INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

REVIEW ARTICLE

Analysis of cyber attacks and security intelligence: Identity theft

Dr. Charu Virmani[1]*, Neha Kaushik[1], Mohak [1], Vishnu Mathur[1], Sanskar Saxena[1]

1 Manav Rachna International Institute of Research and Studies, Faridabad, 121004, Haryana, India

OPEN ACCESS

Received: 11-05-2020

Accepted: 10-06-2020

Published: 17-07-2020

Editor: Dr. Natarajan Gajendran

Citation: Virmani DC, Kaushik N, M, Mathur V, Saxena S (2020) Analysis of cyber attacks and security intelligence: Identity theft. Indian Journal of Science and Technology 13(25): 2529-2536. https://doi.org/10.17485/IJST/v13i25.580

***Corresponding author**.
Dr. Charu Virmani

Manav Rachna International Institute of Research and Studies, Faridabad, 121004, Haryana, India
charu.fet@mriu.edu.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

Abstract

Objectives: To analyse the cybersecurity risks and their impact on the organizations. Researcher attempts to list down the issues and mitigation of Identity theft as a risk. **Methods:** This study develops a theoretical framework for future researchers and organizations for awareness and impact of Identity theft in area of cybercrime. The study has dogged various mechanisms by which watermarking can be applied to overcome to prevent identity theft attack. **Findings:** Researcher has emphasized the need for security solution and listed the steps to achieve security. An integrated view of identity theft and watermarking is formulated and proposed. The right balance between the application and techniques of watermarking opted will protect the user against the various types of identity theft attacks. **Applications**: Identity Theft has gained momentum in online space. The study highlighted various issues, consequences and economy of identity theft attacks with securing networks for unauthorized access. Watermarking plays an important role in authentication and authorization of data and proved a viable solution to mitigate identity theft attack.

Keywords: Cyberspace; identity theft; Security intelligence; watermarking

1 INTRODUCTION

Internet and advanced technologies have an influence on modern society covering a large spectrum of businesses, academic institutions, governments, and IT sector [(1)]. Online users often suffer from identity fraud, hacking, child pornography, etc. The latest technologies like viz. E-commerce, net banking, healthcare and personal data on cloud storage need high security as large number of users is active on this advanced technology. Cybersecurity is the extension or advanced version of the information technology (IT) security which is used to protect systems, applications, and data that are exposed to a variety of attacks via the internet, ranging from data theft to denial of service attacks [(2)].

There are also growing threat at the advent of social networking usage through whatsapp, instagram, twitter, linkedin, Facebook where sharing of personal information is often misused and users become more vulnerable in the hands of hackers.

1.1 Classification of Frauds

Stealing user's information illegally for example, name, date of birth, phone number, bank account number, passwords, etc.[3] for misuse of user's personal details. Various types of fraud have been observed after critical examination of the study:-

- Spoofing/Phishing Scam: E-mail and websites are the best way for spoofing by which phisher steal user's important information.[4]. An E-mail that is sent by the hacker and it looks trustworthy email to the victim and verify that link before victim open site through a link.
- Credit/Debit card fraud: It is a kind of identity theft in which fraudster uses victim's identity or information to make frauds. This fraud is occurred by accessing an unprotected site like online shopping.
- Logic bombs: Code running within a program or system that remains inactive until occurrence of specific conditions. It works only when specified condition i.e. date and time encountered in the code. This can be used by viruses that are attached with links and it spread in user's system without being noticed.
- Hacking: Hackers are experts in technology main purpose of hackers is for security but they can misuse these skills for frauds also. Hackers can access user's system without user's permission with advanced knowledge of technology.
- Cyberstalking: Stalking or harassment that is done via the internet or electronic devices. Some victims may not realize that they are being stalked online and fraudulent spread false rumours about you.
- Email Bombing and spamming: Email bombing is like abusing online or cyberbullying, sending emails continuously without pausing, and overflow the inbox where victim can't do anything to stop these spam emails.
- Slicing fraud: Stealing an extremely small amount of money at a time. In this criminal steal funds and doesn't get any notification.
- Denial of Service (DoS): This may affect by using email, banking, not secure websites, or different services that affect computers or networks.
- Crypto-jacking: Basically, in crypto-jacking criminals hijack PCs secretly and this can be done by clicking on a link in an email or through an unsecured website.

