IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 7 (July. 2018), ||V (VI) || 38-46

A Study of Crimes on Cyberspace

S.Arunpandian[1], S.S.Dhenakaran[2]
[1](Ph.D. Research Scholar, Computer Science, Alagappa University, India)
[2](Professor, Computer Science, Alagappa University, India)
Corresponding Author: S.Arunpandian[1]

Abstract: In spite of more advantages in information security, cybercrime has increased proportionately. Cybercrime is an illegal activity where a computer is used as a tool or target or both. Perpetrator takes any one of these activities for obtaining secured information from other systems. Ethical applications are available in the cyberspace like face book, twitter, and instant message etc. Devices are connected together in cyberspace to converse and share information using TCP/IP protocols. When such a way communication happens, perpetrator with current technology is prying secured information of others. To overcome the problems, nowadays biometric principles are used to secure information. Even though the approach of securing information by biometric is thought complicated, information are hacked without the knowledge of authorized person. This paper illustrates an overview of cybercrime; attacks of cybercrime in biometric and solutions to secure data from the cybercrime.

Keywords - Cybercrime, Authentication, Attacks, perpetrator, cloning, PUF

Date of Submission: 12-07-2018 Date of acceptance: 28-07-2018

I. INTRODUCTION

The first computer security law was legislated by Hessa, at German State that was named as "Data Protection Act" in the year of 1970 against cybercrimes. The Success of Data Protection Act was motivated to enact various security laws needed for e-commerce, e-governance and e-banking to avoid the cybercrime activities. In 2000, parliament of India passed Security Law as Information Technology Act on 17th October [11]. The cyber security finds vulnerability actions, which have been done by the perpetrator. Different kinds of perpetrator come under the cyber crime activities viz,

i) Black Hat
ii) White Hat
iii) Gray Hat

1. Black Hat Perpetrator

Black hat refers to a hacker who breaks into a computer system or network with malicious intent. A black hat hacker may exploit security vulnerabilities for monetary gain; to steal or destroy private data; or to alter, disrupt or shut down websites and networks. The black hat hacker may also sell these exploits to other criminal organizations.

2. White Hat Perpetrator

White hat perpetrator is the opposite of the black hat hackers. They are "Ethical Hackers" experts in compromising computer security system who use their abilities for good, ethical and legal purpose rather than bad, unethical and criminal purpose. Many white hackers are employed to test organization computer security systems. The organization authorizes the white hat hackers to attempt to compromise their systems. The White hat hackers report back to the organization and inform how they gained access allowing the organization to improve their defense. This is known as **"Penetrating Test"** and organization pay **"Bounties"** or award prizes for revealing such discovered vulnerabilities.

3. Gray Hat Perpetrator

Gray hat perpetrators fall somewhere between a block hat and white hat but they may technically consign crimes and arguably immoral things. Black hat hackers would negotiate a computer system without consent. White hat hackers would ask permission before testing the system security and alert the organization after compromising it. Gray hat hackers might attempt to compromise a system without permission. If a gray hat hacker discovers a security flaw in a piece of software or on a website, they may

disclose the flaw publically instead of privately disclosing the flaw to the organization and giving them time to fix it.

The figure below shows total number cybercrime attacks made by the perpetrators (blackhat & grayhat hackers) against the Institution, Organization and Individual in India. To do this type of illegal activities, perpetrator spreads the malware through Email, Messages and Phishing attacks using internet. Malware may have virus, worms, spyware, root kit, ransom ware and Trojan horse. Among these malware, Trojan horse is a hidden piece of code that monitors the keystroke of keyboard. Perpetrator takes the captured data, which is utilized as an input to obtain the secret information.

