Journal of Innovations in Computer Science and Engineering
Shahid Beheshti Unversity

May 2023, Volume 1, Issue 1

Exploring Identity Theft: Motives, Techniques, and Consequents on Different Age Groups

Fatemeh Hora Haghighatkhah [a] Code Orcid: 0009-0003-5654-0583,
Maedeh Mosharraf[b]✉ Code Orcid: 0000-0001-9858-2907
[a] Computer Engineering student, Shahid Beheshti University, Tehran, Iran, fa.haghighatkhah@Mail.sbu.ac.ir
[b] Faculty of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran m_mosharraf@sbu.ac.ir

ABSTRACT

While the growth of technology has greatly benefited humanity, it also brings along several drawbacks that can undermine these benefits. Despite its ability to detect attacks and deter various forms of theft, technology is often regarded as a tool for creating new theft techniques. Conducting a systematic review, this article discusses the current state of the art in terms of identity theft motivations, the techniques employed, and the potential harm inflicted upon victims. The paper findings reveal that the reasons behind such incidents can be categorized into seven main categories: financial, commercial, health and medical, educational, citizenship, Internet of Things (IoT), and informational. Fraudsters employ various methods to steal identity information, which can be categorized as social engineering, vulnerabilities, malware, eavesdropping, and information gathering. However, it is important to note that not all identity theft reasons are a concern for people of all ages. This article addresses the examination of potential threats within different age groups. Tragically, victims of identity theft often endure significant financial, legal, social, and health harm as a result of these malicious activities. One of the primary strategies to combat this crime involves investigating the causes, methods, and age distribution of the potential victim population.

KEYWORDS

Identity theft, financial fraud, social engineering attacks, information fraud, citizenship fraud, age, identity fraud

1. INTRODUCTION

Technology development is akin to a double-edged sword. On one hand, it offers individuals numerous advantages and means to prevent fraud. On the other hand, it has also presented thieves with new opportunities to perpetrate fraud. Identity theft, a crime that has surged in tandem with the widespread use of computers in the past two decades, is carried out by individuals for various reasons across different categories. The number of thefts and frauds is depicted in Figure 1, which unfortunately shows a steep rise in 2021 [1], despite the development of numerous technological ways to stop these thefts as well as robust social and cultural awareness.

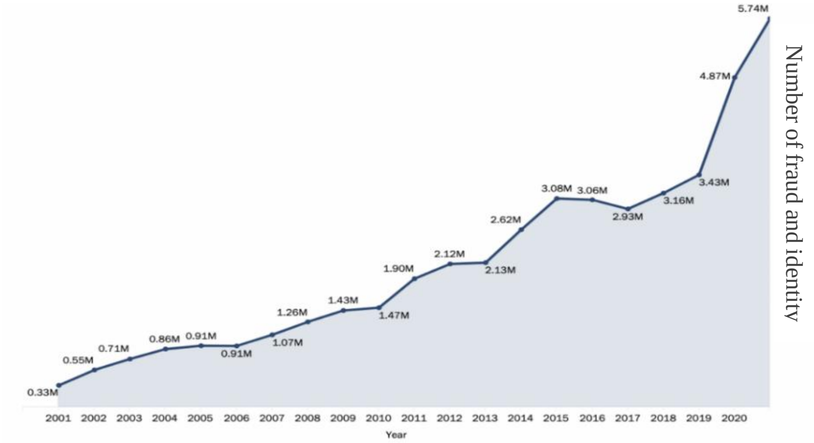

Figure 1. Number of frauds and identity theft reported by year [1]

Reviewing the history of identity theft detection/prevention reveals a significant amount of technical development in this area. Despite the existence of different methods for theft prevention or detection, reviewing the thefts and their objectives can help categorize the reasons for the thefts and their effects. This categorization serves as a warning for officials and industries. It is evident that in order to prevent information theft, it is essential to identify the various techniques employed. One technological

Submit Date: 2023-03-13
Revise Date: 2023-07-16
Accept Date: 2023-07-16
✉ Corresponding author

issue that perplexes engineers is the use of countermeasures to prevent penetration and to discover and close intrusion channels. However, understanding the causes of these crimes and the types of damage involved requires an understanding of the psychological, physical, financial, cultural, and societal harms that such thefts can cause. Therefore, studying identity theft is crucial for several compelling reasons:

- Prevention: Understanding the methods and techniques employed by identity thieves enables individuals, businesses, and organizations to implement effective preventive measures. This knowledge facilitates the development of robust security systems and practices, minimizing the risk of identity theft.
- Public Awareness: Raising awareness about identity theft helps individuals recognize the signs and symptoms of potential attacks. This awareness empowers individuals to be more cautious and vigilant in protecting their personal information, both online and offline [2].
- Legal and Policy Frameworks: Research on identity theft contributes to the development of legal and policy frameworks that address this growing issue. By studying patterns and trends in identity theft, lawmakers and policymakers can enact legislation and regulations that provide stronger protection for individuals and prescribe appropriate penalties for offenders.
- Support for Victims: Understanding the impact of identity theft on victims is crucial for providing them with the necessary support and assistance. Research helps identify the emotional, financial, and legal challenges faced by victims, leading to the development of tailored support services, counseling, and resources [3].
- Cybersecurity Advancements: As identity theft techniques evolve, continuous research is necessary to stay ahead of emerging threats. By studying the latest trends and advancements in identity theft, researchers and technology experts can develop innovative solutions, such as advanced encryption methods, authentication protocols, and cybersecurity tools, to combat these evolving risks [4-5].
- To identify future research directions: Identity theft is a complex problem, and further research is needed to gain a deeper understanding. A literature review of identity fraud can help identify future research directions [6], guiding future efforts to better comprehend and combat identity theft.

Despite the extensive research conducted on identity theft, there remains a significant gap in understanding the comprehensive range of factors associated with its causes, methods, and the specific implications for different age groups. This article aims to explore the causes and methods of theft and their impact on victims. To achieve this, it provides an overview of (1) the reasons for identity information theft, (2) the methods used for theft, (3) the harms and consequences of such theft, and (4) the age of the victims. The exploration is based on an analysis of numerous publications, reports, and upstream documents. Furthermore, the identity theft methods have been categorized and explained in detail based on their effectiveness in this study. All the achievements of this article have been presented in a tree diagram in Figure 2.