1.2 Classification of Identity Theft

Critical examination of the study revealed various ways to steal and use personal information as depicted in Figure 1 .

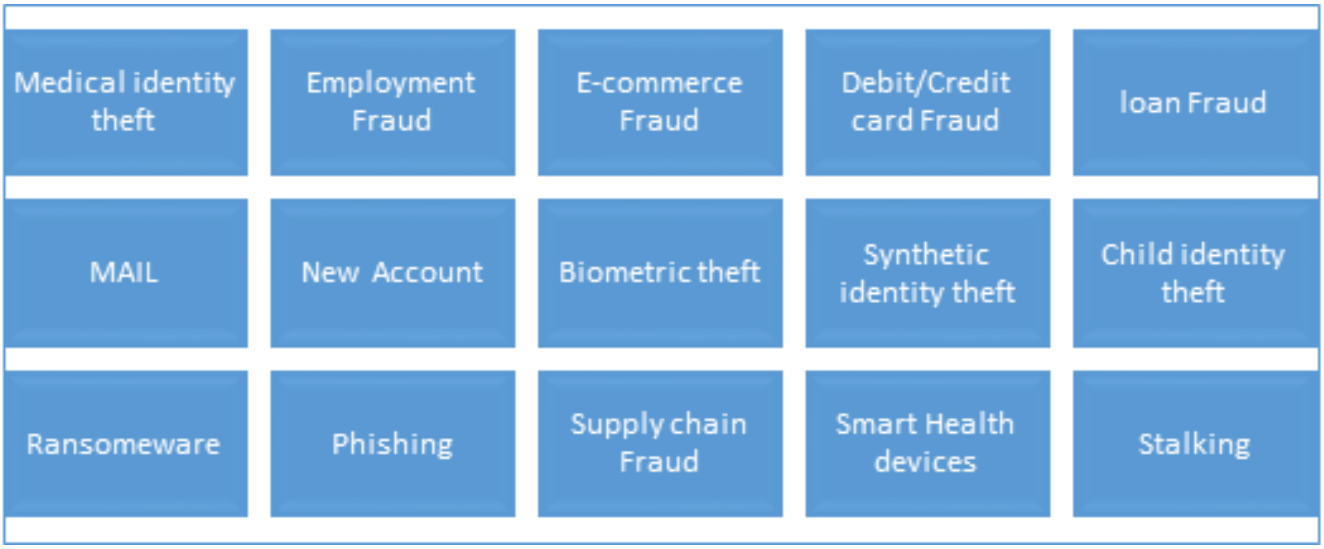

Fig 1. Classification of identity theft

- Mail theft: The most common identity theft through which criminals steal victim's personal information[5]. Theft may steal victim's financial account information and misuse user's information.
- Debit/credit card fraud: Theft can steal victim's account number UPI PIN or security code to make transactions.
- E-commerce Fraud: It is also known as an online shopping fraudster that can steal victim's account information or steal payment information or may change victim's address.

