

[Data Analysis Method 14](#_Toc79508659)

[Ethical Consideration 14](#_Toc79508660)

[Research Design 14](#_Toc79508661)

[Experimentation 15](#_Toc79508662)

[Dataset 15](#_Toc79508663)

[Analysis 16](#_Toc79508664)

[Results 18](#_Toc79508665)

[Countries Without Citizen Authentication 21](#_Toc79508666)

[Discussion 21](#_Toc79508667)

[Conclusion 22](#_Toc79508668)

[Appendix 23](#_Toc79508669)

[References 32](#_Toc79508670)

# Table of Figures

[Figure 1 - Front and back side of the new German ID card (source: Bundesministerium) 2](#_Toc79237541)

[Figure 2 - Summary of authentication services. 3](#_Toc79237542)

[Figure 3 - Electronic functions and data of the ID card. 3](#_Toc79237543)

[Figure 4 - Online Authentication Access System. 5](#_Toc79237544)

[Figure 5 - Roles and Responsibilities of the new eID Card System. 6](#_Toc79237545)

[Figure 6 - National electronic ID - Infineon Technologies. 7](#_Toc79237546)

[Figure 7 - Biometric Identification. 8](#_Toc79237547)

[Figure 8 - Biometric Confirmation via Smartphone. 9](#_Toc79237548)

[Figure 9 - Smart eID Cards. 10](#_Toc79237549)

# Abstract

Electronic identity (eID) cards promise to supply a universal, nationwide mechanism for user authentication. Most developed countries have started to deploy eID for government and private sector applications. The eID card should have interesting design features: it is contactless, it aims to protect people’s privacy to the extent possible, and it supports cryptographically strong mutual authentication between users and services. Privacy features include support for pseudonymous authentication and per-service controlled access to individual data items. The core technology seems ready for prime time and government projects deploy it to the masses. But application issues may hamper eID adoption for online applications. This thesis attempts to identify the privacy and security risk factors of using electronic identification from the end user’s perspective using a survey. Understanding the global state of the art is necessary because Internet services are often global and accessed across national borders, and because there sometimes is a need to bootstrap the user identity from the government-issued or sanctioned credentials.

# Introduction

Global Internet usage in December 2006 surpassed 1094 million users (IWS, 2006), providing for emerging Internet connectivity markets such as the use of secure electronic ID cards. Compared to every other technology, the Internet is a technology that travels faster - the Internet is estimated to multiply twice every 100 days. Electronic ID cards have been growing explosively in many countries since the new millennium and have changed the conventional practice of authentication. Traditional financial institutions provide e-card services that aim at reducing operating expenses, enhance client services, attract customers and increase the customer's share.

Many states had public identification systems in place even before the Internet had become a commodity to hand out certificates of identification to the public. Governments trust their cards, and companies are also present where people and identification papers need to be reliably authenticated. Related certificates, including driving licenses, are used daily for the same purpose and in countries without national ID cards systems. Many European governments believe this, and e-ID card systems are used. The new Personal German electronic ID card is the most recent and the most sophisticated use of an e-ID (Klugler, 2005). The new electronic ID card announced to people as their "most valuable card" aims to offer a universal and safe identification system with privacy advantages to government and private sector applications (Brands, 2000). The majority of services in modern society are electronic, partially on internet servers, and most security is focused on the careful handling of data or cryptographic methodologies. However, certificates of citizen identification, such as security passports and identification cards, are also very physical. Such records became outdated when resources migrate to the Internet or include links between the individual and online accounts and database entries even in daily material circumstances. Governments all over the world also see the need for electronic identities for people. The first electronic card was published in Finland in 1999, and several more were created during the Internet boom. The card has been issued in Finland (Rissanen, 2010).

A picture containing diagram

Description automatically generated

Figure 1 - Front and back side of the new German ID card (source: Bundesministerium)

Everything is getting updated in the present time, and the data are being shared and uploaded online with the help of the Internet. Almost every company has made itself available online due to the increasing demand. The Internet has changed the methods a lot and is still getting updated every day. The data relating to people are also online, that is, identity cards and other essential documents. With the increased use of the Internet and the online demand for cards, the security risks and privacy issues are also increasing and thus needs to be taken care of. Therefore, this paper will identify the potential privacy and security risks associated with the authentication of Electronic ID cards on the Internet.

e-ID promoter sees a future where an identification card replaces username and password, facilitates online and offline market processes and offers online facilities that enable a person or documentation to be present before now. You want us to buy, open bank accounts, check-in hotels, rent cars and file our tax declarations one day using a single e-ID system. It is expected to achieve this aim by piggybacking the authentication scheme on commonly used ID cards. Within ten years, an environment enticing to both people and suppliers would be available if the deployment is complete.

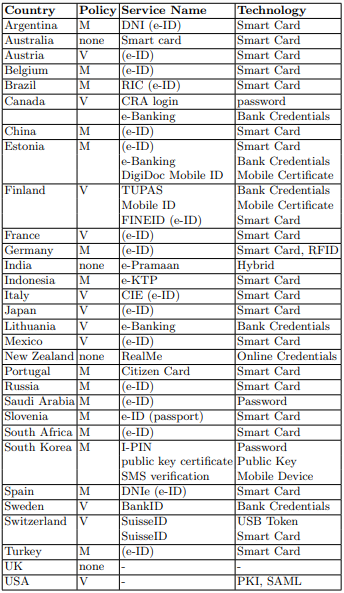


Figure 2 - Summary of authentication services.

In the web-enabled environment, reliable user identification is becoming an even more critical activity. In a business or business climate, the effects of a precarious authentication scheme can be devastating and entail a lack of knowledge on a sensitive basis, denial of service, and data integrity breaches.

Table

Description automatically generated

Figure 3 - Electronic functions and data of the ID card.

The importance of confidence in the customer is not confined only to a device or network access. Many other daily apps often require user authentication, such as banking, e-commerce and network access management, and may benefit from increased security. The Aadhaar project is the world's most significant public character project, dispatched by the assembly of India, which attempts to accumulate biometric and portion data of occupants and store these in a united informational index. Until now, 1036 million customers have chosen the system, and the public authority has spent at any rate 890 million USD on the endeavour. Regardless, there have been general musings over the insurance and security issues related to the Aadhaar project. In this article, we review these issues from a Software designing perspective (Zimmermann, 2019). There are various restrictions on the prevailing user verification methods, including either passwords or user IDs or identity cards and PINs. Direct covert surveillance will unlawfully access passwords and PINs. The attacker has full access to account services as the intruder receives the user identification and password. There is also no way to connect device use or service positively to the actual customer, which means that the owner of the user ID is not safeguarded against repudiation. For instance, the machine cannot know who the user is if the user ID and password is shared with a colleague. A similar situation occurs when a web-based transaction is conducted with a credit card number. Although data is sent over the Web using secure encryption methods, existing systems cannot ensure that the credit card's rightful owner initiated the transaction. The conventional security policy based on a single user ID and password has been insufficient in the current distributed systems world. The data analysis method that will be implemented in the research is thematic analysis. The thematic analysis refers to identifying specific patterns or any theme, which is beneficial in determining the results and leads to a conclusion. The secondary data collected from various sources will be analyzed using the thematic analysis method, and the potential privacy and security risks faced again and again. This will help determine the possible privacy and security risks by taking an example of 'Aadhar Card', and the recommendations will be then provided based on the findings and analysis (Petkovic and Jonker, 2007).

Data frameworks in the advanced age have gotten progressively reliant on data sets to store much preliminary information. A vital capacity of organized information bases is to house confirmation certifications that check character and permit clients to get more vivid individual details. Confirmation data sets are now and again an objective of assault as they possibly give a road to perpetrate further, more worthwhile violations notwithstanding the arrangement of industry-standard best practice suggestions from associations like Open Internet Application Security Project (OWASP), Payment Card Industry Security Standards Council (PCI-SSC), Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE), frequently viable security executions inside industry struggle. Lacking or unacceptable performances have developed a climate where validation data sets and the information put away are shaky. This was shown in the 2016 openness of Yahoo's penetrate, where around one billion client certifications were taken (Mumtaz et al., 2019). The worldwide innovation organization was discovered to utilize out of date security components to ensure client passwords. For example, Dated executions pose a genuine danger as they render verification information profoundly powerless against burglary and expected abuse. This paper offers a novel answer for getting validation data sets on resistant Apache workers. The technique applies the suggested best practice instruments as salt, single direction encryption and cycles to previous and recently made passwords put away on shaky frameworks. The proposed arrangement can be executed worker side, with little change to the current framework, unbeknownst to the client. It can improve framework security, help consistency, save protection, and ensure clients. Strong authentication is a necessary but loosely established principle. Standard government identification certificates are somehow used as evidence of the identity of the credentials holder that is strong or lawfully recognized. This power is based, depending on the nation, on a one-to-one mapping of the person to identifiers or database registry entries or on a decentralized yet stable record of being aware over the lives of the same name. Good authentication online or offline intuitively implies a comparable degree of safety to the conventional paper identification papers of the electronic environment. This also results in technological specifications relating to initial identification checks (identity checks) and authentication mechanisms.

Verification is the crucial security administration utilized in practically all far off applications. All such delicate applications over an open organization need a verification instrument that ought to be conveyed in a confided manner. Researchers have planned an RSA based confirmation framework for a keen IoT climate over the air network utilizing cutting edge industry principles. The framework gives security administrations including X.509 declaration, RSA established Public Key Infrastructure (PKI), challenge/reaction conventions with the assistance of intermediary actuated security specialist co-op. We depict a creative framework model, convention plan, framework engineering and assessment against known dangers.

Diagram

Description automatically generated

Figure 4 - Online Authentication Access System.

Additionally, the executed arrangement planned as extra help for numerous other touchy applications (sensitive city applications, existing digital frameworks and so forth) which needs the support of X.509 authentication dependent on hard tokens to populate other security administrations, including classification, uprightness, non-renouncement, protection, and secrecy of the personalities (Juan, 2019). The proposed plot is thought about in contrast to known weaknesses and given detailed research with mainstream realized validation plans. The outcome shows that our proposed conspire to relieve all the realized security hazards and provide the most elevated level affirmation to brilliant contraptions.

Everything is getting refreshed, and the information is being shared and transferred online with the assistance of the Internet. Pretty much every organization has made itself accessible online because of the expanding request. The Internet has changed the strategies a great deal is yet getting refreshed each day. The information identified with individuals is also on the Internet, character cards and other significant reports. With the expanded utilization of the Internet and the online interest of the cards, the security hazards, just as the protection issues are additionally expanding and consequently should be dealt with. Accordingly, this paper will zero in on recognizing the possible protection and the security changes related to the validation of the Electronic ID cards on the Internet.

However, the widespread deployment of solid electronic authentication has taken much longer than initially expected, and most countries have their solutions that arise from the local culture and history. The investigation is based on the risks of biometric validation and proposes various standards to get and security protecting verification. We further survey the current works of biometric confirmation by examining their disparities and summing up the benefits and disservices of each dependent on the proposed rules. Specifically, it has been concerned that the issues of aliveness recognition and security assurance in biometric verification. Considering the study, it is sorted out various open research issues and further determine different huge research headings that are worth uncommon endeavours in future research.

# Aim and objectives

The research aimed to survey some of the potential privacy and security risks while the authentication process with electronic ID cards is done online. The objectives of this research are listed below:

* To design an effective questionnaire that consists of at least 10 questions that can easily be answered by people without feeling anxious and provides the information requisite for this research.
* To perform hypothesis-based statistical analysis based on the data collected from the survey. There must be at least 3 hypotheses considered in the research. The creation of the hypotheses will be achieved from conversations with the target audience.
* To help visualize the trend of people that try to achieve a solution against privacy and security risks and to visualize the trend of the complete survey as a whole.
* To identify from the analysis at least 3 privacy and security risk factors that people are most experienced with.

# Review of Literature

Diagram

Description automatically generated

Figure 5 - Roles and Responsibilities of the new eID Card System.