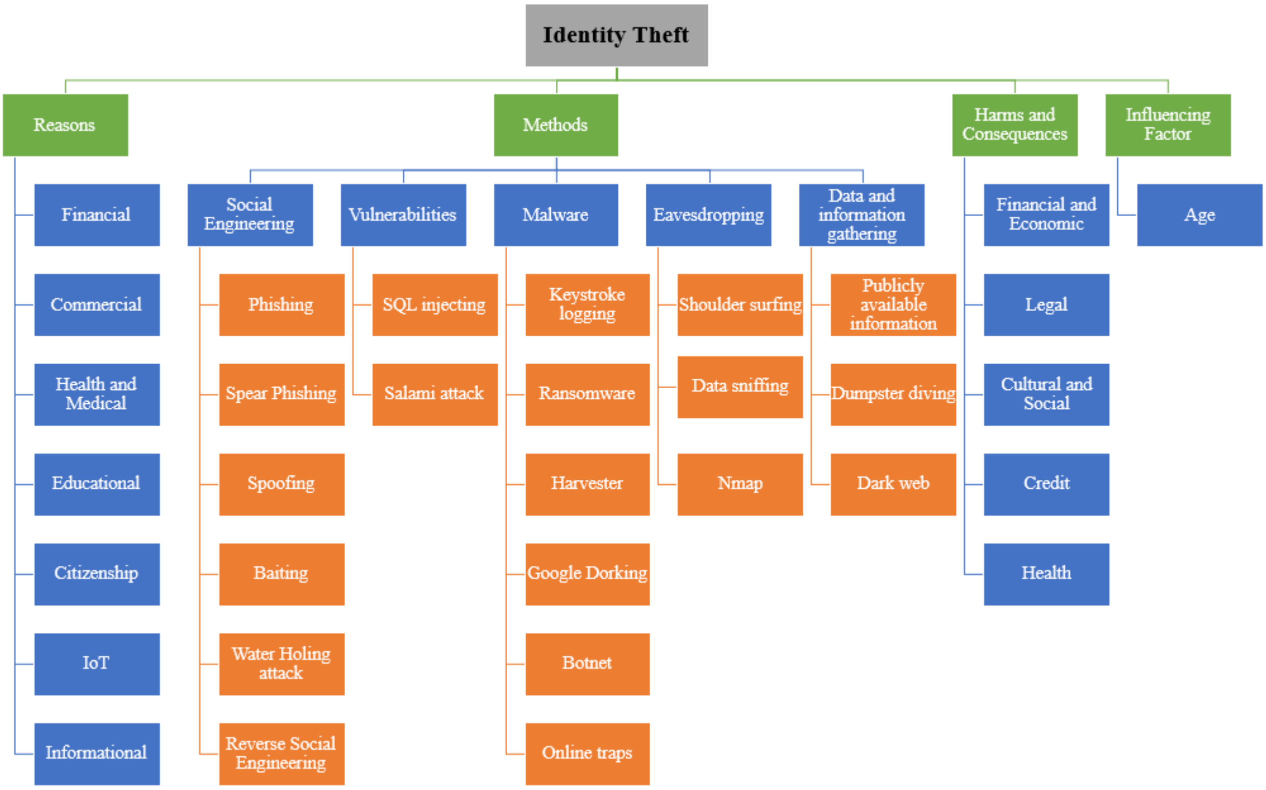

Figure 2. The abstract diagram of this article findings

2. RESEARCH METHODOLOGY

To conduct a systematic review, the Google Scholar database was utilized. This choice was made due to the comprehensiveness of Google Scholar and its indexing of a wide range of articles. Additionally, it provides information on the publication year and publisher of the articles. In this study, English articles published from 2010 onwards were examined as an inclusion criterion, with a specific emphasis on reputable publications. Moreover, the selection of websites was considered for the research purposes. Figure 3 represent the review process and the number of retrieved articles in each step.

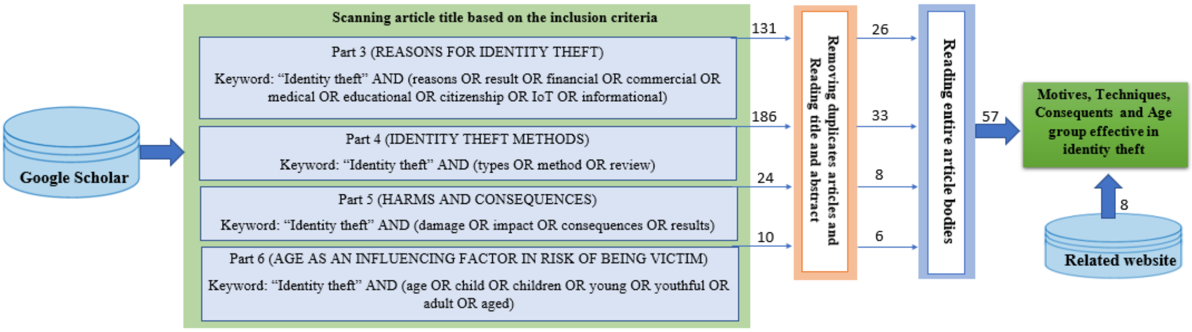
Google Scholar
Scanning article title based on the inclusion criteria
Part 3 (REASONS FOR IDENTITY THEFT)
Keyword: "Identity theft" AND (reasons OR result OR financial OR commercial OR medical OR educational OR citizenship OR IoT OR informational)
Part 4 (IDENTITY THEFT METHODS)
Keyword: "Identity theft" AND (types OR method OR review)
Part 5 (HARMS AND CONSEQUENCES)
Keyword: "Identity theft" AND (damage OR impact OR consequences OR results)
Part 6 (AGE AS AN INFLUENCING FACTOR IN RISK OF BEING VICTIM)
Keyword: "Identity theft" AND (age OR child OR children OR young OR youthful OR adult OR aged)
131
186
24
10
Removing duplicates articles and Reading title and abstract
26
33
8
6
Reading entire article bodies
57
Motives, Techniques, Consequents and Age group effective in identity theft
8
Related website

Figure 3. The systematic review process and the number of reviewed articles

The process of review involved identifying relevant articles pertaining to the discussed topics, including the reasons for identity theft, types of identity theft, damages caused by identity theft, and the influence of victims' age on identity theft. Specific keywords were utilized in addition to other inclusion criteria to retrieve suitable articles. The search focused on the presence of these keywords in articles title or keywords. Articles meeting the inclusion criteria were considered as potential candidates for further examination. Duplicate entries were then removed, resulting in a refined list of candidate papers. These remaining articles were thoroughly reviewed to extract pertinent information and address the research questions.

3. REASONS FOR IDENTITY THEFT

Researchers define identity theft as a precursor to identity fraud [2]. Each year, victims are forced to pay billions of dollars to mitigate the consequences of impersonation fraud. Thus, it can be inferred that individuals encounter significant financial devastation when their identities are stolen [7]. Not all thieves share the same goals. In many cases, identity theft is driven by a financial motive, often involving making money or seeking revenge. Sometimes, the intention behind such acts is to maintain secrecy. However, these underlying motives may not be apparent at first glance.

Many researchers have focused their attention on the financial, commercial, and medical sectors [7: 9]; However, it is important to note that identity thieves sometimes target information for academic exploitation [10] or the abuse of other civil rights, such as the right to vote [4]. With the increasing significance of protecting data obtained from Internet of Things (IoT) technology, a distinct category of reasons emerges, particularly in light of the expanding use of identity information across various industries [5] , [11-12]. Nevertheless, thefts outside these categories also occur due to the valuable nature of data, which can be sold [13-14]. As a result, the reasons and extent of identity theft can be categorized into seven main groups, each with its own commonalities.**Financial**

This category of theft encompasses the misuse of individuals' identity information for various fraudulent purposes, including acquiring goods, services, credit, renting properties or vehicles, obtaining loans, opening accounts, or unlawfully accessing the victim's bank account, often with the intention of financial exploitation [15]. The perpetrator utilizes the victim's personal details to establish new credit accounts and engage in illicit financial activities, such as presenting counterfeit checks or engaging in fraud. Additionally, they may gain unauthorized access to an individual's existing bank accounts and deplete their funds or exploit their credit by obtaining loans or utilizing services. Regrettably, victims of identity theft often discover fraudulent activities conducted using their information after the fact [8-9].

3.2 Commercial

In addition to regular users, numerous government organizations and companies have interconnected business relationships. Consequently, ensuring the security of both individuals' and companies' information becomes a significant challenge for information technology [16]. Business models often encounter difficulties concerning the supply of raw materials, distribution, transportation, warehousing, and the production line due to unauthorized access to organizational information, which encompasses its strengths and weaknesses, decisions, tactics, and strategies. Within the context of companies' interactions with the government, the illicit exploitation of an individual's identity, particularly their social security number, to file fraudulent tax returns and obtain refunds is commonly referred to as tax identity theft [17].

