International Journal for Electronic Crime Investigation

(IJECI)

VOL.1

Issue: 1

October-December 2017

Digital Forensics Research and Service Center
Email ID: IJECI@lgu.edu.pk

Lahore Garrison University,
Lahore, Pakistan.

LGU International Journal for Electronic Crime Investigation

SCOPE OF THE JOURNAL

The IJECI is an innovative forum for researchers, scientists and engineers in all domains of Digital Forensics and Cyber Security to publish high quality, refereed papers. The journal offers articles, survey and review from experts in the field, enhancing insight and understanding of the current trends and state of the art modern technology. Coverage of the journal includes algorithm and computational complexity, distributed and grid computing, computer architecture and high performance, data communication and networks, pattern recognition and image processing, artificial intelligence, cloud computing, VHDL along with emerging domains like Digital Forensics , Cyber security and Offensive Security . Subjective regime is not limited to aforementioned areas; Journal policy is to welcome emerging research trends in the general domain of Digital Forensics and Cyber security.

SUBMISSION OF ARTICLES

We invite articles with high quality research for publication in all areas of engineering, science and technology. All the manuscripts submitted for publication are first peer reviewed to make sure they are original, relevant and readable. Manuscripts should be submitted via email only.

To submit manuscripts by email with attach file is strongly encouraged, provided that the text, tables, and figures are included in a single Microsoft Word/Pdf file. Submission guidelines along with official format is available on the following link; www.research.lgu.edu.pk

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence,kindly contact at this address:
IJECI, Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
Email: IJECI@lgu.edu.pk

LGU International Journal for Electronic Crime Investigation

CONTENTS

LGU International Journal for Electronic Crime Investigation

REVIEWERS COMMITTEE

Malik *et al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 1 issue 1 Dec 2017

Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed

[1] Dr Aftab Ahmad Malik Ph.D (University of Kent England) M.Phill, MSc, L.L.B; Professor Department of Computer Science, Lahore Garrison University (LGU) Lahore Pakistan
Email: dr.aftab.malik@yahoo.com
[2]Engr. Mujtaba Asad BS (EE),MS(Computer Science) MS (EE); Ph.D Scholar, Department of Electronics and Electrical Engineering, Shanghai Jiao Tong University, Shanghai Minhang Campus, Doram Building No 9, China;
Email: mujtaba.asad@live.com
[3]Waqar Azeem Lecturer, Department of Computer Science, LGU,Lahore Pakistan
Email: waqar.azeem@lgu.edu.pk

Abstract:

The purpose of this work is to assign codes to the fingerprints images stored in large databases / Data warehouses, the images require large amount of storage as compared to a numeric code. Moreover, when fingerprint images are compared to other fingerprint images, the process is more time consuming as compared to the numeric codes. It is proposed to keep up all fingerprint images in a separate database file along with their codes. This file may be a supplementary file with respect to Master database file. In addition to this, the codes of fingerprint images may be stored in Master Database/ Data warehouse for all records. The search queries can be processed using the numeric codes. In this manner, the Time Complexity and Space Complexity are reduced considerably. Whenever, any fingerprint image is received for searching its record, first its code is obtained by proposed algorithm and then this code is used to search the record from database/Data Warehouse making entire procedure faster and efficient.

Keywords: Forensic, Biometrics, Image processing, coding fingerprint images, criminal history, Numeric Codes, Database/Data Warehouse

1. Introduction

In criminal Information Systems, the particulars regarding physical appearance such as face prints, fingerprints, DNA code and Iris Code etc are of very important nature. In order to facilitate further discussion and background, following explanation is provided.

Digital Forensic is science related to retrieving and finding out the information found in digital devices related to crime or cybercrime. It helps to access information

available in mobiles, computers or any other storage media. This field is advancing and progressing rapidly. It also helps to uncover and interpret the information electronically. Its objectives are to process and store the information obtained from scene of offence or other sources for further analysis and use.

The Cloud Computing involves machines learning techniques and managed plate form and uses tools to build application with ease. It is called a subset of broad Network Forensic. The robustness and quality can be ensured with application of cloud computing. Cloud forensic plays a pivotal role in between Cloud Computing and digital cloud forensic.

The Elastic Bunch Graph Matching (EBGM) [9] algorithm is used in Computer Vision to recognize the objects of an image on a graph representation derived from other images. The Elastic Bunch Matching returns the similarity value, the positions of the nodes in image, which helps in creating an image graph. Gabor Filters [10] are used in image processing with Gaussian envelop function for texture analysis. The Gabor filters are extensively used in the situations where fingerprint matching and enhancement is processed. They are called band-pass filters and possess the following properties:

- frequency-selective
- orientation-selective

The Biometrics Technology is extensively and commonly used in forensic to analyse for measurement and examine the characteristics of humans like DNA, Irises, voices and face images. The related information can be converted into digital form, encrypted and stored in a database/data warehouse. This is thesis of this paper.