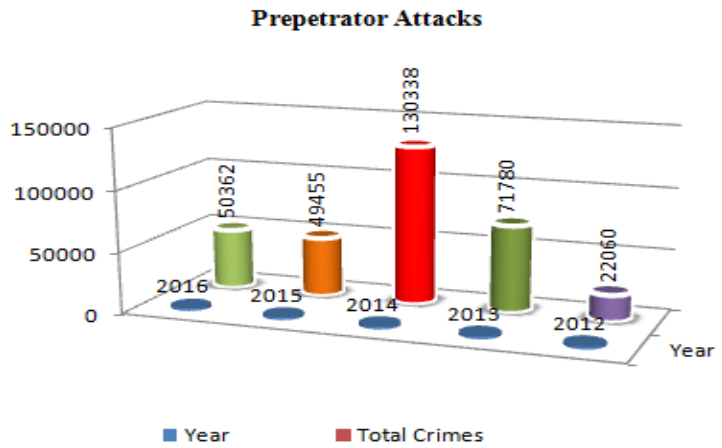

Figure.1. Number of attacks in India

Even though internet security and antivirus applications are presented to protect the crucial hit, these attacks would happen easily with the unadventurous method like brute force and dictionary attacks. To avoid hacking biometric principles are used. In biometric system, information like face, Irish, fingerprint are recorded at the enrollment process and stored as template. This template helps to identify the right person. The conventional method of using password and patterns like a mobile number, Nicknames, Data of Birth are traced by perpetrators whereas biometric concept eliminates the conventional methods.

II. TYPES OF CYBERCRIME ATTACKS

A critical computer program has taken as weapon by the cyber criminals to attack systems, which might not be properly updated and protected. These programs passed as attacks to the internet users by the cyber criminals selecting an organization or departments to obtain volume of money illegally. The Computer Emergency Response Team (CERT) has statistical reports of cybercrime attacks.

1. Cyber Crimes against Persons

The Cybercriminal hides behind counterfeit promotions, giveaways, offers etc. Criminals make security illusions to give up personal information of the internet users [1]. Cybercriminal speaks as a legitimate authority persons of the banks with account holder to access the personal information. Especially, cyber criminals have been using internet fraud auction to abuse credit card information of the individual.

Figure.2. Cybercrime Attacks against individual

1.1 Hacking**:** Entire data and computer programs have been hacked over the computer using unauthorized access or control. Perpetrator destroys these data without any evidence and follows the usual methods such as mobile network, telecommunication.
1.2 Cracking: Among the cybercrime, cracking is a gravest crime in cyberspace until now. Cracking makes dreadful feeling that an unfamiliar person has broken computer systems not including the consent or knowledge.
1.3 Email spoofing: A sender sends message in email but recipient receives message from bogus address instead of original. Here, the spoofed mail has misrepresented its origin.
1.4 SMS Spoofing: A person receiving unwanted message in mobile phone helps to steal the identity of victim by offenders. SMS spoofing considers as very serious crime.
1.5 Cyber stalking: Physical threat creates much panic using computer technology like text message, websites, email etc.
1.6 Defamation**:** To degrade the dignity of a person, an offender hacks the mail and resends it with vulnerable language from unknown mail account.

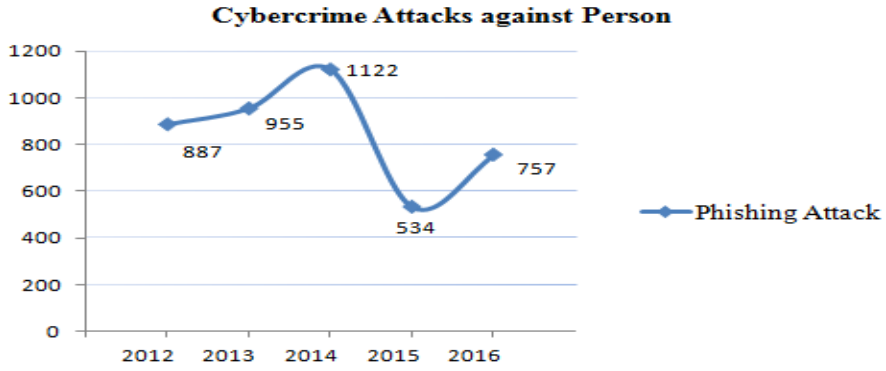

Figure.3. Statistics of Cybercrime Attacks against Person

2. Cyber Crime against Property

Typically, Malware software involves infiltration in computers for personal, website and email chats. These attacks help cyber criminal to destroy computer data or steal the information from internet users and it denies necessary information of the victim, who has already assault of this attack. Here, cybercriminal accesses internet bandwidth (Router) of genuine person without the permission [2]. Such kind of steal also treated as a cybercrime in cyberspace. Following activities are against the person property.