In the customer layer, the threat of identity theft has clearly affected the behavior of online consumers, leading to increased cautious and distrustful [3], [18]. This lack of trust in cyberspace has resulted in substantial financial losses for certain vendors [7], [14]. Attackers gain unauthorized access to people's user accounts on online stores, making purchases on their behalf and changing their address to the thief's location, or they create new accounts with the stolen information on unauthorized online markets, effectively concealing their illicit transactions [7]. Another method employed by fraudsters is the establishment of unreliable online stores, where victims unknowingly provide all their information to the thieves, only to be left empty-handed with no goods or services received despite their payment. In such cases, both the victim's money and personal information are stolen simultaneously [19]. Moreover, infiltrating the user accounts of companies and organizations poses significant risks and carries far-reaching consequences.

3.3 Health and Medical

Medical identity theft can inflict significant harm upon its victims, as it frequently leads to the inclusion of false information in their medical records, resulting in years of medical and financial complications [14]. This form of theft occurs when a criminal submits fraudulent claims to the victim's health insurance or deliberately alters the patient's medical records as an act of revenge or for other motives. One potential consequence of medical fraud is the misleading of healthcare providers and doctors, thereby jeopardizing the patient's life. Moreover, the expenses associated with treatment, hospital services, and insurance benefits are exorbitant in most countries. In cases of such theft, the victim's information may be exploited to obtain treatment, prescription drugs, medical equipment, insurance discounts, or other advantages. These factors underscore the utmost importance of safeguarding the databases of hospitals, doctors' offices, and any other medical facility [9], [20].

3.4 Educational

Although it is expected that the academic world is immune to fraud, there have been numerous attempts to steal identity information in the education industry, and victimizing various stakeholders [21]. Identity theft at the student level involves the unauthorized use of personal information to attend virtual classes, access educational facilities on behalf of registered students, or even take exams for them. Another example of these malicious activities is the exploitation of teachers' or educational managers' identities to gain access to educational systems, tamper with logs, or perpetrate significant frauds. Furthermore, identity theft can be employed to acquire unauthorized access to other individuals' data and educational resources, thereby legitimizing one's own educational accomplishments. The costs associated with identity theft in this domain far exceed the damage inflicted upon education and culture, with potential financial and emotional repercussions [22].

Identity theft in scholarly publishing leads to the proliferation of invalid or junk science. However, examples of this crime in academic writing and publishing are also investigated in [10]. There are various illicit practices involved, such as utilizing unauthorized identity information of well-known individuals in journals or conferences to provide legitimacy, hacking publishers' websites to gain access to reviewers' information and manipulate the judgment and acceptance of articles, and stealing the editor-in-chief's credentials to facilitate the acceptance and publication of articles. Additionally, criminals attempt to manipulate the article acceptance process by falsely listing renowned individuals as the authors or referees of the article [23].

3.5 Citizenship

Citizenship is a relationship of allegiance and the right to protection between an individual and their state. Within the concept of citizenship, citizens are entitled to various rights, such as access to information, welfare, economic and medical facilities, freedom and security, free thinking and expression, education, and research. While the aforementioned categories may fall under this broad umbrella, this investigation specifically focuses on information theft for purposes unrelated to financial, commercial, educational, and medical rights. The theft of a citizen's identification can enable thieves to speak, post, or vote on their behalf, potentially leading to the spread of rumors and the initiation of social movements [4], [24].

3.6 IoT

The introduction of IoT and Internet of Everything (IoE) technology into people's lives and industries necessitates the safeguarding of collected information, as its importance cannot be overstated [25]. Consequently, various methods of theft and intrusion into IoT devices have emerged. Hackers can breach Wi-Fi networks, thereby gaining unauthorized access to any connected IoT device. They employ techniques like network injections, salami attacks, or distributed denial-of-service (DDoS) attacks. Such breaches not only compromise the privacy of IoT data but also grant control of these devices to unauthorized individuals. For instance, assuming control of a greenhouse and making erroneous temperature adjustments can have detrimental consequences for farmers. Additionally, applications associated with IoT devices often require login credentials, which can also be susceptible to theft. Consider a smartwatch that stores sensitive medical and insurance information [11-12]. Implementing secure devices and employing solutions such as an ID management system based on blockchain can mitigate these risks [5].

3.7 Informational

This category is broader in scope compared to other categories, sharing similarities with them. However, the stolen data or information is not necessarily intended for blackmailing the victim, nor is it solely focused on commercial or medical purposes. The value lies in the data itself. The context of this review pertains to websites and programs that collect and store user information, including social networks. Within this context, data is processed and analyzed, resulting in the acquisition of user information. A substantial amount of user data is stored on the internet, which can range from raw data to personal information, such as bank account information, online passwords, passport numbers, driver's license numbers, social security numbers, medical records, and online subscriptions [26]. Criminals can aggregate and analyze this information to gain unauthorized access to secure accounts or even threaten the victims. For instance, by obtaining comprehensive data and analyzing it, one might discover that combining a victim's username on a social network with their year of birth could serve as another user's password. There is even a simpler method- many users disregard safety precautions and employ the same information across multiple accounts to avoid forgetting them on different websites. If any of this information is stolen, all their accounts become vulnerable. Occasionally, thieves find great incentive in selling stolen or leaked data on the dark web or supplying it to companies [27].

4 IDENTITY THEFT METHODS

Identity information is often stolen by highly sophisticated and developed thieves who employ a variety of techniques. The methods and tools utilized in these thefts depend on various factors, including the motive behind the act. In some instances, individuals become victims of their own carelessness, inadvertently leading to the loss of their identity information. For instance, users may unknowingly expose their identity information to thieves by agreeing to a website's terms and conditions after using it for only a few minutes. The techniques employed for information theft can be broadly categorized into five groups, which include:

1) Social engineering: social engineering is “the art, or better yet, the science of skillfully maneuvering human beings to take action in some aspect of their life” [28]. In the context of security, it means the art of inducing people to perform actions or disclose confidential information. This is a trick to use the person himself to collect information that can lead to fraud. Obtaining login information allows access to a computer system or IoT devices. This attack on commercial activities leads to financial loss and damage to the reputation and loss of privacy of users [29]. All social engineering

techniques are based on specific characteristics of human decision-making. Social engineers exploit the weaknesses of human behavior for their own benefit. Psychological tricks are often used by social engineers to get the user to submit to things they would normally disagree with. By using these tricks, thieves take important information from users. Spamming and all types of phishing are the digital versions of social engineering [8], [30-31].

a. Phishing: Phishing is a social engineering approach that persuades the intended victim to divulge personal information [32]. The rationale behind this term is that the attacker uses "bait" to trick the victim and then "fishing" for the personal information they want to steal. In reality, voluntary emails are sent to victims by thieves pretending to be legitimate organizations such as businesses, corporations, or even banks. Then they try to obtain personal information such as credit card numbers and passwords and provide links to fake websites [33]. Vishing and smishing are samples of these phishing attacks.
   i. Vishing: The reason for naming is the use of voice and phishing to carry out the attack. Criminals usually call with a recorded message and instruct the victim to call a number and reveal some personal information. Maybe, they are asked to provide information over the phone rather than being directed to a website. Vishing scammers often use modern Voice over IP (VoIP) features such as caller ID spoofing and automated systems to avoid detection by law enforcement. This can also be done through social media platforms that are used by millions of people [8], [34:36].
   ii. Smishing: Smishing (phishing message service) is a type of phishing attack in which a text message is sent pretending to be a reliable source like a famous online store, with the aim of obtaining confidential information from a user for financial gain. The hacker sends a message to the potential victim that is a social topic or message that the victim might be interested in. By clicking on the link, the hacker steals the victim's information in the same way as a typical phishing method or allows the malware to be automatically downloaded to the victim's device. This malware can be specific to applications related to IoT devices and steal or control related information [8], [31], [37].