Internet banking is acquiring fame in Malaysia because of its comfort, which is accomplished by exciting business cooperation between banking foundations and clients employing sites and portable applications. In any case, the unfathomable acceleration of Internet misrepresentation cases has caused expanded protection and security chances for Internet banking clients. Because of a survey of writing, this research used a system to measure the effect of client insight about the adequacy of biometrics innovation on saw protection and security and its impact on trust and expectation to proceed with Internet banking. Considering the developing practicality of biometrics innovation as an answer for Internet banking issues, the created structure is then used to survey whether the impression of biometrics adequacy for Internet banking altogether affects the connection among trust and view of protection just as security. By testing the structure utilizing an example of 413 Internet banking clients, this research offers critical bits of knowledge into the likely viability of biometrics innovation application in an Internet banking setting to reduce protection and security concerns and improve trust among Malaysian clients. The discoveries uncovered that even though there was an irrelevant connection between saw protection and confidence, seen biometrics viability fundamentally affected the strength of the relationships between both caught guard and saw security with confidence (Morgan, 2019)

Strong authentication is a necessary but loosely established principle. Standard government identification certificates are somehow used as evidence of the identity of the credentials holder that is strong or lawfully recognized. This power is based, depending on the nation, on a one-to-one mapping of the person to identifiers or database registry entries or on a decentralized yet stable record of being aware over the lives of the same name. Good authentication online or offline intuitively implies a comparable degree of safety to the conventional paper identification papers of the electronic environment. This also refers to technical specifications for the initial identity check and authentication methods. For instance, initial personal registration may be expected, which is a direct distinction from ad hoc registration for most Internet-based services. Simple password-based authentication is often considered a poor one, and two considerations should be used in good authentication, preferably physical took paired with memorized secret code or biometrics.

## Password-Based Systems

Not all domestic programmes explicitly comply with these standards in operation. Passwords are used extensively in authentication but are not a reliable tool. Its benefits are customer acquaintance, low costs and relatively quick rollout for service providers. However, strong passwords are difficult to recall, and it is a user's burden to create separate high entropy passwords for various services. As passwords are likely to be leaked, users need to change them regularly. Single sign-on schemes and password safeguards can help users deal with the exhaustion of passwords but do not obliterate password issues. For these purposes, passwords are not regarded as highly authenticated and are seldom used as the only way to ascertain the citizen. But in some countries, password protection is also available. The examples from many countries will be discussed. For several web-based services in South Korea, users must authenticate their true identities even to book a movie ticket, for example, a few years back, most websites only used the individual's name as their secret password as a username and registration name (Oh et al., 2010). However, neither of the providers adequately protected their customer databases, and nearly half of the citizen identification numbers were exposed in multiple attacks, allowing for identity theft. The device had obviously to be changed. Nowadays, users are certified by visiting a service point where the user ID is checked as an I-PIN ID string and a different pass path. If the keys are leaked, you can change the I-PIN ID. The user can select the I-PIN ID, but it must be original. Besides the I-PIN scheme with passwords, smartphone automation via SMS and electronic certificates for authentication used mainly for internet banking is also a feature in South Korea.

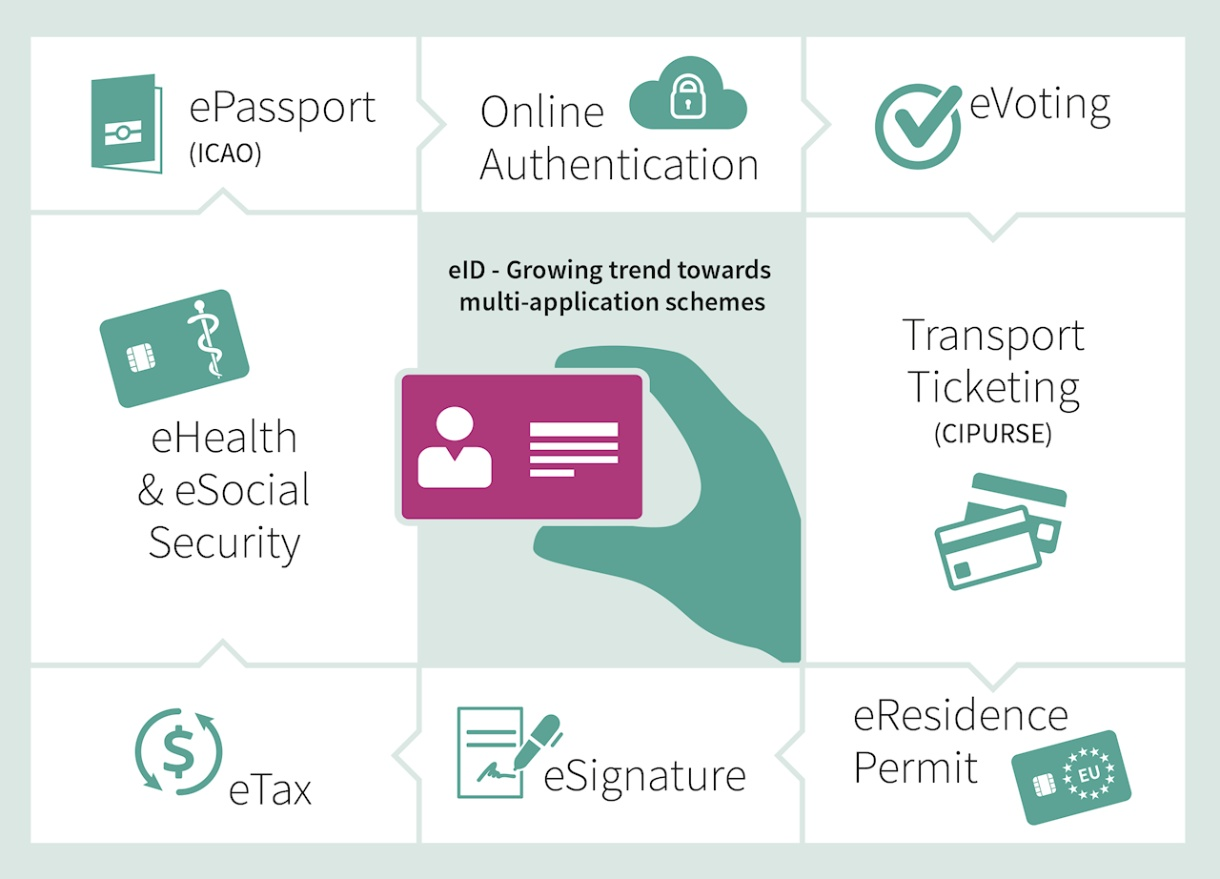


Figure 6 - National electronic ID - Infineon Technologies.

The four layers of e-Pramaan in India are the same. Authentication based on passwords, such as unique keys, hardware or software codes or biometry, is the first authentication process that can be used individually or in conjunction with other authentication techniques. A user's physical identification card is verified during authentication. However, it is also possible to have your registration, whether the password is sent via SMS or postal service. In 2000, New Zealand started to manage its name (Tu and Thomborson, 2009). The system is now known as RealMe and has high-entropy passwords for a single login system. A letter, numbers, and unique characters must be used in a password. If someone in New Zealand resides in a nearby post office where a picture from the customer is taken and added to their email, they can open a RealMe account. If the user is not a New Zealand resident, visas or other paperwork are required. However, an unchecked account can be created by a customer only with services that don't need strong authentication. RealMe also offers better, later defined two-factor authentication. The RealMe user can apply additional checked information such as his address to the account in addition to authentication. If the user approves, the online services may then use that information. This makes it simpler and quicker for the customer to register for new programmes, so they do not have to complete all their details. Saudi Arabia closely regulates the Internet. Traffic is all traffic into a pure government monitoring national content screening scheme. Users must validate their identities at an e-ID authentication office in which they collect a username and password before using any e-services. The recovery scheme for passwords is focused on responses to the recall questions during enrollment. Saudi Arabia has also begun to deploy an intelligent e-ID with electronic chips to protect them from forgery and fingerprint detection instead of for online authentication.

## Biometric Confirmation



Figure 7 - Biometric Identification.

To resolve the trouble of secret word the board and improve the ease of use of validation frameworks, biometric confirmation has been broadly contemplated and has pulled in special consideration in both the scholarly world and industry.

Numerous biometric validation frameworks have been explored and grown, particularly for cell phones. Be that as it may, the current biometric validation frameworks have deserted. Some organic highlights have not been profoundly researched. The existing frameworks could be helpless against assaults, for example, replay assault and experience the ill effects of client protection interruption, which truly impede their wide acknowledgement by end clients. The writing comes up short on an intensive survey on the new advances of biometric validation with the end goal of secure and protection safeguarding recognizable proof. In this paper, we group and altogether audit the current biometric verification frameworks by zeroing in on the security and protection arrangements. The investigation is based on the risks of biometric validation and proposes various standards to get and security protecting verification. We further survey the current works of biometric confirmation by examining their disparities and summing up the benefits and disservices of each dependent on the proposed rules. Specifically, we explore the issues of aliveness recognition and security assurance in biometric verification. Considering our study, we sort out various open research issues and further determine different huge research headings worth noting in future research (Rivera, 2019).



Figure 8 - Biometric Confirmation via Smartphone.

The standard username/secret key or PIN-based confirmation plot, which stays the most famous type of validation, has been demonstrated shaky, dull and defenceless against speculating, word reference assault, key-lumberjack, shoulder-surfing and social designing. Because of this, countless new elective strategies have, as of late, been proposed. In any case, a large portion of them depends on clients having the option to precisely review perplexing and bland data or utilizing additional equipment (for example, a USB Key), which makes confirmation more troublesome and confounding. In this paper, we propose a Digital Memories based client confirmation plot embracing homomorphic encryption and a public essential encryption plan which can ensure clients' protection adequately, forestall following and give staggering security in an Internet and IoT climate. Additionally, we demonstrate our plan's overall dependability and security contrasted with different techniques and present a presentation research and promising assessment results (Hamidi, 2019).

A classic example is Estonia, where electronic identification was established as the world's first to function. Identity is based on the 2002 introduction of e-ID cards. In the early days, online bank credentials became the key authentication mechanism that eventually replaced e-ID. 90% of Estonians now have to work e-ID cards, such as digital signatures, online polls and public transit tickets for all elections in two major towns, Tallinn and Tartu. Tickets are available to all Estonians (Kitsing, 2011).

It should be noted that 24.3 per cent of Estonians cast their votes online during the 2011 Parliament elections (Kitsing, 2011). A smart card consists of a computer chip that allows sensitive data to be processed and saved. This chip can be incorporated into different plastic cards: credit cards, identifiers, school cards, cards with loyalty etc. In general, one of the two networking interfaces offers an intelligent card: touch and contactless. Some smart cards can offer both interfaces (Scherzer, 2002). A contact card involves communication with physical contacts, which are placed into the reader of a card. Contactless cards, by using electric magnetic induction technology such as RFID or NFC, can be reached wirelessly in a limited range. Smart cards provide a manipulative atmosphere in which security-related information, including user passwords, can be stored. User information may also be written on the card's back, such as photographs, names, User IDs, birthdate, etc. Thus, most intelligent cards can have compulsory identification cards, and many today have intelligent card functionality. There are no additional e-ID cards for people. Most devices have contact cards, but some of the latest designs are contactless. The advantage of smart cards compared with passwords is that users have a brief hidden PIN and have two methods for verifying their code and physical card. The chip's key objective is however to increase falsification security of cards and to enable the offline storage of additional information such as biometric data. Just a few of these cards are actively used for online authentication on the Internet. The technical explanation for this is that the card itself is not enough for online authentication: to allow the same card for all online services, a national public-key infrastructure or single sign-on scheme is needed. Numerous countries use intelligent card security, such as Australia, Portugal and Switzerland. In 1999, the European Parliament adopted the Digital Signatures Directive in many countries began developing electronic identity. There have been several discussions, though, and the authentication schemes begin to be used extensively just now, 15 years later.