- Employment Fraud: Maybe fraudsters use victim's identity for a job or business. Companies who claim a higher position in a famous company.
- New Account Fraud: When criminals create a new account by using victim's name/identity/personal information. It has been recommended to pay attention to the messages received.
- Biometric Theft: Verify a person's identity when a device is stolen such as the face, fingerprint, or voice recognition. These attributes are unique but in the wrong hands it's not safe.
- Synthetic Identity theft: Fraudster use fabricated and real data to create fake data or identity. Fraudsters may use fake identity to take a loan or apply for a job or used fake identity in business [6].
- Loan fraud: Loan fraud is comparatively easy as all agencies not provide all the terms and conditions or information which makes it easy to steal user's identity, bank account, etc.
- Child identity theft: It has been recommended that under 16 years of age, children shouldn't create an online account. This information may be used by fraudster to create a new account or may be to open a new bank account.
- Medical identity theft: Theft uses victim's personal information to obtain medical facilities or services.
- Ransomware: Multiple devices are connected with one network for example, all home appliances [7]. Hacker access system in the back end and the user has no idea. Many businesses could be impacted.
- Phishing: This is very common as criminals want user's personal details like name, passwords, phone no, social accounts, or debit/credit cards and they communicate them with the help of email or SMS.
- Supply chain fraud: One need to work on a third party for services. This increases attacks or cybercrimes day by day so update user's software regularly.
- Smart health devices: The Healthcare industry is also not safe from cybercriminals as now these industries can monitor medical condition also suggest to us. It can steal user's information or insurance and maybe messing with medicines or stop pacemakers or reveal user's medical condition.
- Stalking: Cyber Stalking or bulling is very risky these kinds of cases are also increasing. Many people do cyber stalking just for competitions especially in jobs or businesses.

The upcoming section highlights various techniques which are used by criminals to deploy identity theft attack.

1.3 Techniques to deploy Identity Theft

Various techniques have been observed during the study that is used by criminals in today's generation to achieve identity theft [8], discussed as follows:-

- Changing user's address: Criminal changes victim's location/actual address.
- Computer identity theft: Thieves steal victim's personal information or leak important data or delete important files by using hacking or virus by attaching through mail or unauthorized sites.
- Social networking: Thieves steal victim's information through social networking sites so that they do fraud with the identity of the user.
- Employment scam or fraud: Never deal with anyone without knowing their real identity. Do not provide user's documents for a job without knowing about that company.
- Pretexting identity theft: Criminal sends user's false information to obtain user's correct information.
- Skimming identity theft: Thieves steal user's card number (account number, CVV, date, cardholder name etc.) by attaching a device with ATM and that device read the magnetic strip on user's card.
- Phishing identity theft: Criminal forwards you spam and pop-up messages to reveal user's real identity. Regularly update user's firewall, anti-virus, etc. Never click any link in the spam e-mail.
- Fishing identity theft: Thieves can steal user's personal information by providing offers or discounts.
- Don't share OTP: Never share user's OTP because the bank never shares any OTP or call you for OTP or send you an email.
- Disable the autofill feature on user's phone: Never save user's password or don't able to enable autofill especially for banking purposes.

The next section 1.4 shows detailed analysis reports of identity theft for the duration 2018-2019 and section 1.5 shows reports of identity theft and fraud for the duration 2015-2019 respectively.

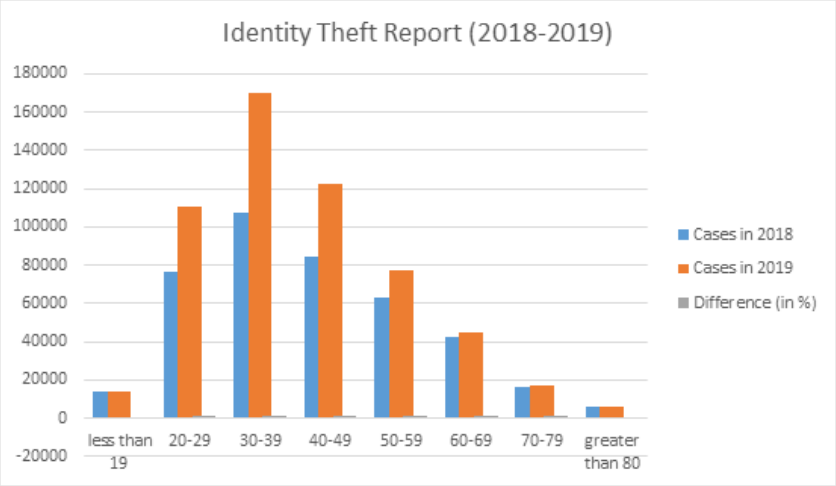

Fig 2. Analysis of Identity Theft 2018-2019

1.4 Reports of identify theft (in 2018-2019) :

As it is clear from Figure 2, most of the identity theft cases can happen in 30-39 age and least cases can happen in greater than 80 age group. Total cases in 2018 are 410927 of identity theft but in 2019 there are 562864 cases that mean 37.0% change from 2018 to 2019. Least change is in greater than 80 age groups that are -5.0% from 2018-2019 [9].

