International Journal of Research in Social Sciences
Volume 9, Issue 5 (May 2019)
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cyber Cloning By Artificial Intelligence and Cyber Crime

***Sanjum Bedi**

Abstract: - Online frauds are used by the perpetrators for nefarious activities. The most potent weapon in the hands of terrorists are the social media platforms. 'Cloning' was just a word found in the dictionary before 'Dolly the Sheep;the first cloned mammal was produced by the technique of cloning in Rosalin Institute in Scotland in 1996. After this discovery, food was cloned and controversies related to cloning of human beings started fuming up. Cloning has now crossed its biological frontiers to step into the virtual world under a new name — Cyber Cloning. Social media platforms are one of the top destinations for Cyber Attacks due to Cyber Cloning. In computer science, cloning is the process of creating an exact copy or replication of another application program or object. However, the replicated application does not contain the original source code. Source code is the language or string of words, numbers, letters and symbols that a computer programmer uses. The source code is the foundation for software creation. The duplicity of the source code is not easy to be detected by an internet user. Identity theft, stealing of money, impersonation, terrorism and other antisocial and antinational activities are performed by the cyber thieves and cyber terrorists. Every sixth social media user in India is a victim of online frauds because social media scams occur due to the ignorance of the internet users as these cloned accounts look ordinary and harmless. Criminals adapt Artificial Intelligence and use software systems for their operations for money motivated crimes.

Keywords: Cyber Cloning, Replication, Artificial Intelligence, Identity Theft, Database Security, Phishing, Sovereignty, Spoofing, Deep Fakes, Biometrics

***Research Scholar, Department of Law, Punjabi University, Patiala.**

INTRODUCTION

Cybercrime investigations become complicated because it is done with the use of complicated technology and it is often difficult to find out the real face of the criminal. Artificial Intelligence technology is used by the cyber criminals to conduct crimes in a more sophisticated manner. Mobile phone technology provides enough data to clone digital instruments by collating the

information by stealing the PIN Codes with the use of artificial technology to make fraudulent withdrawals. **ATM skimming devices**, fake cash machine implantations and more crooked methods give shape to cybercrime. Manipulation of hyper realistic audios, pictures, videos, signatures can be done by deep complicated algorithms through **Digital Cloning**.[1] This kind of emerging technology makes it difficult for the human eye to distinguish between the real and fake. This brings out potential legal and ethical concerns. **'Man –in-the- browser –attack'** is a form of internet threat which is a proxy '**Torjan Horse**'.[2] A Trojan horse is malicious software that looks like a bona fide or legitimate application which can take control of your computer to trick the user and clones all the digital information of the user. A Trojan is designed to damage, disrupt, steal, or inflict some other harmful action on a data or network. Information related to personal lives is obtained by cyber criminals through by the misuse artificial intelligence.

ARTIFICIAL INTELLIGENCE AND CYBER CLONING

Artificial intelligence has the potential to radically change the future use of information technology by the society. The national agencies should develop specific initiatives—aligning with existing national cyber and AI strategies—that confront the AI-enabled cybercrime botching up the technology by giving rise to Cyber Cloning issues. The Bitcoin Scam that took place recently is a glaring example of Artificial Intelligence enable crime. In this incident, the accounts of many high profile figures like former US President Barack Obama, Amazon CEO Jeff Bezos, Microsoft Corp co-founder Bill Gates were hacked in a bitcoin scam.[3] This is done by cloning the digital information of the victim's account and having full control over it. Cyber Cloning is a new class of crime in India. It is tough to procure the right lead and make the right interpretation are very important in solving a cyber cloning crime. However, the relationship

[1] Wesley Fenlon (November 2010) "How does ATM skimming work?"
https://money.howstuffworks.com/atmskimming.htm

[2] Margaret Rouse (January 2017) "Card Skiming" https://whatis.techtarget.com/definition/cardskimming

[3] https://www.hindustantimes.com/business-news/cloned-the-rising-cases-of-cyber-crimes-in-india/story-yR8Emqv3SuzaGoCsYvpBJK.html

between legal/constitutional order and science/technology is quite unexplored in some developing countries.

INFORMATION TECHNOLOGY ACT, 2000 AND CYBER CLONING

Cyber Cloning are a new class of crimes to India, rapidly expanding due to extensive use of internet. The shift from paper-based to electronic transaction has resulted into Cyber Cloning crimes. Cyber Cloning has raised concerns regarding recognition, authenticity and enforceability and handling of documents and signatures. The Information Technology Act, 2000 was enacted in order which was further amended in December 2008 which is comparatively a new legislation to deal with electronic commerce. Still twenty years have passed since this act was enacted and since then, technology has changed at a much faster pace.[4] Till year 2000, India did not have any legislation governing cyber space or Information Technology Law. In consideration to the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and to give legal recognition to electronic commerce.[5] The

credit card and debit card fraud by Cyber Cloning is a wide-ranging term for theft for the purpose to obtain unauthorized funds from an account. The risk of Cyber Cloning has increased manifold especially after the advent of e-commerce.[6]

The fraud of Cyber Cloning begins with either the theft of the physical card or the compromise of data associated with the account, including the card account number or other information. This information would routinely and necessarily be available to a merchant during a legitimate

[4] https://www.cirt.gov.bd/latest-cybercrime-threat-device-cloning-source-americanbanker/

[5] Erik Brynjolfsson and Andrew McAfee, 90 *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York: W.W. Norton & Company, Kindle) 2016.