## Smart-Card-Based Systems



Figure 9 - Smart eID Cards.

Next, we have examples of countries that use citizen authentication intelligent card technologies. As a compulsory government authentication technology, Germany has an electronic id card. It was implemented in 2010. It is based on NFC technology. It provides Offline Verification, Optical Biometric Passport pictures and a Digital Authentication Certificate and digital signatures. For card readers and applications that can be used for the digital signature, there are two protection levels in the device. There have been found vulnerabilities such as ransomware recording PIN codes, but both need to have the card reader during misuse. A separate PIN is secured for the digital signature, and a reader with an integrated keyboard is required for signature. Many counties have other intelligent cards that are used to recognize residents and electronic identification cards. Germany has digital insurance cards with patient information, for example. For historical purposes, regulatory borders between government offices or for supposed confidentiality reasons are not paired with an identification card.

The electronic chip of the Estonian ID card is broadly utilized in Estonia to recognize the cardholder to a machine. For instance, the electronic ID card can gather awards in client dependability programs, verify to public printers and self-checkout machines in libraries, and even open entryways and limited access regions. This paper contemplates the security parts of utilizing the Estonian ID card for this reason. The report shows that the way the ID card is now being used gives practically zero affirmation to the terminal about the personality of the cardholder. An ID card emulator is fabricated to exhibit this, which copies the electronic chip of the Estonian ID card however much as could be expected and can effectively imitate the genuine ID card to the terminals conveyed by and by (Blue et al., 2017). Municipalities issue the CIE card under Italian law, but a digital certificate may be issued by the Ministry of the Internal Affairs Certification Authority, which is held on this card. Italy has a new scheme for accessing electronic government facilities called a National Service Card, besides CIE cards. The CNS is composed of identification certificates and digital signatures. Therefore, it is not an official ID card because it does not have a picture and only municipalities can issue ID cards. Besides, Italy plans to implement the SPID online infrastructure for residents and public and private services in 2015 as a SAMLv2 Identity Provider. The cards listed above can be used in this scheme as authentication tokens. France has now agreed to use smart card technologies to deploy electronic authentication. It will include two photos and two fingerprints, and other details, including marital status, for example, biometric authentication.

Nevertheless, the technology has been resistant because people fear that the biometric data will be passed on to others, and users' privacy will be affected. For several years, this opposition stalled electronic identity for the first time from 2006 to 2008 and was not set for release in 2012. Often focused on a smart card containing an X.50 9 identification and digital signatures certificate and a person photograph and his/her signature, the Spanish 'Documento Nacionales de Identidad electronic You must travel to a National Police station to be authenticated before applying for a passport. A PIN code must be used to protect the card information. Electronic identity cards have also been popular in Asian countries. Municipalities in Japan issue citizen identification cards with an RSA key chip that has been approved by the government. The cards can be used to authenticate online sites and sign digital records. This card is also available from foreign nationals. In addition, an electro-identity system based on smart cards called e-KTP is being developed by Indonesia, one of the world's most populous nations. Theft of identity has led to deployment in recent elections. The e-KTP is constructed on a contactless card with biometric details, including facial, iris, fingerprints and fingerprints. On the other hand, Indonesian cards do not have online certificates.

Data frameworks in the advanced age have gotten progressively reliant on data sets to store much major information. A vital capacity of organized information bases is to house confirmation certifications that check character and permit clients to get to more striking individual details. Confirmational data settings are now and then the aims of an assault when they can lead to more, more useful violations, notwithstanding the arrangement of industry-standard best practice proposals by associations such as the Open Internet Application Security Project (OWASP), the Payment Card Industry Security Standards Council (PCI-SSC). Inacceptable results or inacceptable performance has led to an environment where validation data sets and knowledge is shaky. This was shown in the 2016 openness of a penetrate experienced by Yahoo, where around one billion client certifications were taken (Mumtaz et al., 2019).

The worldwide innovation organization was discovered to utilize out of date security components to ensure client passwords. For example, dated executions pose a genuine danger as they render verification information profoundly powerless against burglary and expected abuse. This paper offers a novel answer for getting validation data sets on resistant Apache workers. The technique applies the suggested best practice instruments as salt, single direction encryption (hashing) and cycles to both previous and recently made passwords put away on shaky frameworks (Giessmann). The proposed arrangement can be executed worker side, with little change to the current framework, unbeknownst to the client. It can improve framework security, help consistency, save protection, and ensure clients.

China is beginning to introduce smart chip ID cards from the third generation. The cards have biometric identification fingerprints. Compared to Western nations, the identification card is commonly used, for example, when purchasing travel tickets or using Internet cafes facilities. However, Internet user authentication should only be used to track criminals and not proactively authenticate online services. The Turkish electronic identification system uses smart cards that include certificates and biometric details such as fingerprints or finger valves and a cardholder's photo (Mutlugün and Adalier, 2009). A section of the information stored on the card, named and certificate, can be accessed by a regular intelligent card reader. Biometric information shall only access with trustworthy card readers and shall be secured by a PIN code. In the last few years, the scheme is piloted, and people should be able to receive digital signature certificates for their electronic identification cards in 2014. South America's smart card technologies are still used, primarily for offline verification. The first Electronic Registry for Civil Identity (RIC) card was obtained by their then-President Lula da Silva in Brazil at the end of December 2010. The passports can be read using contact or contactless technologies, which provide biometric information in the form of a fingerprint (Suoranta et al., 2015). The Brazilian ID card is a travel document in Mercosur countries, including its European counterparts. The digital signature and certificate of identification and photos from the wearer's face and fingerprints are used in Chile's identity cards. The compulsory DNI includes biometric data, including fingerprint and face pictures, social security documents, medical and public transport backgrounds in Argentina, for example; this fears people who fear privacy and families from Argentine history. The DNI is a compulsory national identity card for example.

Mexico first started to distribute electronic cards to children. The card contains iris scans, fingerprints and a photograph as biometric stuff. Identity in Russia has been tested using an internal passport in offline facilities. A clever card replaces them with a wireless stamp of signature. In addition, South Africa is renewing its passport identification paper Identity book to a smart card in the coming years. As seen by the long list of above countries, smartcard solutions are common among countries with or improving their citizens' electronic identity. The movement is generally to integrate intelligent card identification into national identification cards. The main variations are the number of non-identity details included inside the card itself and whether online authentication keys and infrastructure for public and business Internet services are available. Countries with a broad Internet coverage inevitably place greater stress on the authentication of data online and less on the storage of on-card data (Schneier, 2005).

## Non-governmental Identity Providers

### Post Offices

The postal service has become a state monopoly in most countries and, although rivalry has hit the transport of mail, the postal offices continue to be seen as trustworthy officials. The postal service still has a vital job to hand out recorded letters to the right people, including official letters, and therefore requires procedures and qualified staff to validate any citizen's identity. This history allows Post Offices to sell electronic identification certificates. The Swiss Post, for example, offers a digital identity and signature identification in Switzerland that is either saved on a smart card or a USB stick. The token must not be purchased in person from the post office if the recipient's identification is checked by an identity card or a passport. The token is purchased by online form. The PIN code that protects details from the card or USB device can be determined by the user. The intelligent card includes a special card reader, but nearly any device can access the USB stick without any new hardware being installed. The user manuals provide many security threats and risks to the device, e.g., by typing the PIN in a monitor, but also by tapping it against. Today, many people choose a desktop computer over a handheld device. The mobile service SuisseID requires users to use mobile device SuisseID authentication. The device supports Apple, Google, Samsung and Nokia. The variety of mobile devices is a challenge for mobile identity systems which reach the population as a whole.

Verification is the crucial security administration utilized in practically all far off applications. All such delicate applications over an open organization need verification instruments that ought to be conveyed in a confided in manner. In this paper, we plan an RSA based confirmation framework for keen IoT climate over the air network utilizing cutting edge industry principles (Dzikrullah and Rinjani, 2017). Our framework gives security administrations including X.509 declaration, RSA based Public Key Infrastructure (PKI), challenge/reaction conventions with the assistance of intermediary actuated security specialist co-op. We depict a creative framework model, convention plan, framework engineering and assessment against known dangers. Additionally, the executed arrangement planned as extra help for numerous other touchy applications (keen city applications, digital actual frameworks and so forth) which needs the help of X.509 authentication dependent on hard tokens to populate other security administrations including classification, uprightness, non-renouncement, protection and secrecy of the personalities (Juan, 2019). The proposed plot is thought about in contrast to known weaknesses and given detailed research with mainstream realized validation plans. The outcome shows that our proposed conspire to relieve all the realized security hazards and give the most elevated level affirmation to brilliant contraptions.

Internet of Things (IoT) has gotten perhaps the main advances as of late on account of having the different application areas. The assortment of utilizations brings about a lot of clients' private data dissemination that will represent a principal security concern. Client validation is a critical factor in the IoT climate as it permits the client to speak with the gadget safely. The joining of validation innovations with IoT guarantees secure information recovery and vigorous access control (Liu, 2019).

### Bank Credentials

The banks are also a relatively trustworthy group of NGOs. Banks are taught to be vigilant about coping with high-value purchases until their clients are authenticated. Most protection protocols of banks apply national or international requirements, and banks' enforcement is essential if undue liability is to be avoided. They also track the extent of fraud constantly. In addition, anti-money laundering law makes it strictly necessary for banks to authenticate and recognize their clients. Banks are still using keys, but gradually based on smart cards, to enforce their own safe electronic identities. Bank cards can be used as identification token with a smart card chip if the customer already has a card reader's phone. For chip and PIN connectivity based on the Chip Authentication program specifications, some banks provide their customer with special standalone players. A collection of once-passwords that have the benefit of being low-technology and cheap is another good authentication tool used by the banks. To obtain credentials, a customer can go to a bank's office, enter into a customer agreement and show the bank officer his or her passport or other official ID. This authentication is the basis for possible online authentication using the passwords provided by banks. Since the banks have online authentication systems, the use of these systems on other services is natural. This is particularly the case in regions with electronic banking developments, like many countries in northern Europe (Nyman et al., 2014). The banks had to identify standard APIs to authenticate third parties as default identity suppliers. Nine Swedish banks have a bank identification service, for example, and all Finnish banks are using TUPAS, created by the Finnish Financial Services Federation. Many government departments in those countries also recognize online authentication. The gateway Electronic Gates of the Lithuanian government, for example, uses authentication online. Using an online payment method for authentication purposes, whether it closely connects a customer's identity, is one way that banks are expanding their role as generic payment providers. For instance, architecturally the Finnish TUPAS authentication is similar to a national online payment method and uses the same OTP credentials. As said, the authentication offered by the banks has the benefit of being comparatively trustworthy institutions and of being essential to check the identity of their consumers vigorously. The passwords for consumers are known and there are no apparent costs for their use. Authentication is just a small income source for the banks themselves. However, verification locks consumer banking consumers in existing accounts, which are recognized as identity providers by most companies. The main drawback is that authentication becomes difficult if an individual does not have a supported bank account. International students who would authenticate to enrol at the university are a familiar example of this who still require registering before receiving a bank account. Another drawback is that, as the use of bank passwords is increasing, online banking protection can be affected (Fumy and Paeschke, 2010).