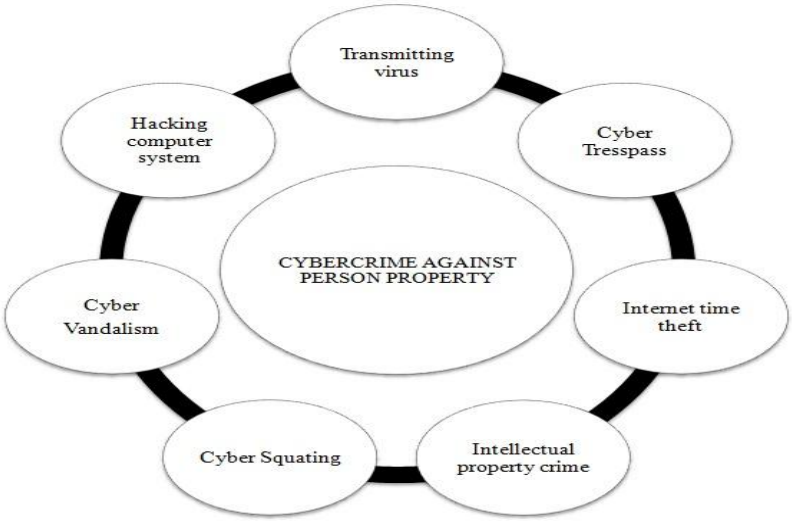

Figure.4. Cybercrime Attacks against Property

2.1 Transmitting virus: Crucial programs consider as virus. This program attaches themselves into the computer, which can spread into another computer on a network. Computer virus removes the computer data by either altering or deleting the data.

2.2 Cyber Trespass: A person has attained rights for computer but it used by another one without the knowledge through wireless internet connection.
2.3 Hacking Computer System: Unauthorized person has been accessing or controlling the famous blogging platform, twitter and Insta-gram over the computer by hacktivism attacks. Due to this activity, there will be loss of computer data.
2.4 Cyber Vandalism: Computer data are stored in system, which is obliterating deliberately when a network service is disturbed.
2.5 Cyber squatting: Two or more persons claim similar domain names to their websites such names are www.flip**k**art.com or www. Flip**c**art.com

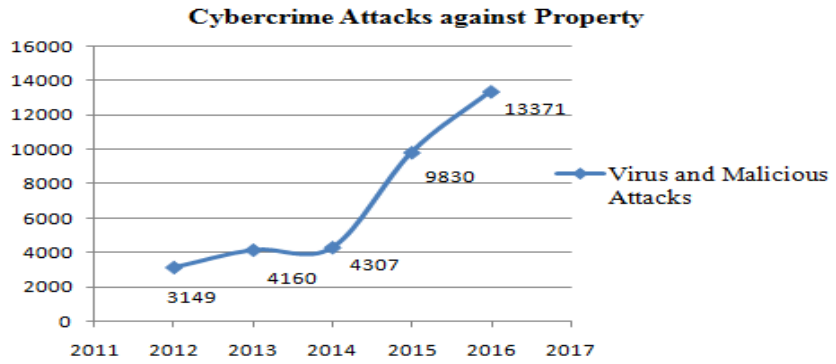

Figure.5. Statistics of Cybercrime Attacks against Property

3. Cyber Crime against Government

Cybercriminal not only attacks private institution but also assault the government organization. A government agency has one or more secured databases based on the departments like bank, transport etc. These databases are hacked with an objective to abuse the confidential information and term "cyber-terrorism" in this context frequently [1]. FBI defines the term as "the premeditate, politically induced assault against computer data, systems, and programs which results in violence non-combat goal by cybercrime agents".