[6] Jurjen Jansen, Sander Veenstra, Renske Zuurveen, Wouter Stol. (2016) Guarding against online threats: why entrepreneurs take protective measures.35(5) *Behaviour & Information Technology*(370)

transaction. The rapid growth of credit card use on the Internet has made database security lapses more serious.

Credit card cloning or "skimming" is a new technique whereby someone creates a cloned version of the card by obtaining the credit card details, copying them onto a bogus card and begins using the credit card. This clone can be also be created by swiping the card on a device called a skimmer. The skimmer captures the data on the magnetic strip of the card. This data is further transferred for making a clone to commit the cyber crimes. Unless you're specifically looking for a skimming device, It is hard to notice anything out of the ordinary unless one is categorically searching for a skimming device.

SIM CLONING

SIM-cloning is a type of Cyber Crime in which the fraudsters duplicate the mobile SIM through specialised software which contains a SIM reader. The SIM reader copies all the information of a SIM card onto another. The fraud starts taking place when the victim receive calls or SMSs from the miscreants and fraudsters to retrieve the personal information stored in the victim's device. The cloned SIM card is then used to make private calls to the victim's bank and giving instructions or to reset the victim's bank account details using text message verification, and money from the victim's account is withdrawn.[7]

A similar strategy is used by a scammer for cloning a Facebook account. Facebook cloning is done to steal the personal photos and information of the victim. A cloner creates a duplicate account with the victim's stolen identity or takes authority over the victim's account. They proceed to friend request people on the targeted victim's friends list, many of whom accept the request with the belief that the person has simply made a new account. It is detrimental for the victim's social life. The victim may be represented to be involved in illegal activities and debauchery. The scammer uses the stolen identity to manipulate the victim's friends into sending money to him/ her.

[7] Mohini Bhardwaj, Amar Jeet Singh. (2011*) Automated Integrated Examination System: A Security Concern.* 20(3) *Information Security Journal: A Global Perspective* (158).

The recipients of the messages proceed to send money because they are under the impression that they are sending it to their friend or a trusted source. There have been cases where scammer leaves no stone unturned to make one believe that they need the money urgently and there is no time for them to receive or make a confirmation call regarding this.[8]

Cloning is not a new wonder, but the ease with which it is now possible to do has alarmed the police and the banking system. The law enforcement agencies are battling a rising instance of the breach without being able to do much beyond asking people not to share their banking details such as ATM PINs and OTPs. However, cloning, though, doesn't require you to share your details willingly. A cheap chip-like device can easily skim the customer data stored on the magnetic strip of your card when it's swiped, transmit it in a readable format to a laptop, from where it can be retrieved and copied on to another card, the clone, albeit an evil one which can do transactions without your permission just as easily as your own card. [9]

A recent government action announced ban on cloned 59 apps which were engaged in activities which is prejudicial to sovereignty and integrity of India. The government invoked it's power under section 69A of the Information Technology Act in view of the emergent nature of threats and decided to block the cloned apps.

Clone phishing is a **phishing attack** where the hacker duplicates a legitimate email that is sent from an authentic organization. The hacker alters the email by substituting or adding a link that redirects to a malicious and fake website. In furtherance to it, the email is sent out to a large number of email receivers and the hacker watches out for the victims who clicks it. When a victim successfully falls for the cloned email, the hacker forwards the same forged email to the contacts from the victim's inbox for extorting money from them.

[8] https://thelogicalindian.com/story-feed/awareness/beware-the-modern-day-forgery-called-sim-cloning-can-leave-you-bankrupt/

[9] https://www.dnaindia.com/mumbai/report-no-need-to-phish-for-this-clone-2592391

An organization can only be fully protected if its employees are well aware of the harmful cyber attacks. The internet users should remain safe and less vulnerable and more proactive enough to combat emerging cyber attacks. One can protect himself from the perils of phishing attacks by adopting the security measures. A very steep percentage of cloned and phished websites could be seen from October 2019 to March 2020. This shows a clear need for introducing high level security system like finger print and retina reading.[10]