In their online citizen authentication programmes, several countries are either at the pilot or implementation stage. In certain jurisdictions, however, people and lawmakers have a strong ideological opposition to cards, especially if their deployment involves a central registry for all residents or if possessing or carrying the card is mandatory. This may also be considered an attack on citizens' freedom. Nonetheless, in these countries, the growth of public and commercial web platforms is also a significant goal. In the UK, for example, the Identity Cards Act was passed in 2006, introducing Id Cards that can be used to fly within the European Union (Tamrakar et al., 2015). Like fingerprints, iron scans and facial images, the biometric details are obtained from a database. The act was later reversed due to primarily worries regarding database security, and passports were needed for those who had already bought the card. The latest 2010 Identity Documents Law allowed the deletion of personal records obtained from the National Register of Identity. Several people in the UK use their driver's licenses as identification forms, and there is even a citizenship passport for young people to use as evidence of age. However, the United kingdom has a government gateway that serves as an online public services hub. It provides two types of authentications: passwords sent via mail after registration and electronic certificates not given anymore. The government released in the United States recommendations for agencies to use electronic identification to eliminate document usage and to accelerate administrative processes. The United States has agreed to encourage people to access government services rather than a centralized government service by selecting the provider of authentication between private sector partners whose certificates already exist. No single device has been widely used, and various government departments use service-specific keys or commercial smart card solutions. In comparison to the department-specific password login, Canada, on the other hand, depends on services in the private sector such as banks to provide access to public services such as the revenue agency.

Many countries have added biometric information to their passports, such as a face or fingerprint. The Japanese passport, for example, has RFID tags with a digital photograph, and EU Schengen member countries must have both a picture and a passport fingerprint. There are also airports where the passport holder can verify his identification by showing the passport to a computer that compares the image on the passport to a photo taken by a machine. This picture is stored in the passport itself. No activities by a passport holder are required to read the data from the chip inserted in the passport. Passports are not, however, commonly used for online authentication.

### Hybrid Systems

Several technologies that operate side-by-side are examples of Finland. Intelligent PKI card-based, one-time password bank credentials and SIM card mobile certificates are accepted without one technology being officially preferred over another. Failure to implement smartcards as the primary way to achieve strong authentication as people choose current or more convenient approaches is the hybrid scheme. The person used to use a mobile phone will easily use cell certificates. The machine is reasonably safe thanks to the PIN and 24-hour coverage of network operators. The passwords can be revoked automatically if the cell phone or their SIM card is compromised. The user must, however, upgrade the SIM card to a new card after revocation. For those that are not familiar with mobile devices, it can be difficult to authenticate (Paul et al., 2011). In Finland, for example, the usage price is Euro 0.17 per authentication, at least relative to bank credentials whose prices are concealed during monthly service adjustments. The authentication price is considered very high. For each authentication case, the service providers relying on the authentication pay a related expense. The Generic Bootstrapping Architecture (GBA) is another telephone framework that reuses mobile network passwords and resources for third-party user authentication. However, this standard was not used extensively, and pilots did not have broad citizen authentication but individual implementations—besides, the two-factor authentication of cell telephone functions as a trusted channel. For example, if additional protection is required, the RealMe authentication mechanism in New Zealand uses two-factor authentication. The program sends a verification code customer's cell phone to validate the code manually into an online service. Two-factor authentication is generally assumed to be safer because it is not sufficient to steal user names and passwords, and a physical mobile device is still required. The customer can detect if his cell phone has been compromised rather than if his password has been stolen. Recently, it was a worry that malware or non-trustful applications would affect messages received on a smartphone using the handset as trusty channels. Trusted computing systems that insulate the credentials from the rest of the computer software can provide a technological solution by hosting E-IDs or implementing the new e-ID architecture. The diversity of mobile applications restricts their use for general citizenship, but the next step of electronic citizenship will be if norms develop.

# Research Methodology

## Data Collection Method

The research includes the secondary data collection method. All the data has been gathered from the research papers, articles, and genuine sources. The theme has numerous sorts of research accessible so dissecting the data becomes easy (Park and Lee, 2018). While managing optional information sources it is important to consider the realness of the data giving sources. The protection of the data gave will be managed will prime concentration and care. Data won't be produced and both positive and negative effects will be thought of while taking the auxiliary information assortment.

## Data Analysis Method

The data analysis method that will be implemented in the research is thematic analysis. The thematic analysis refers to the identification of a certain pattern or any theme, that is beneficial in determining the results and lead to a conclusion. The secondary data that will be collected from various sources will be analyzed using the thematic analysis method and the potential privacy and security risks that are being faced again and again will be identified. This will help in determining the potential privacy and security risks, by taking an example of Aadhar Card and the recommendations will be then provided based on the findings and analysis.

## Ethical Consideration

The research will be finished with every one of the methodologies being valid. No untrustworthy methodology will be taken into training while at the same time making the research (Kumar, 2018). The data of the creators and the sources will be kept hidden, and on the off chance that they will be promoted, it will be done after the appropriate assent of the person. The data won't be controlled and every one of the measurements will be taken as acquired. With the adjustment in insights, the outcomes can be changed, so it will be the fundamental worry to carry out the total interaction appropriately and with the most extreme accuracy. While doing the research no mischief will be created or no issues will be done in the research parameters (Sherif, 2018).

## Research Design

The research will be developed with the guide of subjective information. Subjective information doesn't include numbers and figures while managing them. It manages the words, which makes it simple for interaction and use. Non-numeric information types are viewed as not hard to rehearse in a report. Innovativeness is the essential main impetus as this cycle is an open-finished interaction. In contrast with the quantitative information, subjective information in research configuration is viewed as better as far as cash saving. The quintessence of the research subject is conveyed with the inquiries and investigation of subjective data (Chatfield, 2020).

# Experimentation

The aim of this project is to survey the public about their opinion on the risks regarding the privacy and security of a person on the internet trying to authenticate a specific action with an eID. To this extent, the objectives required to achieve this aim are as follows:

* Collect data in the form of a survey of the public regarding the safety and security of the internet.
* Discuss through literature review the progress of the eID card technology, the risk factors and the probable solutions.
* Analyse the data collected from the survey using statistics to gain a deeper insight into the problem from the perspective of the end-user.

## Dataset

The data was collected from a survey conducted in the US. Internet privacy has gained widespread attention in recent years. To measure the degree to which people are concerned about hot-button issues like Internet privacy, social scientists conduct polls in which they interview a large number of people about the topic. This research will analyze data from a July 2013 Pew Internet and American Life Project poll on Internet anonymity and privacy, which involved interviews across the United States. The dataset has the following fields (all Internet use-related fields were only collected from interviewees who either use the Internet or have a smartphone):

1. **Internet Use**: A binary variable indicating if the interviewee uses the Internet, at least occasionally (equals 1 if the interviewee uses the Internet, and equals 0 if the interviewee does not use the Internet).
2. **Smartphone**: A binary variable indicating if the interviewee has a smartphone (equals 1 if they do have a smartphone, and equals 0 if they don't have a smartphone).
3. **Sex**: Male or Female.
4. **Age**: Age in years.
5. **State**: State of residence of the interviewee.
6. **Region**: Census region of the interviewee (Midwest, Northeast, South, or West).
7. **Conservativeness**: Self-described level of conservativeness of interviewee, from 1 (very liberal) to 5 (very conservative).
8. **Info On Internet**: Number of the following items this interviewee believes to be available on the Internet for others to see:
   1. Their email address.
   2. Their home address.
   3. Their home phone number.
   4. Their cell phone number.
   5. The employer/company they work for.
   6. Their political party or political affiliation.
   7. Things they've written that have their name on it.
   8. A photo of them.
   9. A video of them.
   10. Which groups or organizations they belong to.
   11. Their birth dates.
9. **Worry About Info**: A binary variable indicating if the interviewee worries about how much information is available about them on the Internet (equals 1 if they worry, and equals 0 if they don't worry).
10. **Privacy Importance**: A score from 0 (privacy is not too important) to 100 (privacy is very important), which combines the degree to which they find privacy important in the following:
    1. The websites they browse.
    2. Knowledge of the place they are located when they use the Internet.
    3. The content and files they download.
    4. The times of day they are online.
    5. The applications or programs they use.
    6. The searches they perform.
    7. The content of their email.
    8. The people they exchange email with.
    9. The content of their online chats or hangouts with others.
11. **Anonymity Possible**: A binary variable indicating if the interviewee thinks it's possible to use the Internet anonymously, meaning in such a way that online activities can't be traced back to them (equals 1 if he/she believes you can, and equals 0 if he/she believes you can't).
12. **Tried Masking Identity**: A binary variable indicating if the interviewee has ever tried to mask his/her identity when using the Internet (equals 1 if he/she has tried to mask his/her identity, and equals 0 if he/she has not tried to mask his/her identity).
13. **Privacy Laws Effective**: A binary variable indicating if the interviewee believes United States law provides reasonable privacy protection for Internet users (equals 1 if he/she believes it does, and equals 0 if he/she believes it doesn't).

## Analysis

The sample population size for this survey was 1002 people. Various questions were asked and data was collected and stored accordingly. The following analysis was done:

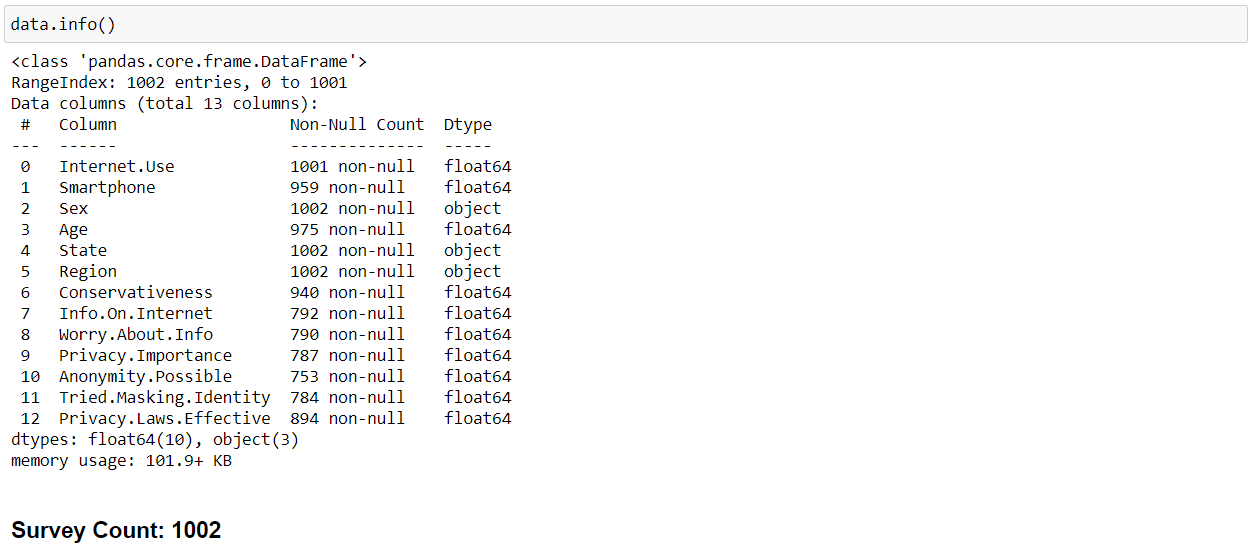


Figure 10 - Metadata on the Survey data.

Figure 10 shows the metadata on the data collected from the survey. The largest count value in the dataset features will give the amount of people that participated in the survey and provided useful and significant information.

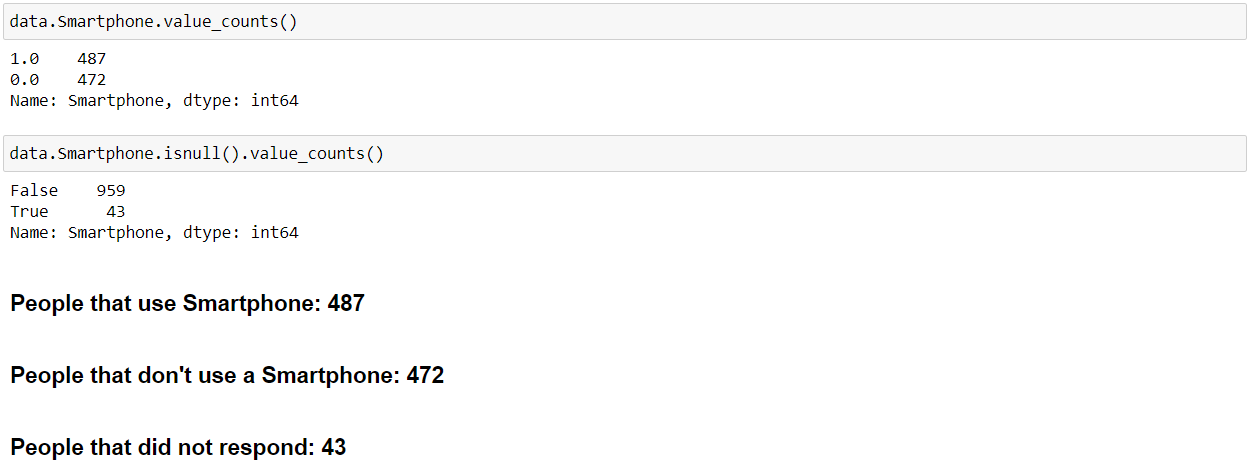


Figure 11 - Answers regarding Smartphone usage.