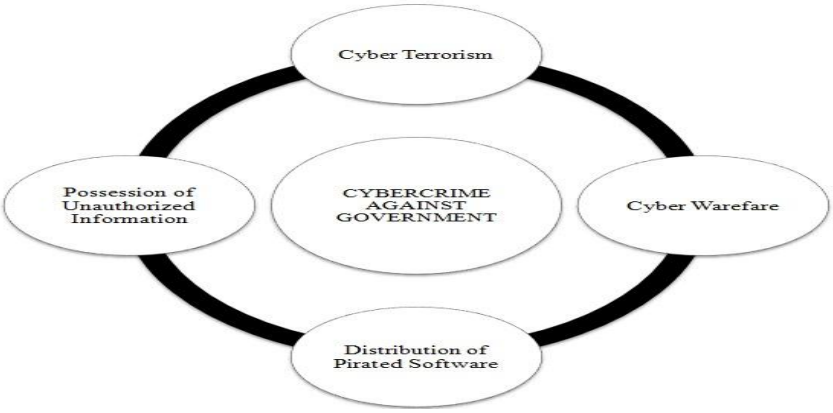

Fig.6. Cybercrime Attacks against Government

3.1 Cyber Terrorism: Cyber terrorism provides the major attacks in the domestic and global concerns. Commonly these assaults happen on internet by the DDS (Distributed Denial of Services), emails and websites on public computer networks such kind of incidents endanger to the integrity of the nation.
3.2 Cyber Warfare: To conduct the harm and spy on the network, this is induced by political. It is a structure of information warfare and sometimes shown as analogous to traditional warfare even though it may controversial.
3.3 Distribution of pirated Software: Cyber criminals have been spreading the pirated software to obliterate the official files and computer data against government sectors.
3.4 Possession of unauthorized information: Terrorist could access easily any information through the internet and it may have possessed of the religious, ideological, religious object.

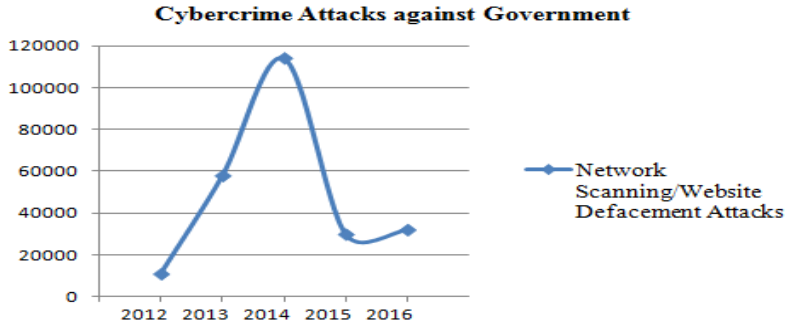

Figure.7. Statistics of Cybercrime Attacks against Government

4. Cybercrime against Society

Very basic activity is a cyber attack in society. Internet users aren't aware of this crime and hence users give the sensitive information for a crazy intention which is mislead to loss their income. Some of the offense is describe below,