2. The applications of biometrics

There are mainly three categories in the field of biometrics:

- Commercial sector
- Government applications such as national ID card, driver's license, social security, welfare disbursement, border control, and passport control.
- Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

3. Review

There exist several techniques to analyse and synthesise the fingerprint images. The fingerprint images are analysed for quality; then sometimes may be improved. [1] Proposed & devised an efficient algorithm for Coding Person's Names in large Databases/ Data warehouses to enhance Processing speed, Efficiency and to reduce Storage Requirements. [1] Allocates numeric codes to Names (First name, Middle name, Last name) using three numeric characters for each, instead of 40 Alpha-Characters, which are normally reserved for one complete name.

A similar approach has been employed for facial image coding by first author of this paper [2] describes how to generate code for facial prints and to use them in databases and data warehouses to reduce Time and Space Complexity and to make the image processing more efficient. In this paper, the philosophy of [1] and [2] is applied to fingerprint images to reduce Time Complexity and Space Complexity. The images [2] also

clarify the points of measurements of distances in case of facial image processing figure 1; similar strategy can be applied to fingerprint at minutiae point as shown in Figure 1.

[3] Describes uses and procedures of OpenCV. It provides built in Library functions for real time image processing. The module imgproc provides basic and important image processing Techniques/Algorithms for filtering, image transformations and conversions.

Figure 1

Voila Jones Algorithm is discussed in [4], which identifies and detects various parts of the facial image, the eyes, nose and mouth using common characteristics of the face. [5] Claims that 99% accuracy in image processing can be achieved in front-pose face image.

Different patterns to code the fingerprints have been presented in [6] in order to use these codes in the software for storage and retrieval of criminal information. [7] Discusses the techniques for Software for Storage and Retrieval of Criminal Information for Police based on physical data.

There are several biometric systems designed to identify humans by matching the characteristics from the database or Data warehouse. The employee's roll call system is one such example; others in daily life are computer login and internet access. The ATM forensic applications such as used in Criminal Information system are elaborated and designed in [6] and [7]. The Face Recognition by Elastic Bunch Graph Matching has been discussed in [11]. A grid of points is launched as shown, then a bunch graph is constructed for recognition, it works with Instructions on getting FERET database. The purpose of FERET is to design automatic Face Recognition System. For Enhanced Security of Digital Images [13] and [14] have been used and developed by the second author of this paper.

4. Brief Analysis of Finger Prints

The relevant algorithms can translate the given image (facial image or fingerprint) into a digital code. The minutiae are important features in fingerprint used to make comparison between 2 images; it has Ridge ending and sudden end of ridge dividing it into two ridges. The following figure 2 shows the split of ridge in Figure 2(a), (b):

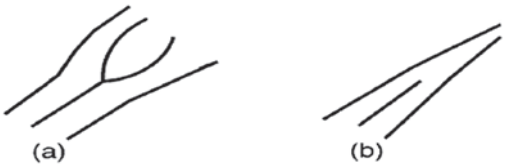


Figure 2

The Minutiae Points

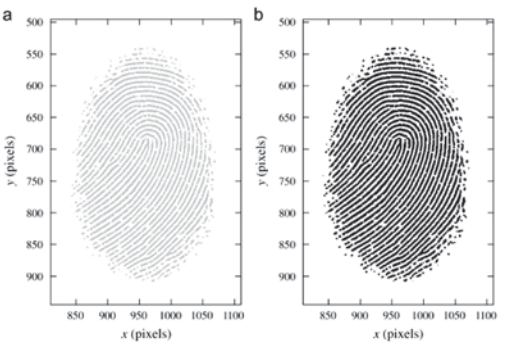


Figure 3a

To process the criminal information regarding storage and retrieval, Cloud Computing and digital forensic are of immense importance. Similarly, these two areas also apply to cyber–crime investigations.

In this paper, main focus will be on storage and retrieval of information based on fingerprints. The structure of fingerprints is unique. In fingerprint, there are spirals, whorls, parabolas, arches, ridges, tented arches, dots and dashes. All fingers have unique code. Therefore, fingerprints are used to retrieve human data from a Database or Data warehouse as unique key like Id-card Number or Employee Number.

5. Fingerprint Patters

The Fingerprint pattern recognition system is being extensively used in identity marching and access control. Most of the systems are designed to match fingerprints image with stored image of fingerprints for authentication using image processing algorithms. The design of the proposed system of the work of this paper depends on assigning fingerprints a unique code.