b. Spear phishing: phishing attacks (emails, voices, texts, or phone calls) are personalized in spear phishing attacks due to the amount of research and time spent on identifying people and then organizing and personalizing this attack, victims take a lot of suffering [38].
   i. Whaling attack: The term "whaling" refers to spear phishing attacks against high-ranking officials and other targets. The text will be tailored to the audience, an upper manager, and the corporate objective [38].
   ii. Pretexting: In the pretexting attack, an adversary uses a pre-designed scenario to legitimize himself with the victims in order to increase the possibility of phishing operations, reduce the suspicion of the victims, and ultimately mislead and deceive them to download a malicious attachment or click on a malicious URL. This kind of scenario to deceive the victim includes actions similar to those used by operators who offer IT after-sales services [39].

c. Spoofing: In this type of attack, the perpetrators fool the target by employing a reliable cover. They conduct their attacks by spoofing the IP or even the domain of a reputable organization. It’s different types include caller ID spoofing, email address spoofing, website spoofing, address resolution protocol, and DNS server spoofing [8], [40] and can be done through:
   i. Wi-fi phishing (Evil Twin): This phishing technique makes use of the Wi-Fi network to launch an attack. The attacker gains access to the access point and provides a stronger signal through it. As a result, the victim's device is connected to a stronger signal and all the information connected to the victim's Wi-Fi is available to the thief. In locations where there is free internet, this technique is highly common [8], [33].
   ii. Phone call: Calls pretending to be from customer service agents such as insurance, medical clinics, and e-commerce companies are some methods of fraud. The aim is to get the person to reveal personal information and login details or change access rights to their accounts [30].
   iii. Typo-squatting: Due to a typo or carelessness, the victim enters a site whose URL is similar to the desired valid site. Many of them are online payment page sites where users enter their confidential bank account information in them and suffer financial fraud. Scammers may also do this to damage the reputation of an online business. Simple and cheap domain registration incentivizes thieves to register domain names in bulk to profit from display advertising, drive traffic to third-party pages, deploy phishing sites, and deliver malware, or active robots [8], [40-41].

d. Baiting: Anything that can pique a victim's interest or stimulate their desire is used by the criminal to get what they want. Examples of baiting include placing malware in a way that might entice a victim to click on it or sending flash memory to a target without a note to stimulate their interest. It entails learning about the target's interests in order to use them as bait [26], [42].

e. Water holing attack: This term refers to predators who stalk their victims in proximity to watering holes in the natural world. In this attack, the attackers compromise websites that the targeted victim is likely to find interesting and infect one or more of them with malware [43].

f. reverse social engineering attack: In a reverse social engineering attack, the attacker employs a variety of strategies to convince the victim to get in touch with her rather than the thief calling the victim. Sometimes, after the initial attack, the victim will ask for assistance from someone who seems to be able to assist them (usually the thief herself). In this instance, the thief gives the victim advice on how to get aid, which results in the theft of his personal data [44-45].

2) Vulnerabilities: Thieves use vulnerabilities in electronic systems or computer software to steal personal information [46].
    a. SQL injecting: One technique involves injecting SQL into application fields to check system reactions. This technique is used to steal from databases that store people's personal information. This attack is the placement of malicious code in SQL statements, via web page input, and is one of the most serious threats to the security of database-based applications [8]. Albert Gonzalez, mastermind of one of the major attacks, used this technique to obtain more than 130 million credit card numbers from five companies and financial stores [30].
    b. Salami attack: A salami attack is when a criminal targets a small portion of a network, modifies them, and re-introduces them into the network without revealing its availability. The main characteristic of the salami attack is how little significance each attack has for the victim in comparison to the whole attack's scope. It means that every time a small part of the device or network information is attacked and stolen. It has a salami-slice-like appearance, as the name implies [11].
3) Malware: Some software is designed to evade detection mechanisms by gathering sensitive information or positioning itself for a high-impact zero-day attack. Although, thieves may also use other safe software for their malicious purposes.
    a. Keystroke logging: There is malware that records and processes all the keyboard movements of people. This means that whatever a person types on their keyboard, including their social network accounts, passwords, and other information, has the potential to be intercepted by hackers and exploited to corrupt all of their accounts [30].
    b. Ransomware: Ransomware threats to publish or block access to data or a computer system, usually by encrypting them. It requests to receive an amount to return them, and after that, there is no guarantee to preserve the disclosed information [47]. This method can lead to fraud in finance and information categories.
    c. Harvester: Harvester was developed by Christian Martorella in Python. This tool provides us with information about email accounts, usernames, and hostnames/subdomains from various public sources such as search engines and Pretty Good Privacy (PGP) servers. Although this tool is only allowed by the legal authorities of any organization and using this tool to abuse someone is against the law, thieves do not care about legality [48].
    d. Google Dorking: Google Dorking is a technique to find vulnerable targets. Google Dorking, also known as Google Hacking, can return information that is difficult to find through a standard search by using advanced search syntax to find and hack vulnerable websites, or IoT devices [49]. It provides a search string that uses advanced search operators to return usernames and passwords, email records, archives, etc. Ethical barriers protect critical information on the Internet. However, access to such information is occasionally required. Although Google Dorking should be used to improve framework security, attackers use this method for illegal practices, including digital scaremongering, modern clandestine activities, and fraud. It may be used to discover foundations, sensitive directories, sensitive documents, compromised servers, community or vulnerability information, multiple online widgets, files containing usernames and passwords, sensitive online purchase data, and pages containing login portals [48], [50].
    e. Botnet: A botnet is a group of connected computers that may have been intentionally infected with malware by cybercriminals or thieves. DDoS attacks, identity theft, and device access are all possible with botnets. A hostile attack known as a "botnet attack" is one that targets a network, network device, website, or IT environment. With the expansion of the IoT, the desire to turn devices into botnets increases, and the way for attackers to steal and access these devices is also opened in this way [51-52].
    f. Online traps :Users may occasionally be advised to utilize third-party products in pop-up windows, such as software, cookies, or plugins. Many blindly accept these messages and download a utility that serves no particular purpose. It is simply malicious software that stealthily gathers user data and transmits it to fraudsters. This pop-up can be a commercial website ad and data can be for the victim's credit account [53]. This method can lead to fraud in the category of finance, commerce, and information.
4) Eavesdropping: Attackers can employ a variety of techniques to initiate attacks, which frequently entail the deployment of different eavesdropping devices to listen in on conversations and examine network activity.
    a. Shoulder surfing: It is done by eavesdropping, looking over a person's shoulder while using an ATM or filling out forms, or physically stealing confidential files or computer hard drives containing identity information [8]. With the advancement of technology, other tools such as hidden cameras and secret microphones have also come to the aid of thieves.
    b. Data sniffing: Targeting local network-using companies and organizations is done through data sniffing. Hackers can gain access to the system and steal data since all network communications are sent to network ports.
    c. Nmap: Nmap ("Network Mapper") is free and open source for network discovery and security auditing. All devices are discovered by Nmap and then all the possible information is regained. It is also useful for tasks such as network inventory, scheduling service upgrades, and monitoring host or service uptime. Nmap employs new techniques to analyze raw IP packets in order to detect what hosts are available on the network, what services they are offering, what OS they are running, what type of packet filters/firewalls are in use, etc [54]. Now, all a hacker would need to successfully get into a targeted system would be to run Nmap on that system, look for vulnerabilities, and figure out how to exploit them. It should be assumed that the attacker controls all the Nmap facilities. He/ she has access to lots of data. For example, to identify potential vulnerabilities in

commercial websites, Nmap can be used by malicious users to steal customer data for fraudulent purposes [55]. Additionally, the open-source nature of this service makes it more appealing to criminals [48].