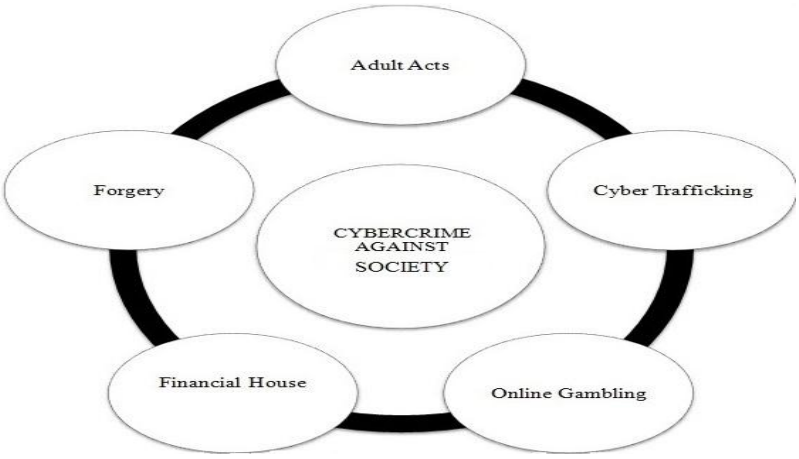

Figure.8. Cybercrime Attacks against Society

4.1 Online Gambling: In cyberspace, most lucrative business has done by cheating and online fraud. Some of the crimes partially published such as contractual crimes, offering jobs and credit card crimes etc.

4.2 Financial House: Networking sites, mobile networking has created for users. Here, perpetrator tries to assault common networking applications by sending spurious mails or social media messages using internet. Example: obtain the password of a credit card without knowledge.

4.3 Cyber trafficking**:** Gravest crime in the cyberspace, which effects on huge amount of persons in drugs, arms weapon and human being etc.

4.4 Forgery: More number of people desires to do the online business transaction for their earning purpose but they are deceived by sending a threatening email in present situation.

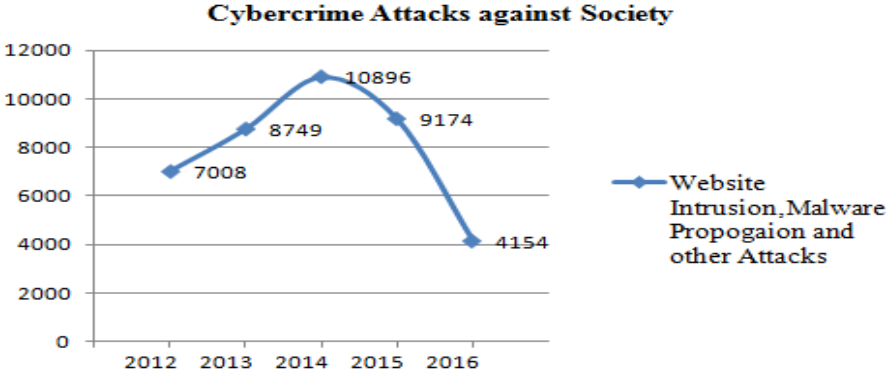

Figure.9. Statistics of Cybercrime Attacks against Society

5. Mobile Phones

Mobile devices plays an important role in day-to-day life for all types of human entertainment. Utilizing devices like Smartphone, tablet PCs, workstations, and other convenient devices make secret information expanding. Biometric security is applied in mobile devices for authentication purpose rather than passwords and patterns. Mobile users are not sign out properly from the applications which makes harm to retrieve the data easily. There are lot cases of coordinating biometric innovation by means of mobile applications improvement that incorporates mobile voting, performing on the online exchanges, managing an account and so on. Individual authentication provides more security other than by using biometric technology, which works on the physiological or behavioral characteristics [11]. The following figure has elucidated Smartphone attacks and showing the rate of increase in phone attacks.