The usual patterns in fingerprints are whorls, loops and arches which are not sufficient for identification and coding. The important feature is ridge endings termed as “hooks” and “eyes” to determine the identity of a fingerprint. However, other features such as line shapes, pores and breaks plays an important role in shape of the fingerprint and hence the coding process. Following pattern indicate [16] minutiae image features (figure 3a and 3b):

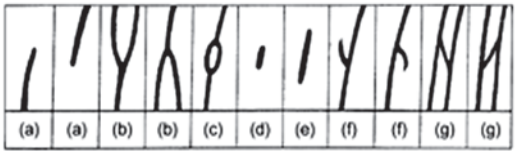


Figure 3b

A live-scan sensor is required in case of digital image processing of fingerprints. In the Automated Fingerprint Identification Systems (AFIS), such devices have been used. The optical and solid state is also commonly used [15] ,[18].

Fingerprint Shapes and Patterns:

The figures 4a and 4b show arches, loops, whorls and composites of fingerprints.

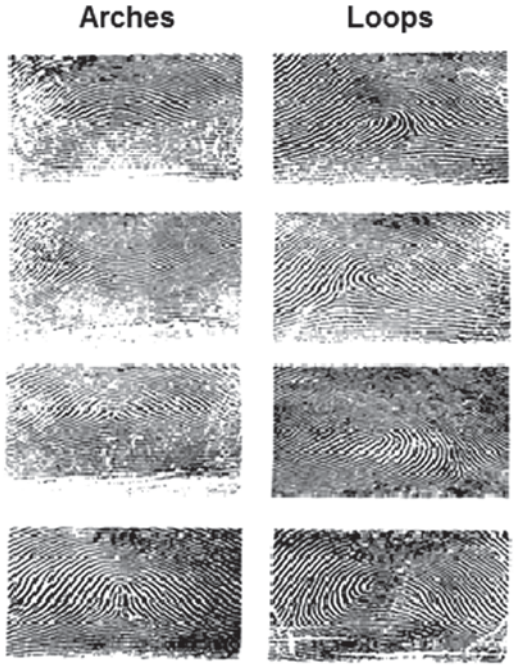
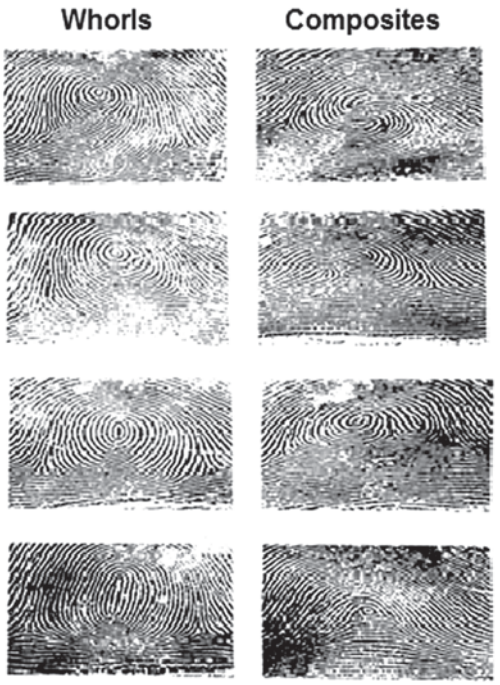


Figure 4a



Source: Sagem Morpho

Figure 4b

6. Assumptions

The assumptions for the proposed system are that only neat and visible images are considered. The damaged images are first repaired by image processing techniques before entry. Fake or severely damaged fingerprints are avoided.

Complete and well defined fingerprint images are used.

7 Biometric Requirements

The characteristics of biometric identifiers include Universality, Uniqueness, Permanence and Collectability.

The feature of collectability means that the characteristics can be measured quantitatively.

While, designing biometric system care must be taken regarding above characteristics, as well as, the verification system must be able to identify an individual by comparing the pre-stored characteristics and the one entered for verification.

8. Steps in Fingerprint coding Scheme

The fingerprint is the query point which can be taken directly from database, if already stored; otherwise it is entered through the scanner.

Step 1: Enrolment and identification of fingerprint

Step 2: Conversion of image into digital form

Step 3: Process of marking and extraction of unique minutiae points

Step 4: Saving minutiae information regarding location and direction

Step 6: Storing the criminal history, physical data, modus operandi and Personal or criminal information is stored along with fingerprint in Database.

Step 7: The match score between the query print and stored image is compared which must be high for same fingerprint low for different prints.

Step 8: Process of conversion of fingerprint image into a (numeric) / digital code and fingerprint image. There is also provision for the 14 Digit code returned by the Algorithm.

9. Graphical User Interface

The Graphic User Interface contains personal information about the person whose image is being processed such as First Name, Middle Names, Last name, gender, occupation, Date of Birth, face image.