5) Data and information gathering: Thieves have access to various methods of gathering information. Often, victims fail to adequately protect their information due to its perceived lack of importance or sheer ignorance. In certain scenarios, the victims themselves unwittingly publish information that burglars require online. Regardless of the circumstances, the loss of personal information can lead to irreparable harm for the victim.
    a. Publicly available information: Fraudsters can collect publicly available data about the victim from sources such as e-commerce user accounts, social networks, or public records. They process this data to infer further private information and specifics [8], [30].
    b. Dumpster diving: This theft attacks the victims' discarded data, such as searching the victim's trash [8]. The thief's objective is to obtain information that the victim no longer wants or has discarded for any reason. Data that has been deleted may not have as strong protection, making it simpler for hackers to access it. This kind of theft may be done by recovering data from discarded personal devices such as a hard drive or a mobile phone, or by attacking the archives of a database.
    c. Dark web: Cybercriminals buy and sell a list of exposed personal information such as emails and passwords on the dark web. The use of this data for identity theft is possible [30]. Buying and selling this stolen data can be extremely risky for its owners and may lead to fraud in the Finance and Data categories.

Many of these methods can be utilized for the purpose of stealing information across various scenarios. However, certain strategies are designed with specific objectives in mind. For instance, whaling attacks are meticulously planned to achieve genuine financial or commercial goals and are seldom employed in other situations. Additionally, Wi-Fi phishing primarily targets IoT devices. While thieves employ a range of techniques, some thefts occur due to consumers' employment of weak passwords. Using a password that is easily guessed or reusing the same password for multiple accounts increases the risk of data breaches. Data theft can also result from poor password practices, such as writing passwords on paper or sharing them with others.

5 HARMS AND CONSEQUENCES

Being a victim of theft or identity theft can have detrimental consequences on the lives of those affected, with long-lasting effects that may persist for years. Furthermore, addressing and eliminating these negative impacts can be an extremely time-consuming task, often appearing insurmountable. Victims of identity theft endure significant harm in various aspects, each of which will be discussed individually. Although the extent of harm may vary among individuals, some victims may face less severe consequences, while others may suffer irreparable losses. The detrimental effects of identity theft are directly proportional to the duration of remaining undetected [2].

5.1 Financial and economic harms

The primary motivation for identity theft is financial gain, and as a result, the majority of victims experience financial loss. This loss can cause serious harm to their bank credit, making it difficult for them to secure a loan, gain employment, open a new bank account, or pass any background checks. Victims of identity theft also have to invest a significant amount of time in repairing the damage, which can adversely affect their careers and result in missed opportunities.

Identity theft can lead to both direct and indirect financial losses. Direct losses tarnish the victim's reputation, as they may face tax-related complications or encounter a fraudulent tax return filed using their stolen social security number, ultimately leaving them burdened with a substantial debt. Moreover, by gaining unauthorized access to the victim's bank accounts, thieves can completely drain their funds [2], [56]. Among all the groups of reasons mentioned in the previous section, the medical category can have the most financial losses. According to Ponemon Institute research in 2013 financial losses associated with medical identity theft can be significantly greater than losses from credit card fraud. 65 percent of medical identity theft victims averaged $13,500 to resolve they paid for this crime [57]. Their expenses included payments to health care providers, payments to insurance for services obtained by thieves, increased insurance premiums, or costs of interacting with an identity service provider or legal counsel [56]. Indirect losses also include necessary costs for correction, legal authorities, restoration of damaged credit, lost time, etc. [2], [58].

5.2 Legal harms

Legal and criminal problems can also arise as a consequence of identity theft. Often, victims remain unaware of their victimhood until they file a complaint or face conviction. Consequently, these individuals may find themselves facing lawsuits due to their substantial debts. In more severe cases, criminals might employ their stolen identification information to commit further offenses, resulting in the creation of a criminal record for the victims. This, in turn, could lead to imprisonment or hefty fines. Establishing the innocence of the victim can prove to be a challenging, time-consuming, and expensive ordeal [2].

5.3 Cultural and social harms

Identity theft and impersonation can inflict dishonor and irreparably damage the reputation and worth of the victim, often necessitating extensive and arduous efforts to rectify. Consequently, victims might face ostracization from society and encounter great difficulty in establishing their innocence. Moreover, as instances of theft and impersonation proliferate, societal trust erodes steadily, leading to far-reaching social repercussions.

5.4 Credit harms

One of the detrimental effects of identity theft is its potential to damage people's reputations [59]. As mentioned, the motive behind identity theft can be driven by revenge, with the thief seeking to jeopardize the victim's reputation. Moreover, even without malicious intent, thieves can exploit the victim's identity by disseminating unethical content under their name, thereby tarnishing their reputation. Additionally, perpetrators can exploit a person's or company's financial credit for deceptive purposes, resulting in harm to their creditworthiness and reputation. Consequently, this erodes the trust others place in the victims, making it difficult for them to regain confidence.**Health harms**

Health damage encompasses both mental and physical injuries that can mutually impact one another. Individuals with heart and digestive ailments, in particular, should prioritize their mental well-being more than others. Furthermore, exposure to stress and nervous pressure can lead to physical ailments.

- Physical Health Consequences: As previously mentioned, one specific category of identity theft revolves around health and medical information. Within this category, patient data can be manipulated or exploited by a third party, potentially leading to medical errors or misdiagnoses. This poses a grave danger, as it could result in the patient's demise, particularly if crucial details like blood type or allergies are tampered with or falsified. Moreover, individuals who fall victim to fraud may also experience physical issues, such as sleep disturbances, headaches, fatigue, changes in appetite, upset stomach, high blood pressure, and muscle tension or back pain, all of which stem from the psychological strain they endure [56]. According to the Identity Theft Resource Center (ITRC), 48% of identity fraud victims reported sleep disruptions, 35% experienced fatigue, and 34% suffered from headaches in the aftermath of victimization [60]. It's crucial to note that the elderly population, who often contend with preexisting conditions like hypertension and heart disease, are particularly vulnerable. Any exposure to identity theft places their health in significant jeopardy [2].
- Mental and Emotional Health Consequences: Being a victim of identity theft or fraud can elicit mental and emotional repercussions comparable to those experienced by victims of violent crimes. The emotional and mental responses encompass a wide range of feelings, including shame, fear, paranoia, disbelief, frustration, anger, and a profound loss of trust. Victims find themselves grappling with a constant sense of re-victimization and perceive their safety to be perpetually at risk. Given the significant number of individuals affected, the term "fraud trauma syndrome" was coined to capture and describe these traumatic experiences [2], [59]. Identity theft has an "aggressive aspect" as it often shocks the victim, resulting in far-reaching consequences that can profoundly impact various aspects of their life. This includes detrimental effects on their health, emotional stability, and interpersonal relationships. There are various reasons behind these destructive emotions, each contributing to the distressing aftermath of identity theft.

When identity theft leads to financial loss, the victim is burdened with debt and the added stress of economic pressure. They may experience feelings of guilt and a lack of confidence, especially if their identity was stolen due to carelessness in safeguarding personal information. As the thief's identity often remains concealed, the victim is plagued by a persistent sense of distrust. Any interaction or request for even the smallest amount of information from individuals or websites instills a sense of threat within them. Moreover, the anonymity of the thief further isolates the victims [61]. These lingering emotions can have severe effects on the victim, disrupting their daily life and overall well-being.