1.5 Reports of identity theft and fraud (in 2015-2019)

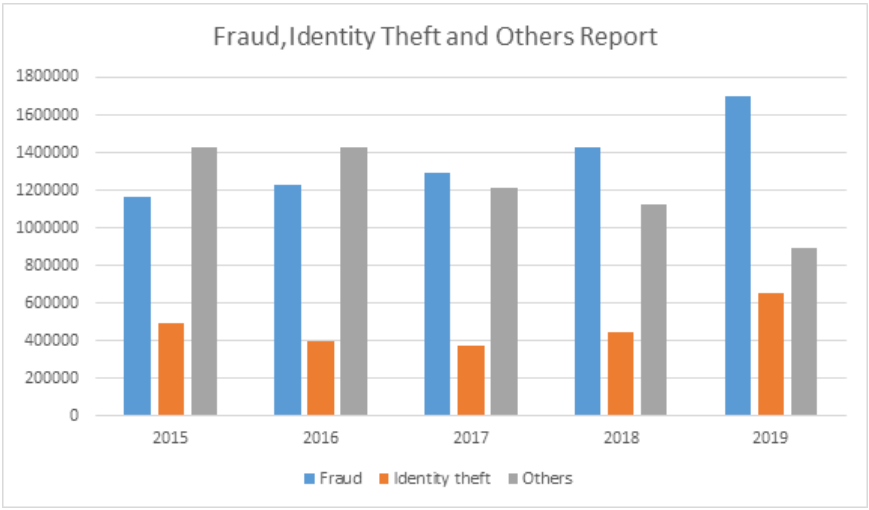

Fig 3. Analysis of Identity Theft 2015-2019

Identity theft and fraud cases have exponentially increased day by day. In 2019, there are 1.7 million cases of fraud, 89200 cases of others, and 651000 cases of identity theft. Identity theft and fraud cases increase form 2018-2019.

The upcoming section elaborates on the counter measures of identity theft.

1.6 Countermeasures of identity theft

As this era is the era of digital technology, it is important to know about how to prevent fraud and identity theft. Following are the counter measures:

- Use a pin and other login methods on user's PC: Most of the people use the same password or username on user's websites, so a hacker can easily hack user's account or assume user's passwords. Now, many operating systems give local passwords because if some try to use that password on another system it will fail.
- Change user's password regularly: Hacker may try to access user's account by frequently changing user's password to reduce the risk. Try not to use the same password or similar password for another account.
- Verify the link that you received: Don't click on a link which you received to the unknown site or attach it with e-mail or any social media app/site and don't allow any site to run JavaScript, pop-ups and track user's physical location. Otherwise, hackers receive user's personal information.
- Check user's privacy setting: Before using any social media, the platform makes sure that you read all the terms and conditions and make it private also so that strangers won't be able to see user's personal information or posts. And also check privacy settings regularly on social media.
- Make sure user's device is secure: Install firewall, anti-virus and also update them regularly on user's smartphone, laptop or any digital devices to protect user's privacy.
- Don't use user's personal information in user's username or in e-mail id: Try to avoid user's personal detail in social media username or any other websites or in user's email id because it is easy to know user's basic information through user's email id or username, for example, date of birth in a username, etc.
- Check user's order status: One can also say order tracking system. Always check details about user's past and present order. After shipping user's order, you can track user's order via site or app. By clicking that link you can check the delivery status.
- Pay user's bill online: It is also known as electronic bill pay. One can check user's balance, or whether user's bill is paid or not. One can also access user's all transaction or online payment history.
- Don't take a survey at home: The simplest way to use user's identity, stranger ask you some basic and simple questions like user's age, family member, religion, status, etc. and fraudster easily get a loan on user's identity.
- Provide less information to 3rd party apps: Especially on social media platforms try not to provide all information or user's personal data.
- Be careful what you post on social media or any other platform: If user's friend and family account get hacked that means hackers can access user's account too. So, try to avoid user's personal feeling, information, etc.