10. Sequence of operation on fingerprint

The fingerprint image passes through the following operation upon entry:

- Resizing
- Lightening
- Smoothing
- Edge detection
- Binarisation
- Thinning
- Final code generation

2. Design:

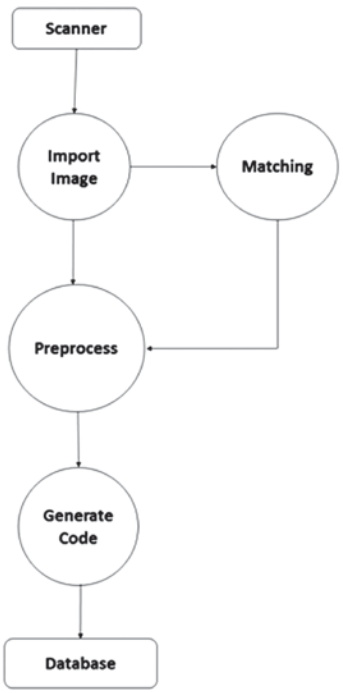


Figure 5

11. Calculation Methodology

Using direction vectors, the orientation image is calculated in the form of a matrix. Its vectors represent ridge orientation at every location. The gradient based approach is employed to determine the gradient, because the orientation vector is orthogonal to gradient.

The Fingerprint image is divided into square-blocks. This is how the gradient is calculated for every pixel. For every block, the orientation vector is computed leading towards averaging procedure using Sobel operator horizontally and vertically.

MATLAB provides bwmorph function to 'Thin" the image. The example of matrix so formed is shown in Figure 7.

Figure 6 shows the minutiae points

Figure 6

Example of Calculation Methodology

-1	0	+1
-2	0	+2
-1	0	+1

x filter

+1	+2	+1
0	0	0
-1	-2	-1

y filter

Figure 7

On the basis of proposed design diagram, the DFD is given in figure 8

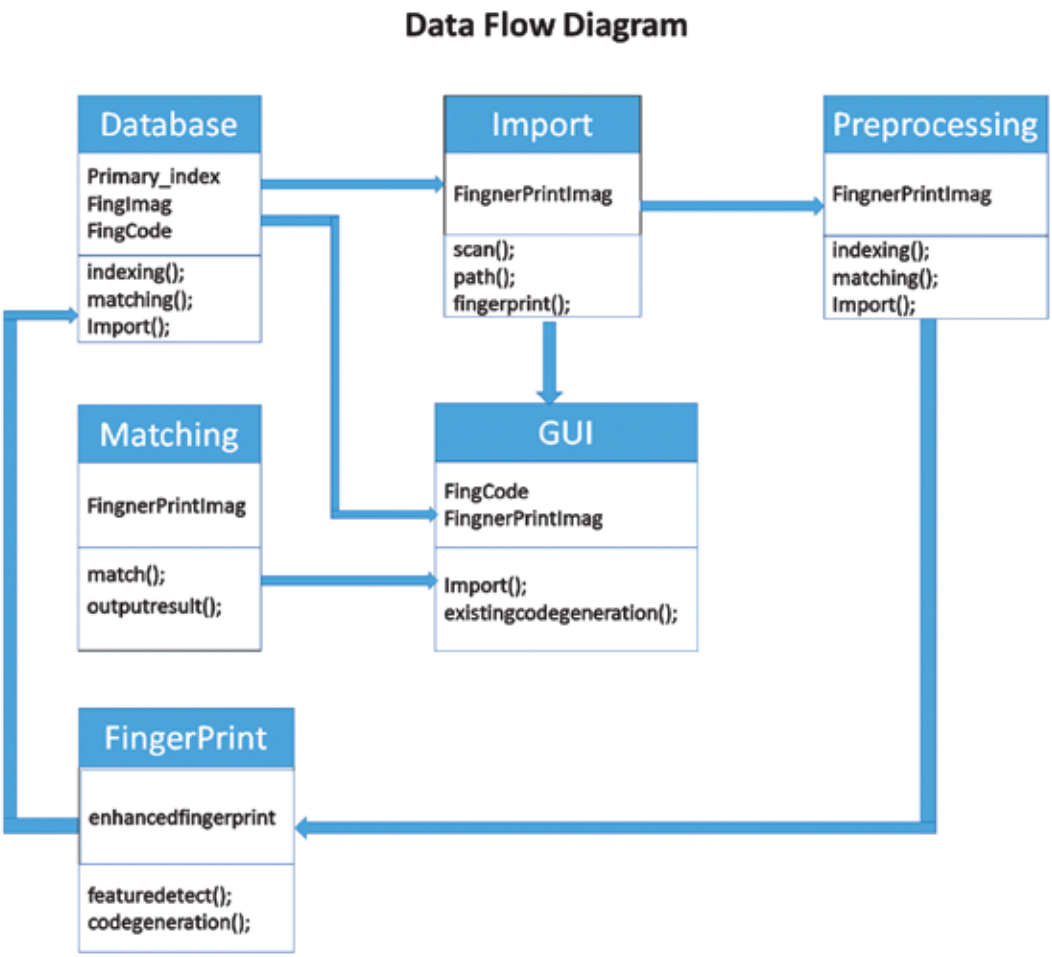


Figure 8

Use cases for Fingerprint images

Use case 1:

Enter or Import fingerprint Image from database.