6 AGE AS AN INFLUENCING FACTOR IN RISK OF BEING VICTIM

Several factors contribute to the heightened risk of falling victim to identity theft. Among these factors, age plays a significant role. People's behaviors vary depending on their age, encompassing diverse attitudes towards personal freedoms, responsibilities, and possessions. Consequently, the potential gains that thieves can obtain from acquiring a victim's personal data may differ across different age groups. Figure 4 provides a visual representation of identity theft incidents reported in 2021, categorized by age [1].

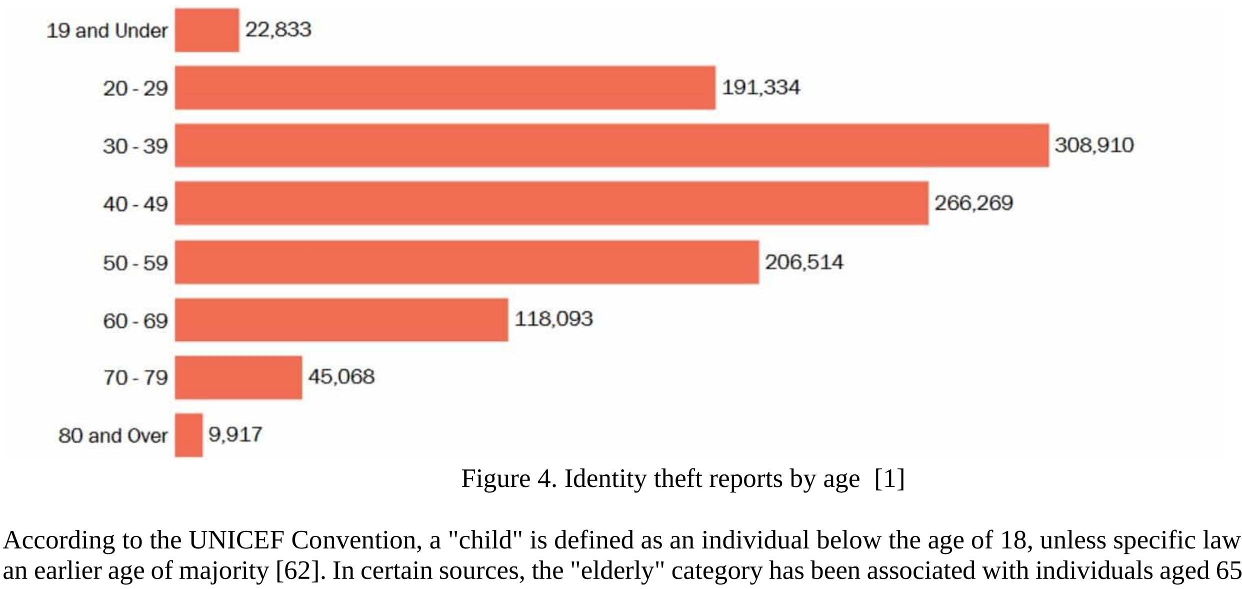

Figure 4. Identity theft reports by age [1]

According to the UNICEF Convention, a "child" is defined as an individual below the age of 18, unless specific laws recognize an earlier age of majority [62]. In certain sources, the "elderly" category has been associated with individuals aged 65 and above, as it marks the end of the working age [63]. Thus, society can be categorized into three distinct age groups: children, youth, and the elderly.

- **Children (under 18)**: Identity thieves often target children as an ideal age group for credit scams. Since children lack a financial history, their identities can be exploited without arousing suspicion, allowing perpetrators to reap financial benefits at the expense of their victims. What makes child identity theft particularly concerning is that it can go undetected for years, only revealing its consequences when these individuals reach adolescence and gain independence. Given their dependence on parents and limited involvement in financial activities and substantial transactions, it can be argued that this age group is less likely to fall victim to such crimes. However, children remain vulnerable to educational information theft, as their school-related data can be targeted. It's worth noting that infancy does not encompass key citizenship rights like voting and freedom of expression, reducing concerns about identity theft in that context. Nevertheless, when it comes to medical information, children with specific illnesses are undoubtedly at risk. Hospitals must take strong measures to safeguard comprehensive birth information to prevent theft and ensure the protection of children's identities [2], [9], [64].

- **Youth (19-64)**: This age group has achieved independence and possesses the capacity to either own an online business or act as consumers in the digital realm. They actively contribute to technological advancements and represent the largest consumer base for such innovations. Due to their extensive online presence, a significant portion of the available data pertains to this particular group, consequently heightening the risk of data theft. They possess the full range of rights enjoyed by citizens, including legal, educational, and medical entitlements, and are therefore responsible for safeguarding the identity information associated with their citizenship. Furthermore, this age group frequently wields IoT technology. While they may not face a high risk of medical identity theft in the absence of a specific ailment, they are not entirely immune either [65].
- **Elderly (over 65)**: Cognitive, medical, psychosocial, and environmental factors can contribute to the financial vulnerability of elderly individuals. Some vulnerabilities arise from concerns about maintaining independence and financial stability, which may prompt older adults to take financial risks. Furthermore, the higher prevalence of memory or cognitive disorders, such as dementia or Alzheimer's, among older adults can impede their ability to detect and respond to fraud. Exploiting the infirmities of the elderly, fraudsters may steal their information to gain access to their civil rights, such as voting and utilizing welfare and medical facilities. Various social engineering techniques are employed to victimize this age group. Due to the effects of aging, these individuals often experience health issues and require medical care, making them more susceptible to medical fraud. Monitoring factors like blood pressure, heart rate, and breathing rate, as well as regular doctor supervision, are crucial for their well-being. IoT devices offer viable solutions for establishing and maintaining this connection. While they may have a lesser presence in commercial activities, particularly in the realm of e-commerce, they are not entirely excluded. Many elderly individuals have a limited presence on the Internet.

The occurrence of different types of identity theft can vary in frequency across various age groups based on their capabilities. Nevertheless, it is important to note that thieves often exploit the personal information of individuals from all age groups, including their family members and social connections, to gather data for theft methods, particularly in social engineering attacks. While the significance of age groups may vary in certain instances of theft, it is worth mentioning that the likelihood of attacks for each age group is summarized in Table 1.

Table 1. The risk of identity theft in age groups and its related reasons

	Financial	commercial	Medical	Educational	Citizenship	IoT	Informational
Children	Low risk	Very low risk	Medium risk	Medium risk	Medium risk	Low risk	High risk
Youth	High risk	Very high risk	Medium risk	High risk	High risk	High risk	Very high risk
Elderly	Very high risk	Medium risk	Very high risk	Medium risk	Very high risk	Medium risk	Medium risk

Young people are often perceived as the socially active generation that is most vulnerable to various types of theft. This demographic holds the potential to earn a significant income, making them susceptible to potential harm. Despite possessing a commendable level of security awareness, this group remains exposed to multiple threats. Therefore, it is imperative for governments to prioritize the establishment of a security-conscious culture and implement proactive measures to prevent attacks within this population.

There is no justification for stealing identifying information, especially when it pertains to children, as it poses a significant risk. For instance, it is rare to come across a child with substantial financial resources or involved in running a successful business. Consequently, the likelihood of information theft affecting children for financial or commercial gain is lower. However, child information theft is not uncommon, primarily due to their limited understanding of security measures, which leads them to unwittingly provide extensive personal information that thieves can exploit, often causing troubles for their parents. Therefore, it is prevalent for perpetrators to employ various forms of social engineering techniques to extract information from children. This concern has become increasingly significant with the proliferation of children's presence on social networks and their extensive usage thereof.

Due to the multitude of health concerns and ongoing medical surveillance, many parents opt to insure their children from a young age. This is because children may be more vulnerable to medical incidents. The early establishment of a child's medical history, coupled with diseases that are specific to their age group, lowers the likelihood of successful theft targeting this demographic. Hence, it becomes dubious whether information can be effectively stolen for medical purposes during childhood.