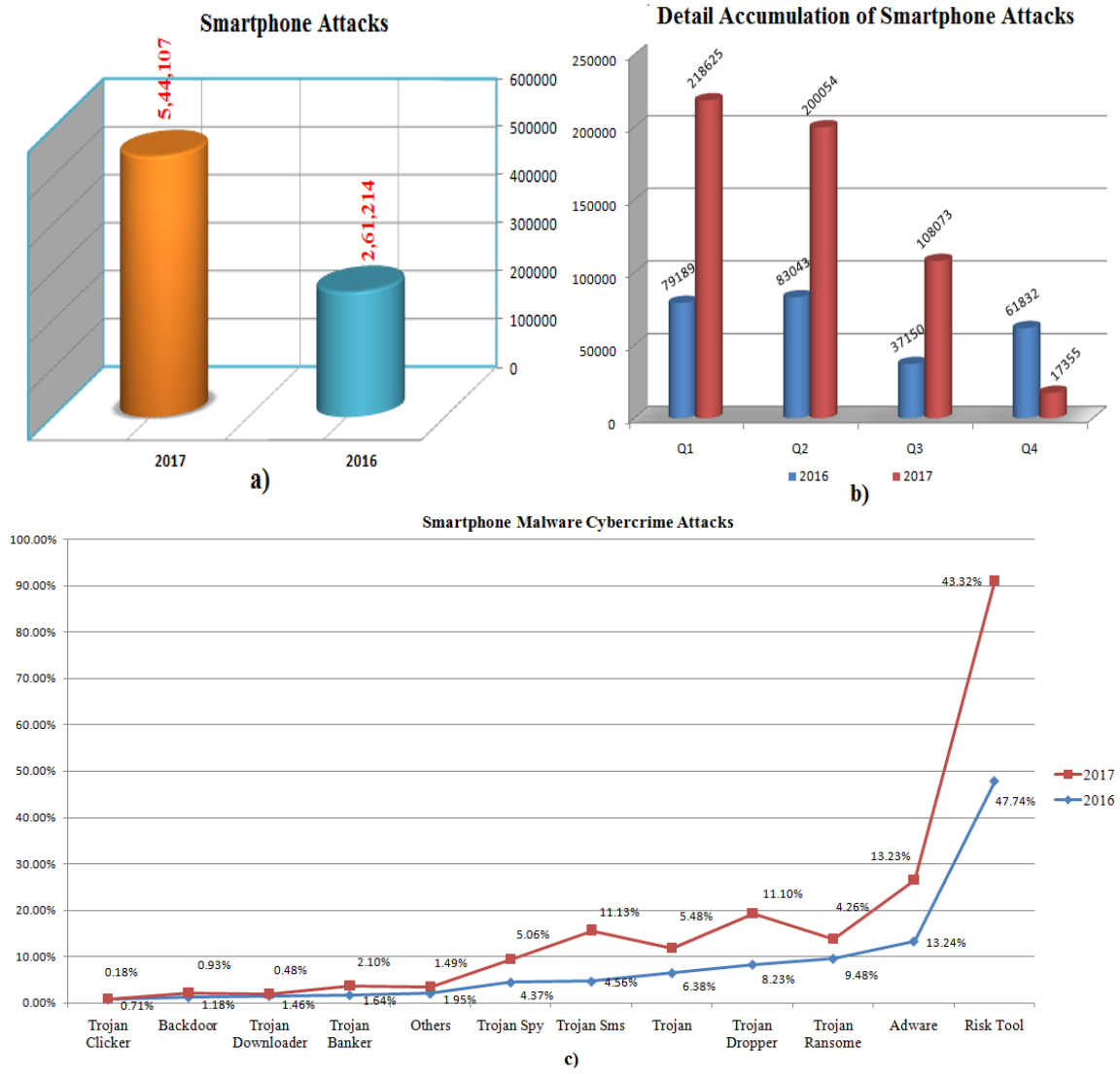

Figure.10. Smartphone Cybercrimes

Biometric replace entering passwords and patterns to unlock mobile phones by conventional methods. Biometric has included within mobile phones to enhance the security of the users like fingerprint, face, signature, voice, Irish recognitions. These modalities help to identify the authenticated person to access device. Various mobile companies have implemented biometric feature for mobile devices. Even if there is number of provisions in biometric mobile device perpetrator hacks the data from mobile using "virtualization threat". This threat makes clone copy of the biometric data and latterly perpetrator has taken full control to access device using these data without the user even knowing.