Description:

- A prompt to either Enter image-file from a file path to import image from existing database.

Use case 2:

- Extracting minutia, ridge ending, bifurcation and all other features in order to produce initial pattern and generate Code
- pattern and generate Code

Use case 3: Conversion into numeric code

Description:

- Apply Thinning on binarised output.
- Extract Fingerprint features and an initial code block
- Secure code block

Use case 4:

Fingerprint code Matching

Description:

- Match the converted code attached to the images in Database.
- Extracting minutia and other features from fingerprint images.

Screenshort of Fingerprint Code Generation

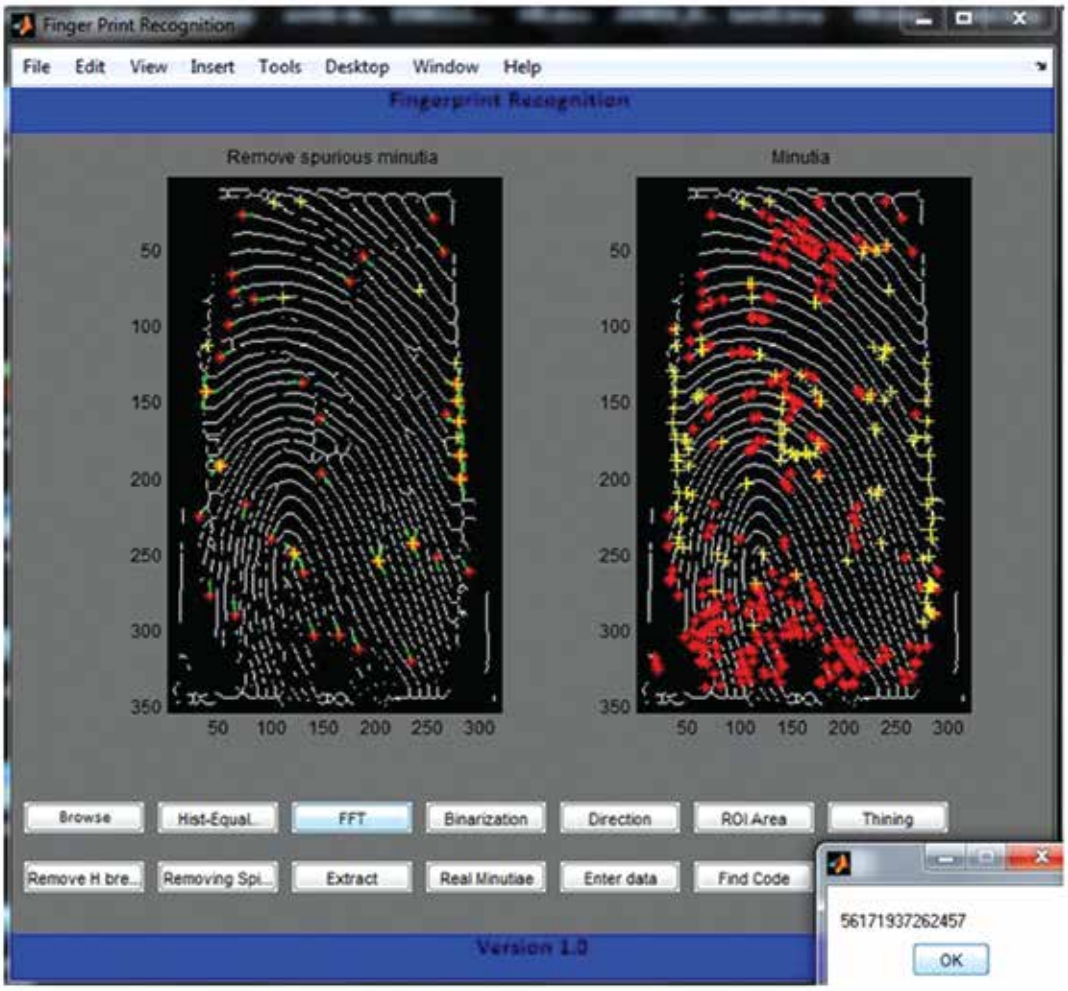


Figure 9

12. Conclusion

The searching the database / Data warehouse using a numeric unique key is faster as compared to searching by comparing images with images. In case of searching the large data base by entering image consumes excessively more time because the comparison of stored image with the entered image involves pixel to pixel and region to region comparison for which the Time Complexity and Space Complexity is very high. In case the database is sorted the relevant record is directly accessed by numeric key. In case the images are stored in an auxiliary file instead of Master Database file.