The next section reflects digital watermarking as a promising solution to identity theft.

2 Digital watermarking

It is a technique of hiding digital information in a carrier signal. It is used to verify the identity of the owners and it used for tracing copyright infringements. Traditional watermark work on visible media like pictures whereas digital watermarking is used on videos, 3D models or images, etc. It is a kind of protection tool for data (copyright protection, video authentication, ID security, fraud detection etc.).

2.1 Watermarking techniques

As technology usage increases and one need our information secret or protected if in case anyone tries to hack user's personal details, he/she get difficulty. For this kind of security, one use watermarking techniques, with the help of watermarking only users can access or use the data [10]. They are based on which domain, kind of documents like text, video, etc. and human perception these things are most important for watermarking or one can also say classified in these categories. Watermarking work in different application like a medical report, copyright protection; protect user's information, etc. Following are the uses of watermarking:-

- Invisible/Imperceptiblity: Add invisible watermark to an image. Pixel values get change when one conveys a secret message. One can't recognize the difference between real and watermarked image
- Embeds code: It embeds a secret message attached to the image.
- Robust: Image has been edited like cropping, editing, compression, etc. This kind of technology is also known as a digital tattoo. One can use a stuck message on the image.
- Forensic: Videos of movies are watermarked.
- Content protection: Audio in movies theatres or blu-ray discs is also watermarked.
- Content integrity: Some time local channels shorten the ads.
- User tracing: Multi content share on the websites as per the demands.

Cybersecurity is an advance version of the Information technology (IT) to protect user's system, data and identity from a vast spectrum of attacks[11]. It consists of combining an image with the fingerprint or security of the owner. It is a kind of secret key which is used by the owner only. Used for mesh pictures together, make memes and comics, protecting pictures, etc. There is a need of more robust security as technology increasing day by day for business, watermarking is one of the known promising solution especially focusing on identity or bank account.

- Confidentiality: It is the technique to maintain confidentiality of the data.
- Integrity: You can monitor user's image with the help of digital watermarking.
- Privacy: It is a technology used to secure user's identity or information and doesn't affect user's data, identity, etc.
- Availability: It provides attributes for providing legitimate data to the user.

It is imperative to decide the design and technologies to be utilized for the security against the attacks. The potential attack unfolds the corresponding mitigation for ensuring security under above listed attributes. Possible mitigation techniques are IDS, Firewall, and Anti-Malware software.

The next section explains some cases of fraud and identity theft which was faced before 2020.

3 Case Study

Following are the cases thoroughly studied for identity theft attack[12–17] :