III. CYBERCRIMES IN BIOMETRIC

Biometric is the science and pattern reorganization technology of measuring and analyzing biological data, which may be either physical or behavioral of the particular person. Data collected at the enrollment process has four basic modules such as sensor module, feature extractor, matcher module and decision module. These four modules make useful information from raw data to do frequent activities for future enhancement and data has utilized to recognize the authorized one. In conventional methods, people had to remember the passwords, tokens, cards for their authentication purpose and they assign these codes as date of birth, names, familiar words etc. Perpetrator obtains passwords using dictionary and brute force attacks to get sensitive information without the knowledge of authorized person whereas biometric provides more security for authentication and need the presence of particular authorized person to access the confidential information. Even though biometric data has protected, Cybercriminal also attacks happen on biometric systems through morphing, 3d techniques.

3.1 Attacks on Biometric

In biometric system, attacks have categorized as direct and indirect. Specifically, direct attack does not require the system functionality. The indirect attack needs inter activity of the system [13].

Attack at the sensor [Type one]: Sensor module is vulnerable to type one attack. Imposter presents bogus biometric traits such as finger print or facial images to bypass the reorganization systems. The sensors do not distinguish synthetic fingerprints, facial images.

3.1.2 Replay Attack [Type two]: Biometric raw data have acquired by the sensors. These data pass through the communication channel to feature extractor module for preprocessing it. Meantime imposter steals the biometric data, stored it somewhere else to bypass the sensors.

3.1.3 Attack on feature extractor module [Type three]: At the point, when the sensor acquires unprocessed biometric information, it sends the raw information to feature extractor module. A fraud pressurize the feature extractor module to create the element esteems picked by the imposters as opposed to delivering the element esteems produced from the first information got from the sensor.

3.1.4 Attack on feature extractor and matcher [Type four]: Perpetrators obstruct the communication channel between the feature extractor and matcher modules and take the element estimations of honest to goodness client. These values can be replayed to the matcher later on.

3.1.5 Attack on matcher module [Type five]: Imposter selects high matching score by generating values to bypass the biometric authentication system regardless of the values obtained from the input feature set.

3.1.6 Database Attack [Type six]: Imposter is modifying or removing existing templates of the protected database by adding new templates. Database templates have a digital mechanism for protect the data using the stenography and water-marking etc. imposter has found more knowledge about the system functionality to make the successful attacks on security provided databases.

3.1.7 Attack on system database and the matcher [Type seven]: Attack can be made possible just when template is transmitting through communication channel between system database and matcher module. It happens when imposter alters or alters the substance of the transmitted templates. An imposter seize the channel to take, replace or modify biometric format.

3.1.8 Accept and Reject of Matcher Module [Type eight]: Matcher module produce the results, these results may override by the imposters. When the match score passes through the communication channel between the matcher module and application device, imposter may tamper it and matcher module cannot take the original decision.

IV. DATA PROTECTION AGAINST CLONING

Perpetrator had been cloning the confidential data of users using skimmer method, which was the earliest hacking technique. In this technique perpetrator captured the passwords like secret key, other information's, when the skimmer inserted into the card readers of the ATM machines [4]. Data breaches are threatening to all the users because a particular sensitive data have been integrating with other applications, which have not provided the strong algorithm for the data. In this manner, several applications have lacked in security level to safe the information from hackers. To avoid these cloning techniques, an innovative method called Physical Unclonable Function (PUF). PUF is a semiconductor device and physical entity, which has

embodied with physical structure of integrated circuit and widely used in cryptography for higher security applications [9]. PUF has a unique physical microstructure and categorized into two types [16],

1. Weak PUF

It produces an inadequate number of Challenge response pairs (**CRP**) and can be completely read out in a very tiny time once an opponent has full physical admittance to it. A Weak PUF can be defined as follows:

- Impractical to be (cloned) physically.
- Amount of CRPs is bounded and linear or polynomially reliant on the number of confront bits

2. Strong PUF

A Strong PUF needs to demonstrate its security under such a solid assault show. Therefore, it can characterize a strong PUF as per the accompanying security properties:

- Impossible to be cloned physically.
- Flexible to display building assaults by giving a polynomial number of picked CRPs with the end goal that a foe can't foresee the reaction of a PUF to a haphazardly chose unused test

Physical Unclonable Function consists of three measurement techniques such as randomness, uniqueness, bit error rate. These techniques utilized in real time PUF applications. PUF has been selecting the operation randomly which is an impossible way to clone or duplicate the structure rather than data stored in non-volatile memory. The PUF will discover more extensive use in smart energy meters, medical devices, and smart surveillance controlling temperature, CCTV, humidity and even smart automobiles. In India the innovation would discover ordinary application in counteracting interruptions in keen co-ordinations systems etc.