It is possible to make exact reproductions of any person's voice by the voice cloning technologies. This is possibly done with another artificial technology technique by which the cybercriminals are able to formulate a perfect voice clone in a spur of a second. This is done by the process of text-to –speech –synthesis under this technology, perfection can be achieved because everything starting from the accent to the speed of the speech can be optimally copied. Under the **Voice Biometric Spoofing,** the criminals use recorded voice attacks, computer altered voice and synthetic voice cloning to fool the biometric systems which is a reliable measure for biometric security. Another evil i.e. the **Phishing Scam done by voice cloning** enables to exploit the victim by making him believe that they are talking to someone they trust. Recently, a UK-based CEO was tricked into transferring more than $240,000 based on a phone call that he believed was from his boss. The Evil effects have crossed all the limitations and have seen to influence and create fake evidence to trick the judiciary. While checks exist to validate the audio and the video evidences presented in the court but such scams surely influence the testimony. Deep fakes are a form of video manipulation where one can change the people present by feeding various images of a specific person they want. Furthermore, one can also change the voice and words the person in the video says by simply submitting series of voice recordings of the new person lasting about one or two minutes long. In 2018, a new app called FakeApp was

[10] **".com"** https://www.organiser.org/Encyc/2020/7/27/Government-of-India-bans-47-Chinese-clone-Apps.html

released, allowing the public to easily access this technology to create videos. This app was also used to create the Buzzfeed video of former President Barack Obama.[11]

It is high time that debit and credit card cloning should be administered by a separate law. Recently, it has been noted in India that such matters are not taken up as a separate issue. Rather, debit and credit card frauds are are only merged with the general law of information technology laws. It should not be ignored that this problem has emerged on a global level requiring a quick immediate concern. *India has done a good job by enacting the IT Act, 2000 yet it failed to keep it updated. For instance, we need express provisions and specified procedures to deal with issues like trojans, backdoors, viruses and worms, sniffers, SQL injections, buffer overflows etc. These issues cannot be left on traditional penal law of India (IPC). Even issues like cyber war against India or cyber terrorism against India have not been incorporated into the IT Act, 2000 yet.*

Aadhaar Biometrics

A fingerprint once impersonated remains with the impersonator forever and never changes. This results in a lot of damage.by the hacker to the property of the victim. of Biometric data, unlike passwords, can never be changed and there is not much the victim will be able to do about it. By cloning the fingerprints, the hackers can very easily gain access to the victim's life. The process of picking up fingerprints is very easy and simple. They can be picked up from objects and masses. Fingerprints can also be skimmed via malicious biometric devices. Fingerprint clones can also be made using dental moulds and dough. According to a research at the Department of Computer Science and Engineering at Michigan State University in the US, fingerprints can be replicated in less than $500 with conductive ink fed through a normal inkjet printer, in a procedure that takes less than 15 minutes. [12]

[11] *Silverman, Craig (April 2018). "How To Spot A Deepfake Like The Barack Obama–Jordan Peele Video". Buzzfeed.*

[12] *Aadhaar Now World's Largest Biometric Database: 5 Facts from UIDAI CEO's Presentation in Supreme Court You Must Know*, The Financial Express, 2018.

International Journal of Research in Social Sciences
Volume 9, Issue 5 (May 2019)
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Other Methods Used For Online Fraud:

Creating fraudulent websites, e-commerce platforms, social media accounts and emails claiming to sell and deliver medical products and the victims are asked to pay for the same via online bank transfer. In **Telephonic Frauds,** the fraudsters have been recently seen pretending to be relatives of a Coronavirus infected patient who has run out of money, thus asking the victims to pay online for the purchase of medicine. In recent **Phishing cases**, a pattern of sending fraudulent emails has been observed where some informative links regarding Coronavirus are sent to the victim and they are asked to click on it. This leads to instant loss of a lot of victim's money. In **Smishing**, a fraudulent SMS message on the phones with a link asking them to click on it. On clicking and visiting the fraudulent website, there is a possibility of malicious content getting downloaded on the phone. This eventually helps fraudsters to capture data from the victim's phone. Another frivolous tool is **Vishing,** where the victim receives a call from a bank asking for bank account details and other sensitive data such as passwords. The calls are made by fraudsters posing as bank officials.

Cloning of debit and credit cards is a process of copying card details using technology or software and then transferring it to another card. The devices used to copy such card information are also called skimmers. Hence cloning is also referred to as **Skimming.** Wrongful loss or wrongful gain through such activities could be prosecuted under IPC provisions (**S.463 to S.471 IPC,** as applicable).[13]Additions to the IT Act in 2008 protect against **identity theft (S.66C) [14]or cheating by impersonating online (S.66D).[15]**

[13] Sections 463 to 471 Indian Penal Code, 1860
[14] Section 66 C, Information Technology Act, Information Technology Act, 2000
[15] Section 66 D , Imformation Technology Act, 2000

International Journal of Research in Social Sciences
Volume 9, Issue 5 (May 2019)
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CONCLUSION

There is a huge shift from paper-based to electronic operations which have raised concerns regarding the recognition, authenticity and enforceability of specific forms of information handling documents and signatures. Influential AI applications are being used in machine learning to build algorithms from data and perform activities like the human brain does. Nowadays, there are powerful computers to do it fast and cheap. These powerful AI applications have been successfully and sufficiently used for the benefit of society. Unfortunately, the very same powerful AI applications could be used by criminals. The future will see even more powerful AI applications - their use for good or evil will depend on our ability to take preventative measures well in time.