- Fraud in during lockdown (the year 2020): Banks warn customers to be aware of some fraud calls, a fraudster is calling the customer and ask for OPT number once you share user's OTP fraudster stole all money form their account. Don't share user's OTP with anyone. Beware of verification calls also they pretend you that they are bankers and they asked some questions for security purposes.
- Identity (the year 2020): Many peoples get some attractive emails like free data, free subscription. And many people click on that link and give a survey and even they forward that fake message also. This is phishing and they steal user's sensitive information. And even many fake mails are getting forward and even criminals are targeting COVID funds also.
- Sony India Private Ltd. (the year 2013): www.sonysambandh.com This website targetted non-resident Indians, NRI's send some products in India and they pay online. Someone ordered cordless headphones to be delivered in Noida. After making payment and clear dues he/she came to know that transaction was denied by the owner.
- Cyberattack on Cosmos bank (the year 2018): The Pune branch of the bank was drained of 94 crores in August 2018. Thieves transferred money or funds to another bank which is in Hong Kong and also gains details of many debit/credit cards. In this case, 14000 transactions were carried out across the 28 Countries and 2800 transactions nationally. This is a malware attack.
- Cybercriminal forum was taken down (the year 2015): A most prolific criminal who hacked several debit/credit cards, information, or personal identity, this is a very complex cybercrime all over the world. They send some formal invitation to join. And candidate post some basic introduction and survey.
- Operation ghost click (the year 2011): It is an international cybercrime or ring that infects many PCs worldwide with a virus. And the user doesn't have any idea about that virus. It used malware which is called DNS Changer it infects or damages millions of PCs in more than 100 countries.
- Hacking website (the year 2018): Hacked US military and government websites and more than 11000 websites all over the world including business sites. The hacker fights for the terrorism center in New York City and uses online name alfabeto virtual.
- Identity theft and fraud scheme (the year 2018): These 11 agencies developed a scheme to steal user's identity or user's personal information these agencies stole a million dollars from debit/credit cards and banks too.
- Email phishing scam (the year 2018): He did $1.1 million email phishing scam in 2018. He stole money from various banks and a third party to fill his need.
- Yahoo mail scam (the year 2013-2014): 2013 affects more than 3 billion and in 2014 million user accounts. Thieves steal users' names, Date of Birth, phone number, and passwords. Yahoo hit many shareholders after breach or fraud and them disclosure that accounts struck a balance.
- DDoS attack (the year 2018): Most popular online code service gets targeted i.e. GitHub which is used by millions of developers. Because of good protection and services, they show an alert message within 10 minutes.
- DDoS attack or Dyn attack (the year 2016): This attack was ruinous for major sites like Netflix, PayPal, Amazon, GitHub, Reddit, etc. done by using malware attack which is known as Mirai. It creates an internet connection out of IoT devices.

To create attack these devices i.e. IoT devices (like smart TVs, radios, monitors, etc.) and this program send a request to the victim.

- Spamhaus attack (the year 2013): With the help of spam emails and messages, and they target peoples. But this attack does not achieve a goal.
- Target Targeted (the year 2013): In December 2013, 110 million customers lost their details within 15-20 days. Including bank details name, address, contact number, email address, etc. approx. 70 million users. This technique is called RAM Scraping.
- Alteryx data leak: Data leaked more than 123 million households with their personal details that are there income, name, family members, etc. including credit/debit cards.
- Marriott hotels: Approx. 500 million guests get targeted include their bank details, personal information (name, residential address, email address, phone number, passport number, etc.)
- Russian Hacker (the year 2014): More than 1.2 billion logins and passwords get stolen more than 420000 websites around the world in August 2014.

4 An Integrated view of Identity Theft and Watermarking

Drawing upon current classifications and the process models of identity theft, a new integrated view is proposed in the Figure 4 .