Children are less likely to make use of industrial tools, and consequently, this demographic tends to be less concerned about IoT-related theft. However, the probability of an attack can be significantly higher among two specific categories: citizenship and education. Thieves may be motivated to target children in order to exploit their IDs for various educational benefits, such as citizenship rights, healthcare and maintenance privileges, recreational advantages, and more. Information theft within official academic settings encompasses both traditional forms of fraud that can occur throughout a child's school years and the misuse of a child's ID to exploit their privileges and capabilities.

7 CONCLUSION

This article serves as an initial step in combating identity theft by examining the motives and methods employed by thieves in carrying out this crime. The study comprehensively investigated seven distinct reasons behind different types of identity theft. It revealed that the primary driving force behind identity information theft is the pursuit of financial gain. The citizenship category encompasses financial, medical, and educational aspects, despite sharing some similarities among them. However, given that identity theft spans across these categories and occurs for various reasons, each category has been individually explored. In addition to financial gain, thieves engage in identity theft for commercial purposes, targeting IoT devices, and seeking valuable information. To illustrate the different methods employed, the study categorizes them into five groups: social engineering, vulnerabilities, malware, eavesdropping, and data and information collection. While any of these methods can be utilized for theft, certain techniques prove more suitable for specific cases.

The utilization of stolen identity information varies across different age groups. The risks associated with information theft are assessed by considering the factors that contribute to the theft and its subsequent use among various age demographics. Furthermore, this paper delves into an examination of the detrimental impact inflicted upon victims of information theft. Researchers acknowledge these harms and take proactive measures to mitigate the risks to victims' physical and mental well-being, as well as the potential financial, legal, credit-related, cultural, and social consequences they face. The remainder of this research focuses on an exploration of distributed systems, particularly blockchain technology, as a means to counteract identity theft within the realms of education, healthcare, commerce, and IoT.

8 REFERENCES

[1] FTC, "Data Book 2021, Consumer Sentinel Network," Federal Trade Commission, Washington, 2022.

[2] A. Ricks and Y.I. Erickson, "Identity Theft and Fraud Victimization: What We Know about Identity Theft and Fraud Victims from Research- and Practice-Based Evidence," Center for Victim Research, Washington, 2019.

[3] G. Inês, M. Martins and C. Cardoso, "Exploring the determinants of victimization and fear of online identity theft: an empirical study," Security Journal, pp. 1-26, 2022.

[4] M. D. Juan, R. P. Andrés, P. M. Rafael, R. E. Gustavo and P. C. Manuel, "A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain," International Journal of Modeling and Optimization, vol. 8, no. 3, pp. 160-165, 2018.

[5] S. Venkatraman and S. Parvin, "Developing an IoT Identity Management System Using Blockchain," Systems, vol. 10, no. 39, pp. 1-17, 2022.

[6] J. Cherus, J. Githeko, J. Siror and K. Njagi, "Identity Fraud: Literature Review and Future Research Directions," DRRI Journal (Multidisciplinary), vol. 5, pp. 36-53, 2014.

[7] A. Tajpour, S. Ibrahim and M. Zamani, "E-Commerce and Identity Theft Issues," International Journal of Advancements in Computing Technology(IJACT), vol. 5, no. 14, pp. 105-111, 2013.

[8] A. Tajpour, "Identity Theft and Fraud Type," International Journal of Information Processing and Management, vol. 4, no. 7, pp. 51-58, 2013.

[9] S.S. Sehgar and Z.A. Zukarnain, "Online Identity Theft, Security Issues, and Reputational Damage," 2 2 2021. [Online]. Available: doi: 10.20944/preprints202102.0082.v1. [Accessed 25 9 2022].

[10] M. Dadkhah, M. Lagzian and G. Borchardt, "Identity Theft in the Academic World Leads to Junk Science," Sci Eng Ethics, vol. 24, no. 1, pp. 287-290, 2017.

[11] S. Vidalis and O. Angelopoulou, "Assessing Identity Theft in the Internet of Things," IT Convergence Practice (INPRA), vol. 2, pp. 15-21, 2014.

[12] S. Rizvi, J. Pfeffer, A. Kurtz and M. Rizv, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in Proceedings of 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, 2018.

[13] H. Alrubayyi, G. Goteng, M. Jaber and J. Kelly, "Challenges of Malware Detection in the IoT and a Review of Artificial Immune System Approaches," Journal of Sensor and Actuator Networks, vol. 10, no. 61, pp. 1-20, 2021.

[14] R.C. Labong, "Identity Theft Protection Strategies: A Literature Review," Journal of Academic Research, vol. 4, no. 2, pp. 1-12, 2019.

[15] Q. Ye, Y. Gao, Z. Zhang, Y. Chen, Y. Li, M. Gao, S. Chen, X. Wang and Y. Chen, "Modeling Access Environment and Behavior Sequence for Financial Identity Theft Detection in E-Commerce Services," in International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 2022.

[16] Z. Vučković, D. Vukmirović, M. Jovanović Milenković, S. Ristić and K. Prljić, "Analyzing of e-commerce user behavior to detect identity theft," Physica A: Statistical Mechanics and its Applications, vol. 511, pp. 331-335, 2018.

[17] B. K. Ngugi, K.T. Hung and Y. John Li, "Reducing Tax Identity Theft by Identifying Vulnerability Points in the Electronic Tax Filing Process," Information and Computer Security, vol. 30, no. 2, pp. 173-189, 2022.

[18] O. Ogbanufe and R. Pavur, "Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection," International Journal of Information Management, vol. 62, p. 102432, 2022.

[19] J.Chen, X. Xie and F. Jing, "The security of shopping online," in Proceedings of the International Conference on Electronic & Mechanical Engineering and Information Technology, Harbin, China, 2011.

[20] D. Burnes, M. DeLiema and L. Langton, "Risk and protective factors of identity theft victimization in the United States," Preventive Medicine Reports, vol. 17, 2020.

[21] L. Seda, "Identity theft and university students: do they know, do they care?", Journal of Financial Crime, vol. 21, pp. 461-483, 2014.

[22] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, 2023.

[23] G. Mohamedbhai, "The scourge of fraud and corruption in higher education," nternational Higher Education, pp. 12-14, 2016.

[24] G. McKeever, "Social citizenship and social security fraud in the UK and Australia," Social Policy & Administration, vol. 46, no. 4, pp. 465-482, 2012.

[25] Y. Liu, Y. Wang, X. Wang, Z. Xia and J. Xu, "Privacy-preserving raw data collection without a trusted authority for IoT," Computer Networks, vol. 148, pp. 340-348, 2019.

[26] A. A. Alsufyani and S. Alzahrani , "Social Engineering Attack," International Journal of Advanced Research in Engineering and Technology (IJARET), vol. 11, pp. 965-975, 2020.

[27] M. Schäfer, M. Fuchs, M. Strohmeier, M. Engel, M. Liechti and V. Lenders, "BlackWidow: Monitoring the dark web for cyber security information," in 11th International Conference on Cyber Conflict (CyCon), 2019.

[28] C. Hadnagy, " Social Engineering: The Art of Human Hacking," USA: WILEY, 2010.

[29] S. Badotra and A. Sundas, "A Systematic Review on Security of E-commerce Systems," International Journal of Applied Science and Engineering, vol. 18, no. 2, pp. 1-19, 2021.

[30] C. M. Steel, "Stolen Identity Valuation and Market Evolution on the Dark Web," International Journal of Cyber Criminology, vol. 13, pp. 70-83, 2019.

[31] I.S. Mambina, J.D. Ndibwile and K.F. Michael, "Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach," IEEE Access, vol. 10, pp. 83061-83074, 2022.