13.Acknowledgement

The authors acknowledge the encouragement from Mr Kaukab Zuberi Director DFRSC, Lahore Garrison University Lahore.

14. References

1 Aftab Ahmad Malik: "Algorithm for Coding Person's Names in large Databases/ Data Warehouses to enhance Processing speed, Efficiency and to reduce Storage Requirements"; Journal of Computer Science and Information Technology, LGURJCSIT, Volume 1 issue 1, January-March 2017; ISSN 2519-7991

2 Aftab Ahmad Malik & Asad Mujtaba: "Algorithm for using Codes in place of Facial images during Image Processing in large Databases/ Data Warehouses to reduce storage, Enhance efficiency and Processing speed; Journal of Computer Science and Information Technology, LGURJCSIT, Volume 1 issue 2, April-June 2017; pp 1-9; ISSN 2519-7991

3 Piyush Patel ""code to generate unique ID for face recognition using OpenCV "[closed] by Stack Overflow Community; which is a community of 6.6 million programmers ; http://stackoverflow.com/questions/16980195/code-to-generate-unique-id-for-face-recognition-using-opencv

4 Shahwar H and Adnan Khan : " Face and Face Parts detection in image processing"; LGURJCSIT: Journal of Computer Science and Information Technology, Vol 1 issue 1, January-March 2017; ISSN 2519-7991

5 Sarah A. Downey 2011, "Unique identity for Facial Recognition";

6 Aftab Ahmad Malik: "Software for Finger Prints Storage and Retrieval of Criminal Identification System for Police", Research Journal, University of Engineering Technology, Lahore, Volume 12; No. 4; PP: 1-18

7 Aftab Ahmad Malik: Software for Storage and Retrieval of Criminal Information for Police", Research Journal, University of Engineering Technology, Lahore, Volume 13 ; No. 1 PP: 1-28

8 Brandon McKinney." Face Patterns", https://www.pinterest.com/pin/512425263825056246/

9 Laurenz Wiskott 2014, “Elastic Bunch Graph Matching”, Scholarpedia, 9(3):10587, Revision #143316] doi:10.4249/scholarpedia.10587

10 Gabor Filters , “ The Computer Vision Lab at GET ,University of Paderborn ,Department of Electrical Engineering, Grundlagen der ElektroTechnik , HNI

11 Laurenz Wiskott, Jean-Marc Fellous, “Face Recognition by Elastic Bunch Graph Matching”, Book: Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, ISBN 0-8493-2055-0, pp. 355-396, (1999).

12 Maurric Hess and Giovanni Martinez, “Facial Feature Extraction based on the Smallest Univalue Segment Assimilating Nucleus (SUSAN) Algorithm”, SUSAN (Smallest Univalue Segment Assimilating Nucleus), Image Processing and Computing Vision Research Lab (IPCV-LAB), Escuela de Ingenieria Electrics, Universidad de Costa Rica

13 Engineer Mujtaba Asad,” Enhanced Security of Digital Images using Discrete Cosine & Discrete Wavelet Transform”, MS (EE) Final Thesis, GC University Lahore, 2014.

14 J. Zafar, and Engineer Mujtaba Asad, “ Enhanced Security and Reinstatement Computing of Images Using Fragile Invisible Integer Wavelet Watermarking Scheme”, Proceedings of the World Congress on Engineering 2015 Vol I , WCE 2015, July 1 - 3, 2015, London, U.K.

15 A. K. Jain, J. Feng, and K. Nandakumar, "Fingerprint Matching", IEEE Computer Magazine: February 2010, pp. 36-44, Feb. 2010

16 D.Braggins, "Fingerprint sensing and analysis", Sensor Review, vol. 21, no. 4, pp. 272-277, 2001

17 John Edgar Hoover, “The Science of Fingerprints, Federal Bureau of Investigation”, John Edgar Hoover.html http://www.scientificlib.com/en/Technoogy/Literature/FBI/TheScienceOfFingerprints.html

18 T. Harris, "How Fingerprint Scanners Work", HowStuffWorks.c

Nizami e*t al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 1 issue 1 Dec 2017

The Reality of Cyber Security

Syeda Marrium Nizami[1] and Gulfraz Naqvi[2]
Lahore Garrison University
mariyum002@yahoo.com[1], gulfraz.naqvi@gmail.com[2]

Abstract

The purpose of this article is to provide information about cyber security. It gives an analysis that would be useful in taking measure to prevent attacks. The judgment of this analysis is made by expertise and knowledge of databases, hardware, encryption, networks, and firewalls. Moreover it will give users an idea about how to keep computer system running smoothly, which ensures that they are considering such actions which could prevent them from their data being theft or financial information being stolen. Further the article gives an insight view about the techniques, which could restrain intruder from accessing, and revealing user's personal information.