V. CONCLUSION

Innovations have been introduced by technologists for protecting information using new algorithms in every technological era. Similarly, perpetrators use different strategies to break the innovative approach for getting the money or sensitive information. Even the biometric security has applied for authentication in various applications; perpetrators thieve the information's using another tactics such as black box, morphing, skimmer techniques. These techniques are enough to clone data easily. To avoid data breaches, Physical Unclonable Function have used to whcih did not allow perpetrator for making illegal activities which is implemented in integrated circuits and used in high security requirements.

REFERENCES

[1]. Available at: https://www.legalindia.com/cyber-crimes- and-the law/
[2]. Available at: https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/cyber-terrorism.html
[3]. Gunjan, Vinit Kumar, Amit Kumar, and Sharda Avdhanam. "A survey of cyber crime in India." Advanced Computing Technologies International Conference on. IEEE, 2013.
[4]. Available at: https://www.bayometric.com/biometrics-future-iot-security/
[5]. Available at: https://www.bbvaopenmind.com/en/iot-implementation-and-challenges/
[6]. Available at: https://www.kaspersky.com/blog/4-ways-to-hack-atm/13126/
[7]. Kour, Jaspreet, M. Hanmandlu, and A. Q. Ansari. "Biometrics in cyber Security." Defence Science Journal 66.6 (2016): 600
[8]. Hwang, Kyu-Man, et al. "Nano-electromechanical Switch Based on a Physical Unclonable Function for Highly Robust and Stable Performance in Harsh Environments." *ACS nano*(2017).
[9]. Herder, Charles, et al. "Physical unclonable functions and applications: A tutorial." Proceedings of the IEEE 102.8 (2014): 1126-1141.
[10]. Available at: http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/IoT-implementation-in-mind-Five-critical-factors-you- must-conside
[11]. Available at: http://www.m2sys.com/blog/mobile-biometrics-2/5-recent-trends-in-biometric-technology/
[12]. Available at: https://www.imore.com/talk-mobile/future-authentication-biometrics-multi-factor-and-co-dependency-talk-mobile
[13]. [13] Uludag, Umut, and Anil K. Jain. "Attacks on biometric systems: a case study in fingerprints." Security, Steganography, and Watermarking of Multimedia Contents VI. Vol. 5306. International Society for Optics and Photonics, 2004
[14]. [14] Available at: https://www.softwaresuggest.com/blog/iot-going-play-major-role-biometric-systems/
[15]. [15] Available at : http://www.business-standard.com/article/news-cm/rbi-has-issued-cyber-security-framework-in-banks-117080200207_1.html

[16]. [16] Gao, Yansong, et al. "Emerging physical unclonable functions with nanotechnology." *IEEE access* 4 (2016): 61-80.

AUTHORS PROFILE

S.Arunpandian, received her M.Phil degree in Alagappa University, Tamil Nadu. Now he is pursuing her Ph.D (Computer Science) research in the same university. The field of his research is Biometric Security in cryptography.

S.S.Dhenakaran, a faculty member is working in the Department of Computer Science, Alagappa University, Tamil Nadu, India. He has acquired a doctoral degree in Computer Science and Engineering during 2008. Completed post graduation in mathematics during 1984, PG degree in computing during 2003. To his credit, he has more than 95 articles in international journal and conference. His field of research is Data Security using Cryptography. His familiar research fields are Optimization Techniques, Algorithms and Data mining.

S.Arunpandian "A Study Of Crimes On Cyberspace ." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 7, 2018, pp. 38-46