Figure 11 shows the analysis of people in the survey that are equipped with smartphones and use it as a part of their daily lives. From the above image, it can be inferred that out of the 1002 people, 487 people carry a smartphone with them, 472 people do not have a smartphone and 43 did not respond to this question at all. The number of people that do not have a smartphone is unexpectedly high given the age of technology and social connections. But this itself is not enough. Smartphone usage is only connected to this research since it makes easier for the public to connect to the internet wherever they are with relative ease. Therefore, this data has to be complimented with the usage of the internet. This is provided by Figure 12. This provides us more insight into how many people are actually connected to the internet.

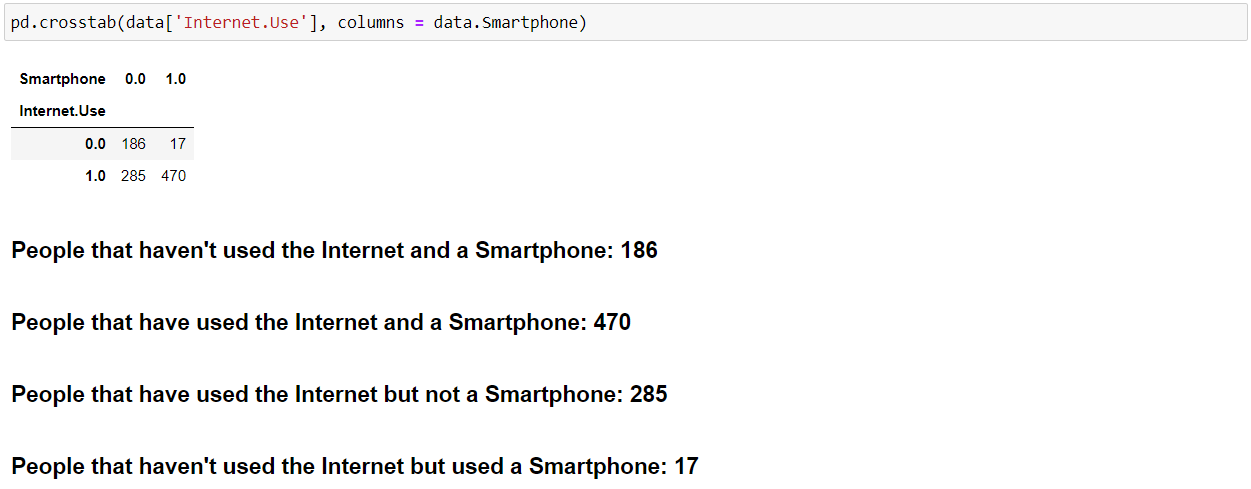


Figure 12 - Internet usage along with the Smartphone.

For the other questions of the survey, the analysis will be done in terms agreement and disagreement count. From 1002 people, the number of people that are concerned about their information and data on the internet are 48.86%. The percentage of people that are concerned is very high. It can be inferred that almost 50% of the sample population is not sure regarding their data security on the internet. With so many people concerned about their privacy and security on the internet, people must have looked into the solutions regarding this issue. The most common solution considered in this survey is to become anonymous on the internet. 36.92% of the sample population believe that it is possible to become anonymous on the internet and 16.32653% of the population has actually tried to become anonymous on the internet disregarding the results of their efforts. The concern at this point of the data analysis is that even though there is a large number of people that support the internet which resulted in its popularity, how come a small sample population provide a strong probability in the opposite direction. To solve this anomaly, age was considered to be a deciding factor. It can be fairly assumed that people that that ages above 45 may not be able to appreciate the internet and cause more of an issue regarding privacy. The trend of the data collected with respect to age is as follows:

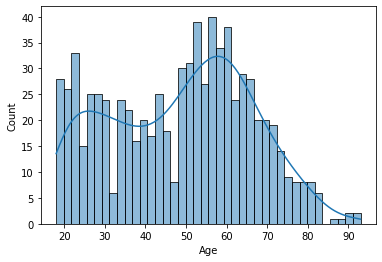


Figure 13 - Data Trend with respect to Age.

The author was interested in whether certain characteristics of interviewees, for example their age or political opinions might affect their opinions on the topic of the poll (in this case, opinions on privacy). Figure 13 helps investigate the relationship between the characteristics Age and Smartphone and outcome variables Info On Internet and Tried Masking Identity. People that do not trust the privacy and security measures of the internet often choose to mask themselves and surf the internet. Approximately 11.75% of the population under study and consideration mask their identities while surfing the internet.

# Results

In certain nations, the provider of electronic citizens' identification is not the state itself, but a trustworthy agency. The postal service has become an official monopoly in most countries, and even though it has come into contact with mail, the post offices are now considered to be a kind of trustworthy government agent. Furthermore, the postal service carries out the vital duty of sending recorded letters to the right people, including the official ones, requiring a procedure and training staff for verification of a citizen's identity. This history allows post offices to provide electronic identification credentials. For instance, Swiss Post offers digital identification and signature credentials in Switzerland that are either stored on a smart card or USB stick (Schryen and Rich, 2009). The token is purchased electronically but must be fetched in person by the postal service until the recipient's identification is checked by a passport or identity card. The user may determine the pin code that protects the card or USB device details. A special card reader is required for the intelligent card, but almost any device will use this stick without having to add any new hardware. The user manuals list several security hazards and dangers against the programmed code, such as typing in a PIN on a hacked device but against it as well. (Markantonakis et al., 2009). Most people now prefer a desktop computer over a handheld device. The SuisseID Mobile Service enables mobile device authentication to be enabled (Mettler and Guenduez, 2019).

The leakage of biometric information on an e-passport faces its unique risks: security risk both for its use and for external biometric systems. Biometric information can play a major role in E-passport systems as designated as optional in this figure. The "world exchange" feature is a facial image—a digitized headshot—which means the global norm of biometric authentication will be used. It is defined by the ICAO guidelines as the obligatory global interoperability minimum. Fields of iris and fingerprint data are optional, which can be used at the discretion of the issuing country. We note that the US-VISIT service includes visitors' fingerprint biometrics which can be saved on an ICAO e-passport in the relevant fields. Biometric identification system advocates also say that the credibility of such schemes should not require confidentiality. For example, the publication of an image of John Does' fingerprints does not prevent Doe's identity from being verified: it must always, in theory, be seen to be compared between the general public image of such prints. This is all the truer in a safe setting such as an airport, which might not be easily physical spoofing. In the US-VISIT initiative and the initial implementation of ICAO passports, confidentiality seems to be especially superfluous at first glance. As discussed above, the worldwide biometric is recognizable. The banks are also a relatively trustworthy group of NGOs. Banks have been seen to take caution in handling high-value transfers as their customers are authenticated. Many of the security protocols of the banks follow national or international requirements and bank enforcement is essential if undue liability is to be avoided. The extent of the fraud is often continually monitored.

In addition, law to prevent money laundering imposes strict conditions for banks to authenticate and recognize their clients. Banks have their own secure, password-based and more and more smart card-based electronic identity deployment (Lyon, 2009). Bank cards can be used as identification tokens with an intelligent card chip because the customer has already a device with a card reader. Some banks provide their customers with special standalone readers for the Chip-and-PIN-based login according to CAP. The list of one-time passwords (OTP), which has the benefit to be low-tech and cheap, is another powerful authentication tool used by banks. For the certificates to be obtained, a client must go to a branch of a bank, create a customer connection and show the bank officer the passport or other official documentation. This authentication shapes the foundation for potential online authentication with the credentials provided by the bank. Since the banks have online security schemes, other services will naturally be used. This extends particularly to regions that, like many northern European countries, have evolved electronic banking. The banks had to identify standard authentication APIs for third parties, to become generic identity providers. For egg, nine Swedish banks have BankID, and all Finnish banks have TUPAS, a common service API (Rissanen, 2010) defined by the Federation of Finnish Financial Services. Many public institutions in those countries also accept the authentication of online banks. For instance, online bank authentication is used by the Lithuanian Government Electronic Gates portal (Laurinaitis and Štitilis, 2008). One way in which the function of the banks as generic authentication providers has grown is to reuse (or misuse) for authentication purposes if an online payment system closely links the identity of the online consumer to the payment. The Finnish TUPAS authorization, for example, is very similar to a national online payment procedure architecturally and uses the same OTP credentials. As said, the authentication of the bank has the benefit that the banks are comparatively trustworthy institutions and, in any event, they have to firmly check their customers' identities. The certificates for consumers are known and use of them does not cost visibly. Authentication offers only a small source of proceeds for the banks themselves, but authentication services lock consumer banking clients in existing banks recognized as identity providers by most companies. A huge downside is, if a person does not have a sponsored bank account, the authentication becomes difficult. International students unable to enroll in university, but must register to get a banking account, is a familiar example of this. Another drawback is that with the increasing use of bank credentials, online banking safety can be affected.

Key US and other governments efforts seek to fuse the identity card generation with radio frequency identification (RFID) and biometric technology. Towards fraud reduction, identification controls are easier, and safety is improved together with RFID and biometric technology. Around the same time, new threats arise from these developments. With a modern authentication platform and a special focus on its implementation on passengers, we examine the privacy and security ramifications of this global experiment. The government of the United States, as part of its policy for U.S.-VISIT, mandates the acceptance in the United Nations Visa Waiver Program (VWP), including Japan, most Western European nations and a few others, of biometrically allowed passports by 22 countries by October 2006. Biometric information will be included in every US passport by the end of 2005. The recommendations published by the ICAO, a United Nations organization with a Mission to Set International Passport Requirements, are dependent on the passports. The ICAO Recommendations, as outlined in ICAO Document 9303, call for RFID chips and data storage and wireless transmission microchips to passports. The ICAO recommendations are referred to as 'standards' in this article. They are a standard de facto, but not a standard ratified. Such chips will be present in the initial rollout of United States passports that are biometrically enabled, and in other countries' biometrically enabled passports. In a few years, next-generation passports often referred to as e-passports, would be a prominent and popular way. The ICAO Specification states that the biometric for identity authentication in travel documentation is recognized as internationally interoperable. Thus, e-passports contain digital photos of their bearers' faces. Furthermore, the specification specifies optional biometric fingerprints and iris results. In reality, in addition to the headshot in the US-VISIT programmed visitors are required to provide two fingerprint photographs. The ICAO specification also provides for the inclusion of writing capabilities for the saving of details like digital visas in e-passports. Of note, in a project that predated the ICAO standards, one nation has already used ePassport’s. Since 1998 Malaysian passports have been fitted with a chip with a picture of the passport holder thumbprint, a second-generation e-passport from 2003 containing only the details derived from fingerprints. When a Malaysian citizen is flying through Kuala Lumpur International Airport a digital gate, which reads the thumbprint from the chip and compares it to a scanner-pressed thumbprint. More than 5,000,000 e-passports are currently being circulating in the first generation and 125,000 are in the second generation. E-passports are important to themselves, but, as harbingers of a tsunami of RFID and biometrics in identification papers, they still deserve to be scrutinized. For example, the Personal Identity Verification (PIV) card is another next-generation ID card intended for use in the United States shortly. For workers and contractors federal government in the USA, the PIV cards would function as ID badges and cards of entry. The National Institute of Standards and Technology is developing rapidly as a standard for government ID cards (FIPS 201). We assume that PIV cards would incorporate the same mix of technological processes as e-passports: the RFID and biometrics combinations. However, fingerprint identification will likely be the biometrics of choice for PIV cards. At the time of the writing, a measure, the Real ID Act, was recently passed by the United States House of Representatives; this seems to be a potential catalyst for states to issue biometric cards and potentially RFID tags too.