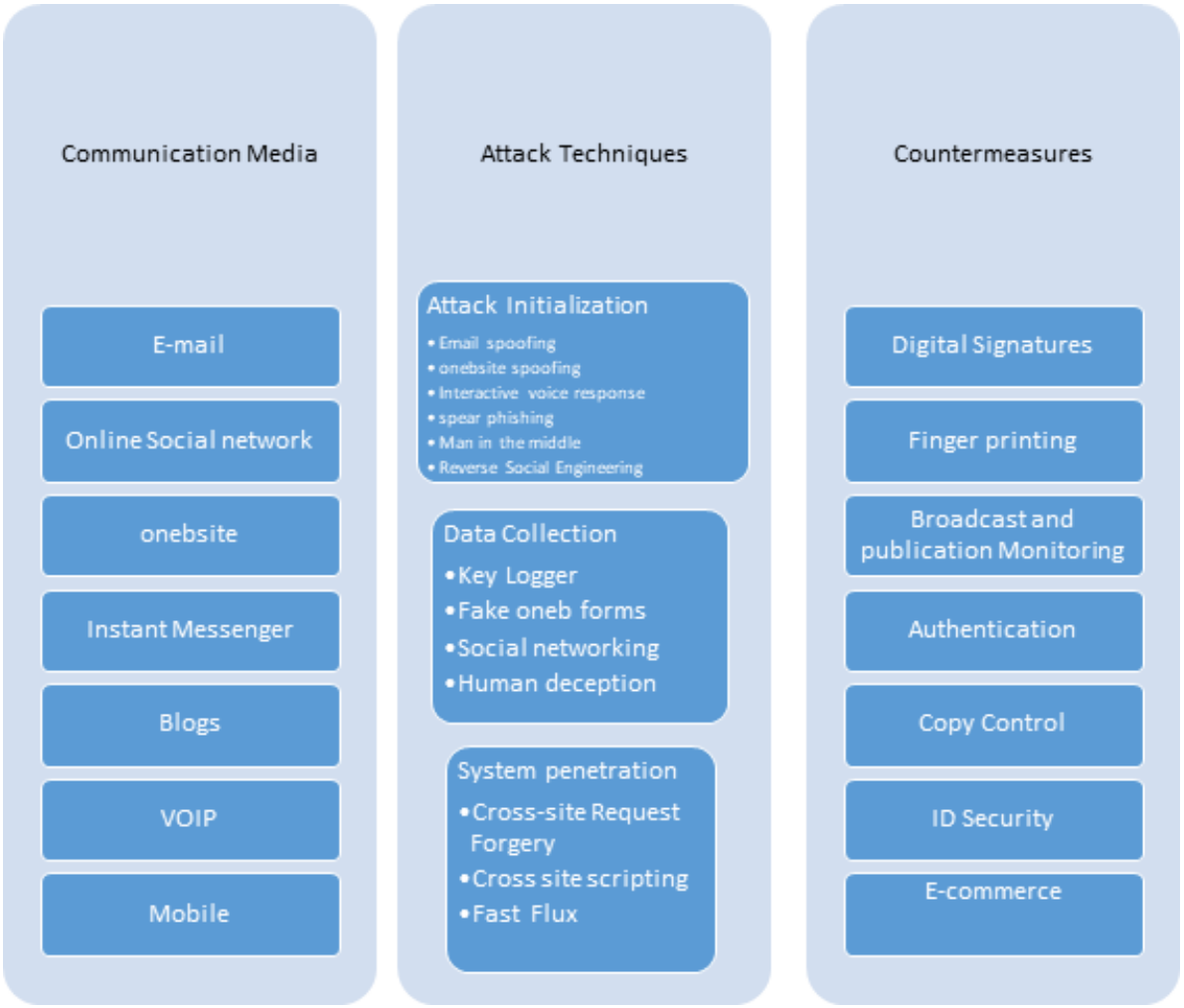

Fig 4. Integrated view of identity theft and watermarking as a solution

Communication medium in the above figure represents the mode of interaction of the victims with the applications targeted by types of identity theft attacks. To succeed in attack, there are various techniques that can be utilized. Broadly these techniques can be classified into initialization of the attack, collection of the data and system penetration. Initialization process involves the analysis of the social context of the user. Data collection techniques emphasizes on the mechanisms to collect information from users during the user's interaction with the success of attack. System penetration exploits system resources for facilitating identity theft attack The Countermeasures section of the view represents the use of watermarking techniques that can be integrated with application and embedded algorithm to mitigate the possibility of identity theft attack. It ensures the fundamental role of ownership, reliability, protection of data and other aspects of the information can also be verified.