Keywords: cybercrime, cyber-terrorism, cyberspace, cyber attacks, Cyber war, cyber terrorism

1. Introduction

Information is power. [1] Nowadays cyber security is the submissive compulsory and the upper most priority of government. The request of cyber security for sparing foundation has expanded to a considerable measure, to a degree where government has made its need to manage cyber dangers by upgrading cyber security. Increased the assurance of consumers, ensure the likelihood of requesting system on which our subsidence can depend, and enhance national security all these things depends on Cyber security. [2] However, to preserve privacy, freedom, alteration, and the motivating nature of the Internet cyber security achievements must be attentively mended set. Each part of the country's critical framework must be considered independently to design an active and fair cyber security strategy.

General, cyber terrorism has been defined as the use of computers and the internet to engage in terrorist activity [3]. The new daring challenges for the legal world are pose growing with the Inventions, discoveries and technologies that broaden scientific horizons. New difficulties in legal matters are posed by the Information Technology that are brought by computers, the Internet, and cyberspace. While managing the Information innovation, it has

demonstrated the lack of law. With regards to Information innovation still there is appropriate need of enactment to manage cybercrime issues.

On the off chance that harsh arrangements are played out the highlights have made the web an accomplishment that, it scatter and a nature in which it is controlled by the client, and its support for modernization and free-form might be in risk. On the off chance that low approach of supporting the highlights of web is viewed as it's an accomplishment in itself, which is extremely various and controlled by the clients. Despite the fact that this strategy if offering control to the client backs the belief system of innovation, yet it can be a wellspring of danger to the general public.

Cold War, corruption, violation, civil crime and terrorist activities are classical approaches that arises in our surrounding and those act cause physical damage to an individual. The fundamental difference between those approaches of crimes and cybercrime, or cyber warfare or cyber terrorism is of the “cyber” adjunct. Here cyber war refers to the battle in cyberspace and includes cyber attacks against a nation state and defect critical infrastructure of casting communication network. Psychological warfare is executed when the utilization of the internet is shown by the digital fear mongering. Digital psychological warfare is executed when fear based oppressors have determined the internet. It is generally known to mean wrongful strikes and dangers of assault against PCs, systems and the data put away in that when done to threaten or pressure an administration or its kin to encourage political or social targets. The motivation behind cyber Terrorism is to assault basic foundation, including sites, organizes, and to take data from these Critical Infrastructures to pressurize the legislature and its kin to accomplish political, social or money related goals. The goal of most of the cybercriminals is to achieve monetary awards against the computer-related corruption.

2. Threats from Cyber crime

Respectively, from the point of view of Information security, a threat can be explained as the possibility that can cause something unpleasant or violent, an unwanted incident that can harm an asset, system or organization. Basically there are three basic origins of the threat:

- Intentional threat
- Accidental threat
- Environmental threat

The use of malicious software or illegal software are the examples of intentional threats. The errors that are caused because of the failure of the hardware, or because of the error in design made by the human or because of service failure are the examples of Accidental threats. On the other hand lightning, thunderstorms or earthquakes are the examples of environmental threats. We can get rid of all these threats or can at least minimise these threats to great level, by taking some efficient steps and actions to confine the harmful affect within each organisation. Threats in whatever way, if not correctly managed, can produce an undesired influence on socio-economy and security of human lives.

3. Cheap method

Conventional, space and cyber- warfare are the categories of the dimension of warfare. Cyber warfare is cheap. Conventional warfare and space warfare are expensive. To many groups and individuals it is easily accessible. There are many individuals who have these capabilities and abilities to undermine the critical infrastructure of the state. Whereas cyber warfare allows asymmetric warfare. The intensity of the destruction caused by the cyber warfare could be similar to the conventional war, as if someone get access to personal computer of a victim through internet, it is inexpensive in contrast to the cost of making, maintaining and using advanced military capabilities that's why it is very pleasant for many of the attackers to use this strategy to harm other nations.

Nowadays less technical knowledge is required and the more of hacking tools and techniques are utilised by the hackers in order to achieve the hacking goals, these tools and techniques are becoming more powerful than ever before. Furthermore, on Internet all of these tools are accessable, which is easier to use, at a very low cost or are free of charge in some occurrences.

Having finite potential and insufficient prospects with great possibility of being caught, there are known threats. Having several potentials and broad fortuity and provide low possibility of being caught, there are also emerging threats. These are some of the difficulties we face in today's world.

4. Case History

Till the day regularity bodies either from academic end or from internal legal body have failed to reach to the consensus to define "terrorism" [4].

Different organisations have defined terrorism in a different way, either its relevant to the government body or any other legal system. Since it's not yet properly defined in every part of the world and international community is slow to reach any conclusion which is agreed universally, this act is emotionally and politically charged in different circumstances.