Mobile providers now also provide electronic identification in many countries in addition to banks. The Mobile Certification consists of a smart card which is a small smart card that connects a mobile phone to the user and the subscriber account, which is placed on the subscriber identification module (SIM) card. The keys can be used for user authentication, data encryption and verification, and transaction confirmation (Bennett and Lyon, 2008). The user gets the phone's confirmation message and types in a PIN code during the authentication process. The networking maintainer serves as a trustworthy party and notifies the service of effective authentication (He and Paar, 2007). The particulars can differ somewhat between countries, but the basic protocol is the same. In Austria, Finland, Estonia, Latvia, the Netherlands, Norway, Poland, Slovenia and Turkey, for instance, mobile certificates are in use (Shukri and Hafiz, 2015). The user who is used to using a cell phone will use mobile certificates easily. The machine is reasonably safe with the PIN code and 24-hour network operator customer service. The keys will be removed automatically if the cell phone or its SIM card is compromised. The user must, however, upgrade the SIM card to a new card after revocation (Suoranta et al., 2015). For people who are not familiar with cell telephones, authentication may be difficult. In Finland, for instance, a user's price per authentication is 0.17 euros, which is at least considered high relative to bank passwords which have cost secrets in monthly improvements to service. For each authentication case, service providers that rely on authentication often pay a comparable charge. Generic Architecture of Bootstrapping (GBA) (Sher and Magedanz, 2006) is another phone-based framework reusing third party authentication credentials and technology in the mobile network. This norm is not commonly implemented, however, and pilots do not have general citizenship authentication but rather unique applications. Two-factor authentication is another means of using cell phones, which makes a telephone a confidential contact channel. For example, if extra protection is required, the RealMe authentication scheme in New Zealand uses two-factor authentication. When authenticating, a verification code is sent to the user's cell telephone and the code is manually entered into the online service to validate the connection (Chang and Wu, 1991). Two-factor authentication is generally considered more robust because it is not enough to steal username and password, and the SIM card is still used on the physical mobile device. The user can detect whether the cell phone is robbed rather than stolen. A recent worry that using the phone as a trustworthy source could compromise messages received from a smartphone is that Malware or untrusted apps could cause (Schneier, 2005). Confident computer technology to separate the credentials from the rest of the system applications may offer a technological solution by eID hosting or deployment of modern eID architecture (Tamrakar et al., 2015), but such systems have not yet been deployed. The diversity of mobile networks currently restricts its use in general citizens' authentication, but if norms develop, the next path of electronic citizens' identification will also be.

The ICAO and PIV ventures have the same goal: clear authentication of documentation that describes their supporters unequivocally. The reliability of ID card authenticators depends on data integrity and physical integrity. For instance, DOA’s passport must bear an irrefutable pedigree snapshot, with guarantees that no replacement or alteration has been carried out for the authorities to determine John Doe's identification with certainty. Passports that enable unauthorized individuals to reach a country without this guarantee may be forged. Strong authentication demands more than manipulation tolerance. The privacy of data contained on the ID card is crucial too. Data security is critical. For the value and credibility of an authentication scheme, the protection of biometric and biographical data is important. Data confidentiality in particular offers a valuable form of security against falsification and spoofing. Protecting the data on the e-passport from unauthorized access is also an important aspect of system security. For other reasons too, the security of confidentiality for storage data is essential. RFID and biometrics are a technology that is extremely privacy-sensitive. Passports carry sensitive information like birthdate or ethnicity. The anonymity, physical safety and mental comfort of next-generation passports and identity cards rely on the consistency and architecture of the data security mechanisms.

Many of these schemes may be regarded in two ways as hybrid systems: either one technological mechanism incorporates two or more authentication mechanisms or several systems operating side by side with separate methods are part of the national total infrastructure. In the case of a multi-method authentication system, any physical token (intelligent card), PIN code and biometry are usually combined. Software and SMS are popular as a second authentication medium in business networks, but the widespread use of citizenship does not occur. By allowing the use of a single method for some facilities, multi-method authentication systems may provide various degrees of safety. The Indian e-Pramaan, for example, offers various authentication levels (Belapurkar et al., 2009). Many nations have now applied organic data in the form of a face picture or fingerprint to their passports. The Japanese passport, for example, has an RFID sticker with a digital snapshot (Garfinkel and Rosenberg, 2006) and the Member States of the European Union that are part of the Schengen area must have photographs and fingerprints on their passports. Many airports have an electronic passport inspection where a biometric passport applicant may check their identification. The passport is displayed on a machine comparing the picture contained in the passport with the actual picture taken by the machine itself. No acts by the holder of the passport are essential for reading data from the chip embedded in the passport. The passports are not, however, commonly used for online authentication. One example is Finland, where intelligent PKI based applications, bank credentials with one-time passwords and mobile SIM card certificates are all approved without any official preference for one technology over the others. One system can also be used as a side-by-side example. This hybrid scheme results from the failed implementation of smart cards as the main authentication mechanism, as people favour current or more convenient systems.

## Countries Without Citizen Authentication

In their online citizen authentication programmes, several countries are either in the pilot or implementation process. But people and lawmakers are strongly opposed to cards in some regions in terms of ideology, namely if their deployment involves a central registry of all residents or if it is necessary to own or hold a card. This can also be seen as an attack on citizens' freedom. Nevertheless, in these countries, the growth of online public and commercial resources is also a significant aim. The Parliament adopted the Identity Cards Act, for example, which introduced identity cards for travelling within the European Union in 2006. In 2006, Parliament passed the Act. Fingerprints, iris scans and face pictures were included in the biometer details stored in a database. The act was subsequently repealed, mostly because of issues about database privacy, and those who already bought the card would now receive passports (Jain and Kumar, 2010). The new 2010 Identity Documents Act allowed the deletion of the personal details obtained from the National Identity Register (Ogasawara et al., 2008). In the UK, some are using their driving licenses as identification cards and there's also a Citizen Card, which young people can use as evidence of age (Beynon-Davies, 2006). However, the United Kingdom has a government portal that acts as an online government services portal. It provides two types of authentications: passwords sent via post-registration mail and non-emitting digital certificates.

The government has released in the USA recommendations for agencies to use electronic identification for programmes to limit paper usage and accelerate administrative processes (Santos et al., 2008). Instead of a centralized governmental agency, the U.S. wanted to provide people access to government services by selecting a private sector verification contractor that already has their credentials (Santos, 2011). There has been no widespread usage of a single scheme and various government departments use service-specific codes or smart card solutions. Canada depends on the expertise of the private sector, such as banks, in addition to department-specific password login to include federal services such as the Revenue Agency (Clement et al., 2008).

# Discussion

When states substitute paper-based id papers with electronic identities, smart cards incorporated in national identification cards prove to be a favoured alternative. This is an obvious alternative for offline authentication, as the handle-proof chip and cryptographic details make it more difficult for identity cards to be copied and falsified. In addition, the chip has a two-factor authentication PIN code or biometric identity information in one single physical box. In India, for example, by 2013, 23% of the population had enrolled for the e-Pramaan scheme. About 2.2 billion individuals (33% of the global population) are expected to have an electronic ID in 2009 and more than 900 million carts have biometrics such as photographs of facial and fingerprint. There is, however, a division between countries where the cards are used mainly for offline identification tests and countries where they contain online authentication cryptographic credentials. There are first category jurisdictions with priority over physical security and citizen power, but still with business solutions and risk assessment to satisfy the need for online authentication and therefore no need for modern authentication technologies. In the second category, examples of high-internet penetration countries are easy to identify and increasingly evolving countries that use emerging technology aggressively to improve their public services. In certain countries, the government is seen as a natural supplier of people' electronic identification because it provides certificates of birth, passports and taxes and benefits to its citizens. Government departments provide databases for store confidential citizens' records, and the existing technology can be used for electronic identification. In addition, businesses relying on government authentication need not spend money to develop their client authentication solutions (Kitsing, 2011). Biometric identification is the identification verification through biological characteristics analysis. It is the key process by which people authenticate each other. You execute biometric identification when you identify a friend with her voice or ears. Computers will execute with greater efficiency the same procedure and biometric authentication is gaining currency as a way for individuals to become authenticated to computer systems. In this article, we use the term biometry to refer to authentication between humans and orders. Practicable biometrics are not available on a human-to-human identification basis for computer applications. The three biometrics favouring e-passport implementations include, for example, common computer-oriented biometrics such as fingerprints, facial acknowledgements and iris. Face recognition requires photographic vision imagery; it is effectively the automatic analogue to the usual facial recognition process. Fingerprint identification is also quite loosely equivalent to the fingerprint match used in forensic cases, and to an automatic procedure (but often based on a different class of fingerprint features). Optical or silicone sensor types may be taken by fingerprint scanners. The identification of the iris also means pictures. The iris is the light ring part of the pupil's retina. For example, someone with "blue eyes" has blue irises. Iris scanning takes place in biometric systems through non-invasive camera scanning. Often, a sensor is called the unit that collects user data in a biometric system. The biometric authentication method in most applications is approximately equivalent. An authenticated consumer enters the sensor with an original biometric image of high-quality. In a data structure known as a prototype, the machine stores the data collected during registration. For later user authentication the blueprint acts as the guideline. This may consist of an actual biometric image, such as a fingerprint image, or of information obtained from it, such as the relative positions of special items in the fingerprint. The customer shows again the biometric on a sensor to demonstrate his identity during an authentication session. In a general procedure called a match, the verifying agent matches the biometric data recently provided with the information found in the prototype for the customer. The prototype and authentication picture can only fit successfully if they have a fixed and frequently complex and supplier-specific metric to make them equally identical. The Estonian Prime Minister said digital signatures save time and time by digitally signing the first intergovernmental agreement in 2013, along with the Finnish Prime Minister. In addition to Estonian residents, Estonia now offers its electronic identification to encouraged new companies in the country (Kitsing, 2011). However, authenticating electronic identity cards to internet providers did not disappear, except in all countries where the system was introduced – people did not buy card readers. In Spain, for example, 27% of people had a dine-card, but only 2% had a card reader and fewer than 5% had used it for online services in 2010 to authenticate. The lack of mature digital identities, according to the OECD, slows the worldwide growth of the internet economy. However, each nation seems to be local about the factors determining the progress or failure of new citizens' identification technologies. The success and lack of interest in technology in one country can not be explained by technological factors (Lyon, 2009). The fear of losing privacy and freedom is a common cause for the resistance to electronic state identification. Two accounts give rise to those fears: Firstly, it is seen that the storage of one consolidated database of citizens' data is dangerous because it would draw attackers or the government might exploit it. Secondly, the issuer of the Identification may follow up online and physical movements of people through the uses of the electronic identity. Two state issues with the e-ID provided by the Electronic Frontier Foundation (Rissanen, 2010): If the national identification card is compulsory, it can be used to discriminate against individuals, and if the code includes biometric information, the protection presumption is wrong, because biometric information cannot be reissued when it is impaired. For cultural and historical reasons, attitudes to such questions differ across countries; some countries put their governments more confident than others, and some prefer private services to governmental ones. Much of the countries that we assessed are called democracies, and only China, Russia and Saudi Arabia are considered as hybrid states, and Turkey (Mutlugün and Adalier, 2009). From the world viewpoint, some of the worries are clear: identification cards have, for example, been used to recognize genocide victims in Rwanda, where the cards provide details about the tribe. Often known for monitoring the citizens' online movements, Totalitarian regimes are helping people to create those restrictions through their availability of powerful electronic identification. In the United Kingdom and the United States, the aforementioned claims have led to the cessation of electronic identification government programmes. The countries choose service- or trade-specific authentication schemes instead. Such political resistance is likely to prevent global or regional norms like Europe from being adopted.