5 CONCLUSION

Cybercrime and cyber security are interconnected issues that cannot be separated. The advancements in the information technology have led to the analysis of cybersecurity and a great deal of work is yet to taken for the acceptance of true system. The growth of each nation and economic well-being concerns with the protection of information and its cybersecurity infrastructure. Major challenge is to maintain the right balance and strike an integrated picture to formulate the policies. The proposed integrated view of identity theft and watermarking as a solution to mitigate the attack can depend upon the domain of the application for which the service being offered. Thus, it is concluded that the watermarking plays a significant role in cyber security.

References

1) Braun SK. Forensic evidence of copyright infringement by digital audio sampling analysis - identification - marking. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*. 2014;3(3):170–182. Available from: https://doi.org/http://dx.doi.org/10.17781/P001337.
2) Zhang H, Jiang R and Li A. A Framework to Construct Knowledge Base for Cyber Security. In: and others, editor. 2017 IEEE Second International Conference on Data Science in Cyberspace . 2017,. Available from: https://doi.org/10.5121/ijaia.2015.6102.
3) Heonett R, Rudrapattana S and Kijsanayoth P. Cyber-security analysis of smart SCADA systems with game models. In: and others, editor. Proceedings of the 9th annual cyber and information security research conference. ACM . 2014,. p. 109–112. Available from: https://doi.org/10.1177/1550147718794615.
4) Thomas J. Individual cyber security: Empoonering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*. 2018;12(3):1–23. Available from: https://doi.org/10.5539/ijbm.v13n6p1.
5) Anderson KB, Durbin E and Salinger MA. Identity Theft. *Journal of Economic Perspectives*. 2008;22(2):171–192. Available from: https://dx.doi.org/10.1257/jep.22.2.171.
6) Luna R, Rhine E, Myhra M, Sullivan R and Kruse CS. Cyber threats to health information systems: A systematic review. *Technology and Health Care*. 2016;24(1):1–9. Available from: https://dx.doi.org/10.3233/thc-151102.
7) Mercuri RT. Scoping identity theft. *Communications of the ACM*. 2006;49(5):17–17. Available from: https://dx.doi.org/10.1145/1125944.1125961.
8) and TN. Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors. *International Journal of Cyber-Security and Digital Forensics*. 2014;3(1):72–83. Available from: https://dx.doi.org/10.17781/p001287.
9) Romanosky S, Telang R and Acquisti A. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*. 2011;30(2):256–286. Available from: https://dx.doi.org/10.1002/pam.20567.
10) Hille P, Walsh G and Cleveland M. Consumer Fear of Online Identity Theft: Scale Development and Validation. *Journal of Interactive Marketing*. 2015;30:1–19. Available from: https://dx.doi.org/10.1016/j.intmar.2014.10.001.
11) Harrell E. Victims of Identity Theft . 2016,. Available from: https://www.bjs.gov/content/pub/pdf/vit16.pdfhttp://hdl.handle.net/20.500.11990/1084.
12) van de Weijer SGA, Leukfeldt R and Bernasco W. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*. 2019;16(4):486–508. Available from: https://dx.doi.org/10.1177/1477370818773610.
13) Andringa M, Glau L, Slaton J and U S Patent Application. Method and System for Preventing and Detecting Identity Theft . . Available from: http://www.ipwatchdog.com/2014/12/04/jpmorgan-chase-software-patent-portfolio-grows-larger/id=52454/.
14) Ricks A and Irvin-Erickson Y . 2019,. Available from: http://hdl.handle.net/20.500.11990/1196.
15) Zaeem RN, Manoharan M, Yang Y and Barber KS. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security*. 2017;65:50–63. Available from: https://dx.doi.org/10.1016/j.cose.2016.11.002.
16) Sproule S and Archer N. Measuring identity theft and identity fraud. *International Journal of Business Governance and Ethics*. 2010;5(1/2):51–51. Available from: https://dx.doi.org/10.1504/ijbge.2010.029555.
17) Manap NA, Rahim AA and Taji H. Cyberspace Identity Theft: An Overview. *Mediterranean Journal of Social Sciences*. 2015;Available from: https://dx.doi.org/10.5901/mjss.2015.v6n4s3p290.