[32] W. Priestman, T. Anstis, I.G. Sebire, S. Sridharan and N.J. Sebire, "Phishing in Healthcare Organisations: Threats, Mitigation and Approaches," BMJ Health & Care Informatics, vol. 26, no. 1, pp. 1-6, 2019.

[33] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," Future Internet, vol. 12, no. 10, 2020.

[34] K.S. Jones, M.E. Armstrong, M.K. Tornblad, and A.Siami Namin , "How Social Engineers Use Persuasion Principles During Vishing Attacks," Information & Computer Security, vol. 29, no. 2, pp. 314-331, 2020.

[35] N. Leena, "Cyber Crime Effecting E-commerce Technology," Oriental Journal of Computer Science & Technology, vol. 4, no. 1, pp. 209-212, 2011.

[36] J. Phomkamin, C. Pumpuang, P. Potijak, S. Sangngam, I. Ketprasit, and B.G. Mujtaba, "Engagement Strategies for E-commerce Businesses in the Modern Online World," SocioEconomic Challenges, vol. 5, no. 4, pp. 24-34, 2021.

[37] D. Kim, Y. Pan and J. Park, "A Study on the Digital Forensic Investigation Method of Clever Malware in IoT Devices," IEEE Access, vol. 8, pp. 224487-224499, 2020.

[38] E. RajaS and R. Ravi,, "A Performance Analysis of Software Defined Network based Prevention on Phishing Attack in Cyberspace Using a Deep Machine Learning with CANTINA Approach (DMLCA)," Computer Communications, vol. 153, no. 1, pp. 375-381, 2020.

[39] F. Sharevski and P. Jachim, "Alexa in Phishingland: Empirical Assessment of Susceptibility to Phishing Pretexting in Voice Assistant Environments," in Proceedings of IEEE Symposium on Security and Privacy Workshops, San Francisco, 2021.

[40] Z. Jiang, Z. Zhao, R. Li, J. Zhao and J. Du, "PHYAlert: Identity Spoofing Attack Detection and Prevention for a Wireless Edge Network," Journal of Cloud Computing: Advances, Systems and Applications, vol. 9, no. 5, 2020.

[41] J. Szurdi, B. Kosco, G. Cseh, J. Spring, M. Felegyhazi and C. Kanich, "The Long “Taile” of Typosquatting Domain Names," in 23rd USENIX Security Symposium (USENIX Security 14), San Diego, 2014.

[42] C. Iuga, J. R.C. Nurse, and A. Erola, "Baiting the hook: factors impacting susceptibility to phishing attacks," Human-centric Computing and Information Sciences, vol. 6, pp. 1-20, 2016.

[43] K. Krombholz, H. Hobel, M. Huber and E. Weipp, "Advanced Social Engineering Attacks," Journal of Information Security and Applications, vol. 22, pp. 113-122, 2015.

[44] T. Li, K. Wang and J. Horkoff, "Towards Effective Assessment for Social Engineering Attacks," in Proceedings of 27th IEEE International Requirements Engineering Conference (RE), Jeju, Korea, 2019.

[45] Y. S. Saini, L. Sharma, P. Chawla and S. Parashar,, "Social Engineering Attacks," in Emerging Technologies in Data Mining and Information Security, Kolkata, India, 2022.

[46] "OECD Policy Guidance on Online Identity Theft," in OECD Minisiterial Meeting on the Future of the Internet Economy, Seoul, 2008.

[47] N. Popli and A. Girdhar, "Behavioural Analysis of Recent Ransomwares and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware," Singapore.

[48] G. Saroj and R.G. Patil, "A Survey Paper on Identity Theft in the Internet," International Journal of Trend in Scientific Research and Development (IJTSRD), vol. 3, no. 4, pp. 969-970, 2019.

[49] "How to Use Google for Hacking Websites, Iot Devices, Cameras, etc.," 10 10 2017. [Online]. Available: https://cyware.com/news/google-dorking-how-to-use-google-for-hacking-websites-iot-devices-cameras-etc-cd577. [Accessed 15 10 2022].

[50] N. Amara, H. Zhiqui and A. Ali , "Cloud Computing Security Threats and Attacks with their Mitigation Techniques," in Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 2017.

[51] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, F. Aloul, "Botnet Attack Detection using Machine Learning," in Proceedings of 14th IEEE International Conference on Innovations in Information Technology (IIT), UAE, 2020.

[52] Y. Meidan, M, Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai and Y. Elovici, "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22, 2018.

[53] "Spyware and Malware," FEDERAL TRADE COMMISSION, 2022. [Online]. Available: https://www.ftc.gov/news-events/topics/identity-theft/spyware-malware. [Accessed 10 4 2022].

[54] "Nmap: Discover your network," [Online]. Available: https://nmap.org. [Accessed 30 9 2022].

[55] I. Baako, S. Umar and P. Gidisu, "Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study," International Journal of Computer Network and Information Security(IJCNIS), vol. 11, pp. 19-25, 2019.

[56] K. Golladay and K. Holtfreter, "The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes," Victims & Offenders, vol. 12, pp. 741-760, 2017.

[57] P. Institute, "Survey on Medical Identity Theft," Ponemon Institute, United States, 2013.

[58] D. Lukic, "Identity Theft Consequences, Why Should you Take it Seriously," 2021. [Online]. Available: https://www.idstrong.com/sentinel/identity-theft-consequences-why-should-you-take-it-seriously/. [Accessed 27 9 2022].

[59] D. Glodstein, S. L. Glodstein and J. Fornaro, "Fraud trauma syndrome: The victims of the Bernard Madoff scandal," Journal of Forensic Studies in Accounting & Business, vol. 2, pp. 1-9, 2010.

[60] I. T. R. Center, "The Aftermath The Non-Economic Impacts of Identity Theft," Identity Theft Resource Center, San Diego, 2017.

[61] M. Salcines, "A Lasting Impact:The Emotional Toll of Identity Theft," Equifax, Atlanta, Georgia, 2015.

[62] "Frequently Asked Questions on the Convention on the Rights of the Child," UNICEF, [Online]. Available: https://www.unicef.org/child-rights-convention/frequently-asked-questions. [Accessed 15 10 2022].

[63] M. R. Hannah Ritchie, "Age Structure," Our World in Data, 2019. [Online]. Available: https://ourworldindata.org/age-structure.

[64] C.D. Marcum, G.E. Higgins, M.L. Ricketts and S.E. Wolfe, "Becoming someone new: Identity theft behaviors by high school students," Journal of Financial Crime, vol. 22, no. 3, pp. 318-328, 2015.

[65] S. R. Department, "Share of Adults in the United States Who Use the Internet in 2021, by Age Group," 26 7 2022. [Online]. Available: https://www.statista.com/statistics/266587/percentage-of-internet-users-by-age-groups-in-the-us. [Accessed 15 10 2022].

Fatemeh Hora Haghighatkhah is a Bachelor’s student of Computer Engineering at Shahid Beheshti University. She is interested in research in the fields of artificial intelligence applications, e-commerce, information security, and blockchain. She pursues them with motivation and enthusiasm, and she is also concerned about them. She has participated in several projects in these areas and has gained valuable experience in applying new technologies to solve real-world problems. She is passionate about pursuing her academic goals and contributing to the advancement of science and society.

Maedeh Mosharraf is an Assistant Professor of Computer Engineering Software and Information Systems at Shahid Beheshti University (SBU) where she has served since 2021. She received her M.Sc. (2013) and Ph.D. (2019) in Computer Engineering from University of Tehran (UT). Her current research involves “Blockchain technologies and cryptocurrency”, “Digital transformation”, “Electronic commerce”, and “Technology enhanced learning”.