# Conclusion

The aim of this research project was to explore the privacy and security risks that come with using eID cards to authenticate actions on the internet through the eyes of the end users i.e., the public. To this extent, a dataset made from a famous survey conducted in the US on internet privacy concerns was used. This dataset provided a deep insight into the issues the public faces with privacy and security regarding their data on the internet. The exploration was not the only aim but merely an objective of this research to achieve the aim of identifying the most concerning risk factors according to the public that uses the eID service for online authentication. The objectives completed to achieve this aim were to consider a survey that had at least 10 questions that would be easy for the public to answer thereby providing the research with large amounts of significant data. The second objective was to hold conversations with people based on their experiences using the eID services and the internet in general. These conversations will then be the source of at least hypotheses that would be used to analyse the data statistically. The final objective was to visualize the trend of the dataset from the survey to observe the tendencies of people i.e., whether they proceed towards finding their own solution to tackling this issue or not. From this, a cumulative list of at least 3 privacy and security related risk factors was garnered.

# Appendix

**import** numpy **as** np

**import** pandas **as** pd

**import** seaborn **as** sns

**import** matplotlib.pyplot **as** plt

**import** os

**for** dirname, \_, filenames **in** os**.**walk('./'):

**for** filename **in** filenames:

print(os**.**path**.**join(dirname, filename))

./AnonymityPoll.csv

./Internet Privacy Survey Analysis.ipynb

./.ipynb\_checkpoints\Internet Privacy Survey Analysis-checkpoint.ipynb

In [2]:

data **=** pd**.**read\_csv('AnonymityPoll.csv')

In [3]:

data**.**head()

Out[3]:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Internet.Use | Smartphone | Sex | Age | State | Region | Conservativeness | Info.On.Internet | Worry.About.Info | Privacy.Importance | Anonymity.Possible | Tried.Masking.Identity | Privacy.Laws.Effective |
| 0 | 1.0 | 0.0 | Male | 62.0 | Massachusetts | Northeast | 4.0 | 0.0 | 1.0 | 100.000000 | 0.0 | 0.0 | 0.0 |
| 1 | 1.0 | 0.0 | Male | 45.0 | South Carolina | South | 1.0 | 1.0 | 0.0 | 0.000000 | 1.0 | 0.0 | 1.0 |
| 2 | 0.0 | 1.0 | Female | 70.0 | New Jersey | Northeast | 4.0 | 0.0 | 0.0 | NaN | 0.0 | 0.0 | NaN |
| 3 | 1.0 | 0.0 | Male | 70.0 | Georgia | South | 4.0 | 3.0 | 1.0 | 88.888889 | 1.0 | 0.0 | 0.0 |
| 4 | 0.0 | NaN | Female | 80.0 | Georgia | South | 4.0 | NaN | NaN | NaN | NaN | NaN | NaN |

In [4]:

data**.**info()

<class 'pandas.core.frame.DataFrame'>

RangeIndex: 1002 entries, 0 to 1001

Data columns (total 13 columns):

# Column Non-Null Count Dtype

--- ------ -------------- -----

0 Internet.Use 1001 non-null float64

1 Smartphone 959 non-null float64

2 Sex 1002 non-null object

3 Age 975 non-null float64

4 State 1002 non-null object

5 Region 1002 non-null object

6 Conservativeness 940 non-null float64

7 Info.On.Internet 792 non-null float64

8 Worry.About.Info 790 non-null float64

9 Privacy.Importance 787 non-null float64

10 Anonymity.Possible 753 non-null float64

11 Tried.Masking.Identity 784 non-null float64

12 Privacy.Laws.Effective 894 non-null float64

dtypes: float64(10), object(3)

memory usage: 101.9+ KB

Survey Count: 1002

In [5]:

data**.**Smartphone**.**value\_counts()

Out[5]:

1.0 487

0.0 472

Name: Smartphone, dtype: int64

In [6]:

data**.**Smartphone**.**isnull()**.**value\_counts()

Out[6]:

False 959

True 43

Name: Smartphone, dtype: int64

People that use Smartphone: 487

People that don't use a Smartphone: 472

People that did not respond: 43

In [7]:

pd**.**crosstab(data**.**Sex, columns **=** data**.**Region)

Out[7]:

| **Region** | **Midwest** | **Northeast** | **South** | **West** |
| --- | --- | --- | --- | --- |
| **Sex** |  |  |  |  |
| **Female** | 123 | 90 | 176 | 116 |
| **Male** | 116 | 76 | 183 | 122 |

In [8]:

pd**.**crosstab(data**.**State, columns **=** data**.**Region)

Out[8]:

| **Region** | **Midwest** | **Northeast** | **South** | **West** |
| --- | --- | --- | --- | --- |
| **State** |  |  |  |  |
| **Alabama** | 0 | 0 | 11 | 0 |
| **Arizona** | 0 | 0 | 0 | 24 |
| **Arkansas** | 0 | 0 | 10 | 0 |
| **California** | 0 | 0 | 0 | 103 |
| **Colorado** | 0 | 0 | 0 | 19 |
| **Connecticut** | 0 | 8 | 0 | 0 |
| **Delaware** | 0 | 0 | 6 | 0 |
| **District of Columbia** | 0 | 0 | 2 | 0 |
| **Florida** | 0 | 0 | 42 | 0 |
| **Georgia** | 0 | 0 | 34 | 0 |
| **Idaho** | 0 | 0 | 0 | 8 |
| **Illinois** | 32 | 0 | 0 | 0 |
| **Indiana** | 27 | 0 | 0 | 0 |
| **Iowa** | 14 | 0 | 0 | 0 |
| **Kansas** | 14 | 0 | 0 | 0 |
| **Kentucky** | 0 | 0 | 25 | 0 |
| **Louisiana** | 0 | 0 | 17 | 0 |
| **Maine** | 0 | 4 | 0 | 0 |
| **Maryland** | 0 | 0 | 18 | 0 |
| **Massachusetts** | 0 | 19 | 0 | 0 |
| **Michigan** | 31 | 0 | 0 | 0 |
| **Minnesota** | 15 | 0 | 0 | 0 |
| **Mississippi** | 0 | 0 | 11 | 0 |
| **Missouri** | 26 | 0 | 0 | 0 |
| **Montana** | 0 | 0 | 0 | 5 |
| **Nebraska** | 11 | 0 | 0 | 0 |
| **Nevada** | 0 | 0 | 0 | 8 |
| **New Hampshire** | 0 | 7 | 0 | 0 |
| **New Jersey** | 0 | 16 | 0 | 0 |
| **New Mexico** | 0 | 0 | 0 | 5 |
| **New York** | 0 | 60 | 0 | 0 |
| **North Carolina** | 0 | 0 | 32 | 0 |
| **North Dakota** | 5 | 0 | 0 | 0 |
| **Ohio** | 38 | 0 | 0 | 0 |
| **Oklahoma** | 0 | 0 | 14 | 0 |
| **Oregon** | 0 | 0 | 0 | 20 |
| **Pennsylvania** | 0 | 45 | 0 | 0 |
| **Rhode Island** | 0 | 4 | 0 | 0 |
| **South Carolina** | 0 | 0 | 12 | 0 |
| **South Dakota** | 3 | 0 | 0 | 0 |
| **Tennessee** | 0 | 0 | 17 | 0 |
| **Texas** | 0 | 0 | 72 | 0 |
| **Utah** | 0 | 0 | 0 | 11 |
| **Vermont** | 0 | 3 | 0 | 0 |
| **Virginia** | 0 | 0 | 31 | 0 |
| **Washington** | 0 | 0 | 0 | 28 |
| **West Virginia** | 0 | 0 | 5 | 0 |
| **Wisconsin** | 23 | 0 | 0 | 0 |
| **Wyoming** | 0 | 0 | 0 | 7 |

US States in the Midwest Census Region: Kansas, Ohio, Missouri

US State in the South Census Region with the Largest Number of Interviewees: Texas

In [9]:

pd**.**crosstab(data['Internet.Use'], columns **=** data**.**Smartphone)

Out[9]:

| **Smartphone** | **0.0** | **1.0** |
| --- | --- | --- |
| **Internet.Use** |  |  |
| **0.0** | 186 | 17 |
| **1.0** | 285 | 470 |

People that haven't used the Internet and a Smartphone: 186

People that have used the Internet and a Smartphone: 470

People that have used the Internet but not a Smartphone: 285

People that haven't used the Internet but used a Smartphone: 17

In [10]:

data**.**isnull()**.**sum()

Out[10]:

Internet.Use 1

Smartphone 43

Sex 0

Age 27

State 0

Region 0

Conservativeness 62

Info.On.Internet 210

Worry.About.Info 212

Privacy.Importance 215

Anonymity.Possible 249

Tried.Masking.Identity 218

Privacy.Laws.Effective 108

dtype: int64

People that did not respond on their Internet Usage: 1

People that did not respond on the Availability of a Smartphone: 43

In [11]:

limited **=** data[(data['Internet.Use'] **==** 1) **|** data**.**Smartphone **==** 1]

In [12]:

limited**.**head()

Out[12]:

|  | **Internet.Use** | **Smartphone** | **Sex** | **Age** | **State** | **Region** | **Conservativeness** | **Info.On.Internet** | **Worry.About.Info** | **Privacy.Importance** | **Anonymity.Possible** | **Tried.Masking.Identity** | **Privacy.Laws.Effective** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0** | 1.0 | 0.0 | Male | 62.0 | Massachusetts | Northeast | 4.0 | 0.0 | 1.0 | 100.000000 | 0.0 | 0.0 | 0.0 |
| **1** | 1.0 | 0.0 | Male | 45.0 | South Carolina | South | 1.0 | 1.0 | 0.0 | 0.000000 | 1.0 | 0.0 | 1.0 |
| **2** | 0.0 | 1.0 | Female | 70.0 | New Jersey | Northeast | 4.0 | 0.0 | 0.0 | NaN | 0.0 | 0.0 | NaN |
| **3** | 1.0 | 0.0 | Male | 70.0 | Georgia | South | 4.0 | 3.0 | 1.0 | 88.888889 | 1.0 | 0.0 | 0.0 |
| **5** | 1.0 | 1.0 | Male | 49.0 | Tennessee | South | 4.0 | 6.0 | 0.0 | 88.888889 | 1.0 | 1.0 | 0.0 |

In [13]:

limited**.**info()

<class 'pandas.core.frame.DataFrame'>

Int64Index: 792 entries, 0 to 1001

Data columns (total 13 columns):

# Column Non-Null Count Dtype

--- ------ -------------- -----

0 Internet.Use 792 non-null float64

1 Smartphone 772 non-null float64

2 Sex 792 non-null object

3 Age 770 non-null float64

4 State 792 non-null object

5 Region 792 non-null object

6 Conservativeness 747 non-null float64

7 Info.On.Internet 792 non-null float64

8 Worry.About.Info 790 non-null float64

9 Privacy.Importance 787 non-null float64

10 Anonymity.Possible 753 non-null float64

11 Tried.Masking.Identity 784 non-null float64

12 Privacy.Laws.Effective 727 non-null float64

dtypes: float64(10), object(3)

memory usage: 86.6+ KB

In [14]:

limited**.**isnull()**.**sum()

Out[14]:

Internet.Use 0

Smartphone 20

Sex 0

Age 22

State 0

Region 0

Conservativeness 45

Info.On.Internet 0

Worry.About.Info 2

Privacy.Importance 5

Anonymity.Possible 39

Tried.Masking.Identity 8

Privacy.Laws.Effective 65

dtype: int64

People in the New Data Frame: 792

Features with Missing Values in the Data Frame:

Smartphone, Age, Conservativeness, Worry.About.Info, Privacy.Importance, Anonymity.Possible, Tried.Masking.Identity, Privacy.Laws.Effective

In [15]:

data['Info.On.Internet']**.**mean()

Out[15]:

3.7954545454545454

Info.On.Internet Average: 3.795

In [16]:

data['Info.On.Internet']**.**value\_counts()

Out[16]:

0.0 105

4.0 104

3.0 101

2.0 95

5.0 94

1.0 84

6.0 67

7.0 63

8.0 40

9.0 18

10.0 13

11.0 8

Name: Info.On.Internet, dtype: int64

Frequency of 'Zero' in Info.On.Internet: 105

Frequency of Max Value in Info.On.Internet: 8

Percentage of People Concerned about their Information on the Internet: 0.4886

In [17]:

data['Worry.About.Info']**.**value\_counts()

Out[17]:

0.0 404

1.0 386

Name: Worry.About.Info, dtype: int64

In [18]:

(data['Worry.About.Info']**.**value\_counts()[1])**/**data['Worry.About.Info']**.**count()

Out[18]:

0.48860759493670886

In [19]:

(data['Anonymity.Possible']**.**value\_counts()[1])**/**data['Anonymity.Possible']**.**count()

Out[19]:

0.3691899070385126

People that think it is Possible to be Anonymous on the Internet: 0.3692

In [20]:

(data['Tried.Masking.Identity']**.**value\_counts()[1])**/**data['Tried.Masking.Identity']**.**count()

Out[20]:

0.16326530612244897

Percentage of People that have Tried Identity Masking: 0.1632653

In [21]:

(limited['Privacy.Laws.Effective']**.**value\_counts()[1])**/**limited['Privacy.Laws.Effective']**.**count()

Out[21]:

0.2558459422283356

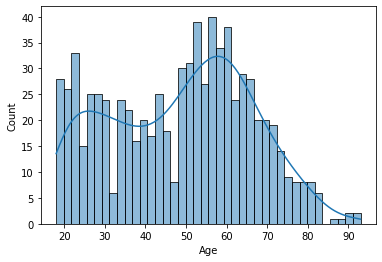
Percentage of People that find US Internet Privacy Laws Effective: 0.2558

In [22]:

age **=** limited**.**Age[**~**limited**.**Age**.**isnull()]

sns**.**histplot(age, kde **=** **True**, bins **=** 40)

plt**.**show()



Often, we are interested in whether certain characteristics of interviewees (e.g. their age or political opinions) affect their opinions on the topic of the poll (in this case, opinions on privacy). In this section, we will investigate the relationship between the characteristics Age and Smartphone and outcome variables Info.On.Internet and Tried.Masking.Identity, again using the limited data frame we built in an earlier section of this problem.

Best Presented Age Group in the Population: 60

In [23]:

limited[limited**.**Smartphone **==** 0]['Info.On.Internet']**.**describe()

Out[23]:

count 285.000000

mean 2.922807

std 2.449707

min 0.000000

25% 1.000000

50% 3.000000

75% 5.000000

max 11.000000

Name: Info.On.Internet, dtype: float64

In [24]:

maskers **=** limited[ (limited**.**Smartphone **==** 1) **&** (limited['Tried.Masking.Identity'] **==** 1)]**.**shape[0]

non\_maskers **=** len(limited[ (limited**.**Smartphone **==** 1) **&** (limited['Tried.Masking.Identity'] **==** 0)] )

print(maskers **/** (maskers **+** non\_maskers))

0.19254658385093168

In [25]:

xx **=** limited[ (limited**.**Smartphone **==** 0) **&** (limited['Tried.Masking.Identity'] **==** 1) ]**.**shape[0]

yy **=** limited[ (limited**.**Smartphone **==** 0) **&** (limited['Tried.Masking.Identity'] **==** 0)]**.**shape[0]

In [26]:

print("Percentage of People that Mask their Identity while Browsing the Internet: ", xx **/** (xx **+** yy))

Percentage of People that Mask their Identity while Browsing the Internet: 0.11743772241992882

# References

1. BELAPURKAR, A., CHAKRABARTI, A., PONNAPALLI, H., VARADARAJAN, N., PADMANABHUNI, S. & SUNDARRAJAN, S. 2009. Distributed systems security: issues, processes and solutions, John Wiley & Sons.
2. BENNETT, C. J. & LYON, D. 2008. Playing the identity card: Surveillance, security and identification in global perspective, Routledge.
3. BEYNON-DAVIES, P. 2006. Personal identity management in the information polity: the case of the UK national identity card. Information polity, 11, 3-19.
4. BRANDS, S. 2000. Rethinking public key infrastructures and digital certificates: building in privacy, MIT Press.
5. CLEMENT, A., BOA, K., DAVIES, S. & HOSEIN, G. 2008. Towards a National ID Card for Canada? External drivers and internal complexities. Routledge.
6. DZIKRULLAH, F. & RINJANI, M. A. 2017. A framework design to develop an integrated data system for smart e-government based on big data technology. Bulletin of Social Informatics Theory and Application, 1, 41-51.
7. FUMY, W. & PAESCHKE, M. 2010. Handbook of EID Security: Concepts, Practical Experiences, Technologies, John Wiley & Sons.
8. GARFINKEL, S. & ROSENBERG, B. 2006. RFID: Applications, security, and privacy, Pearson Education India.
9. GIESSMANN, E.-G. Transparency and Security for Client-Side Encrypting Cloud Storage Applications.
10. HE, S. & PAAR, I. C. SIM card security. Seminar Work, Ruhr-University of Bochum, 2007.
11. JAIN, A. K. & KUMAR, A. 2010. Biometrics of next-generation: An overview. Second generation biometrics, 12, 2-3.
12. KITSING, M. Online participation in Estonia: active voting, low engagement. Proceedings of the 5th international conference on theory and practice of electronic governance, 2011. 20-26.
13. KLUGLER, D. 2005. Advance security mechanisms for machine-readable travel documents, Technical reports. Federal Office for Information Security (BSI), Germany, 41-46.
14. LAURINAITIS, M. & ŠTITILIS, D. 2008. Alternative payment systems: Lithuanian outlook. Intelektinė ekonomika, 43-51.
15. LYON, D. 2009. Identifying Citizens: ID cards as surveillance, Polity.
16. MARKANTONAKIS, K., TUNSTALL, M., HANCKE, G., ASKOXYLAKIS, I. & MAYES, K. 2009. Attacking smart card systems: Theory and practice. information security technical report, 14, 46-56.
17. METTLER, T. & GUENDUEZ, A. A. 2019. From SuisseID to SwissID: Overcoming the key challenges in Switzerland’s e-credential market.
18. MUTLUGÜN, M. & ADALIER, O. Turkish national electronic identity card. Proceedings of the 2nd international conference on Security of information and networks, 2009. 14-18.
19. NYMAN, T., EKBERG, J.-E. & ASOKAN, N. Citizen electronic identities using TPM 2.0. Proceedings of the 4th International Workshop on Trustworthy Embedded Devices, 2014. 37-48.
20. OGASAWARA, M., LYON, D. & SNIDER, L. 2008. ID troubles: The national identification systems in Japan and the (mis) construction of the subject.
21. OH, Y., OBI, T., LEE, J. S., SUZUKI, H. & OHYAMA, N. Empirical analysis of Internet identity misuse: a case study of South Korean real-name system. Proceedings of the 6th ACM workshop on Digital identity management, 2010. 27-34.
22. PAUL, C. L., MORSE, E., ZHANG, A., CHOONG, Y.-Y. & THEOFANOS, M. A field study of user behaviour and perceptions in smartcard authentication. IFIP Conference on Human-Computer Interaction, 2011. Springer, 1-17.
23. PETKOVIC, M. & JONKER, W. 2007. Security, privacy, and trust in modern data management, Springer.
24. RISSANEN, T. 2010. Electronic identity in Finland: ID cards vs. bank IDs. Identity in the Information Society, 3, 175-194.
25. SANTOS, R., CORREIA, M. E. & ANTUNES, L. Securing a health information system with a government-issued digital identification card. 2008 42nd Annual IEEE International Carnahan Conference on Security Technology, 2008. IEEE, 135-141.
26. SANTOS, R. F. S. 2011. Securing a health information system with a government-issued digital identification card.
27. SCHERZER, H. 2002. Application interface for smart cards used as secure signature creation devices, version 0.6, CEN/ISSS, WS E-Sign, Draft CWA. Group K, January.
28. SCHNEIER, B. 2005. Two-factor authentication: too little, too late. Communications of the ACM, 48, 136.
29. SCHRYEN, G. & RICH, E. 2009. Security in large-scale internet elections: a retrospective analysis of elections in Estonia, the Netherlands, and Switzerland. IEEE Transactions on Information Forensics and Security, 4, 729-744.
30. SHER, M. & MAGEDANZ, T. Secure access to IP multimedia services using generic bootstrapping architecture (GBA) for 3G & beyond mobile networks. Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks, 2006. 17-24.
31. SHUKRI, M. & HAFIZ, M. 2015. The privacy and security of an identification card: Malaysian perspective. University Malaysia Sarawak, Tech. Rep, 65855.
32. SUORANTA, S., HAATAJA, L. & AURA, T. Electronic Citizen Identities and Strong Authentication. Nordic Conference on Secure IT Systems, 2015. Springer, 213-230.
33. TAMRAKAR, S., EKBERG, J.-E. & LAITINEN, P. On rehoming the electronic id to TEEs. 2015 IEEE Trustcom/BigDataSE/ISPA, 2015. IEEE, 49-56.
34. TU, Y.-C. & THOMBORSON, C. Preliminary security specification for New Zealand's igovt system. Proceedings of the Seventh Australasian Conference on Information Security-Volume 98, 2009. 79-88.
35. Blue, J., Furey, E. and Condell, J., 2017, June. A novel approach for secure identity authentication in legacy database systems. In 2017 28th Irish Signals and Systems Conference (ISSC) (pp. 1-6). IEEE.
36. Chatfield, S.L., 2020. Recommendations for secondary analysis of qualitative data. The Qualitative Report, 25(3), pp.833-842.
37. Hamidi, H., 2019. An approach to developing smart health using the Internet of Things and authentication based on biometric technology. Future generation computer systems, 91, pp.434-449.
38. Juan, M.D., Andrés, R.P., Rafael, P.M., Gustavo, R.E. and Manuel, P.C., 2018. A model for national electronic identity document and authentication mechanism based on blockchain. Int. J. Model. Optim, 8(3), pp.160-165.
39. Kumar, R., 2018. Research methodology: A step-by-step guide for beginners. Sage.
40. Liu, J., Lyu, Q., Wang, Q. and Yu, X., 2017. A digital memories-based user authentication scheme with privacy preservation. PloS one, 12(11), p.e0186925.
41. Morgan, D. and Parsovs, A., 2017, November. Using the Estonian Electronic Identity Card for Authentication to a Machine. In Nordic Conference on Secure IT Systems (pp. 175-191). Springer, Cham.
42. Mumtaz, M., Akram, J. and Ping, L., 2019, August. An RSA based authentication system for smart IoT environment. In 2019 IEEE 21st International Conference on High-Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 758-765). IEEE.
43. Park, N. and Lee, D., 2018. Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. Personal and Ubiquitous Computing, 22(1), pp.3-10.
44. Rivera, R., Robledo, J.G., Larios, V.M. and Avalos, J.M., 2017, September. What a digital identity on the blockchain can contribute in a smart city environment. In 2017 International smart cities conference (ISC2) (pp. 1-4). IEEE.
45. Sherif, V., 2018, March. Evaluating preexisting qualitative research data for secondary analysis. In Forum Qualitative Sozialforschung/Forum: Qualitative social research (Vol. 19, No. 2).
46. Zimmermann, V. and Gerber, N., 2017, July. “If It Wasn’t Secure, They Would Not Use It in the Movies”–Security Perceptions and User Acceptance of Authentication Technologies. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 265-283). Springer, Cham.