Various legal systems and government agencies use different definitions of 'terrorism'. Moreover, the international community has been slow to formulate a universally agreed upon, legally binding definition of this crime. These difficulties arise from the fact that the term 'terrorism' is politically and emotionally charged. [5] There are several case histories of cyber threats recorded:

4.1 The Japanese government experienced a Cyber-attack Use of Styles

According to a report on 4 Aug 2004, the Japanese government's computer systems were under attack. Almost synchronously, eight of the Japanese government agencies' computer networks were disordered, in telecommunication terms that are furthermore known as barrage jamming. The damaged

networks were not available for a few hours and sock networks experienced rejection-of-service attacks.

4.2 For hours, hackers congest the US customs' computers

In August 2005, the case was reported where thousands of people were concerned by the viruses that have made the US Customs and Border Protection system victim for certain hours.

The attack took place on the computers, which were placed on Huston, Miami, New York, Los Angeles, and few other airports, the viruses left a heavy burnt.

4.3 Hacker's attack on Estonia's Critical Infrastructure.

Among many dark days of the cyber world the history will remember those three weeks when Estonian critical infrastructure systems were under attack by the hackers, who have hijacked critical infrastructure system of Estonia in May 2007, and have completely disturbed the government, banking, media and police websites, the attacks disabled Internet communications as online transactions were disturbed heavy economic trouble were obtained.

4.4 Russia and Georgia Cyber-warfare

In August Russia's aggression of Georgia had moved into cyberspace as the Russians educated to annoy and achieve candid routing calculated for Georgia.

It is said that the network traffic to Georgia was hijacked by the Russians and changed the path to their attendant. Many Internet servers were under the command and control of Russia there were many Internet servers of Georgia.

Network to a dead lock. This was a simple example of framework attack. To resolve this issue the concerned agencies took three months to eradicate this.

4.5 Cyber-attack on Malaysian Critical Infrastructure

Malaysia's Internet framework was invaded by the Code Red worm, in 2001. They have injected a worm, which had spread in their system very rapidly and brought national communication down.

The approximate minimum losses was RM22mil, which does not includes the losses to the business fraternity and other sectors.

Then later in 2003 the worm by Blaster and Naachi was another mishaps to the Malaysian Critical Infrastructure. The cause of the Incident is the Nacchi worm, which has propagated by the blaster worm in scanning machines through network for vulnerability assessment. This vulnerability found was inly found in the Windows NT, 2000 and XP software were exploited by these worms. The approximate loss was RM31mil, which does not include loss of productivity and the cost of lost opportunity was estimated cost to eradicate this worm .

4.6 Modern hostilities

Whenever there is conflicts between

countries nowadays, cyberspace is the new war frontier. The disfigurement of websites is a popular method of a cyber attack. A website is "vandalized" when a wicked activity like Web defacement is applied. Often the site's original content are replaced with a political or social messages the hacker. Hacker may delete all the content available on the site considering the security accountability of the site. A good example to illustrate this scenario is conflict between US-China in May 2001, which resulted after a Chinese fighter was misplaced at sea from an incident after colliding with a US naval reconnaissance plane.

5. Conclusion

In conclusion, the threats that have taken birth because of the internet or generally because the computer are presenting a difficulty of today and the coming tomorrow. A comprehensive manner of actions are required to address them. A country standing alone cannot deal with the cyber threats. To deal with threats and sensitivity in the cyber world there is a need to have strategic connection. To intensify the security of cyberspace Coordination and collaboration from all parties is very consequential.

6. References

1 See Cybersecurity, Civil Liberties and Innovation: Hearing Before H. Comm. on Energy and Com., 111th Cong. (2009) (statement of Gregory T. Nojeim), available at http://www.cdt.org/security/20090501_cybersecurity.pdf; Cybersecurity: Preventing Terrorist Attacks and Protecting Cyberspace: Hearing Before S. Comm. on the Judiciary, Subcomm. on Terrorism and Homeland Security, 111th Cong. (2009), available at http://www.cdt.org/files/pdfs/20091117_senate_cybersec_testimony.pdf.

2 Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.

3 Clay Wilson, Cong. Research Serv., RL32114, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 5 (2005)", (Wilson argues that defining any particular act as Cyberterrorism is problematic because of the inherent difficulties in determining the attackers identify, motive and intent, but recognizes the potential for Cyberterrorism). Available on http://www.dtic.mil/get-tr-doc/pdf?AD=ADA44479, Retrieved on 12 March, 2009.

4 Myra Williamson, *Terrorism, War and International Law: The Legality of the Use of Force against Afghanistan in 2001*. p. 38, Ashgate Publishing. United Kingdom, 2009.; Alex P. Schmid, *The Definition of Terrorism.* p. 39, *The Routledge Handbook of Terrorism Research.* Routledge, 2011.

5 Bruce Hoffman, *Inside Terrorism,* p. 32, 2nd ed., Columbia University Press, 2006, p. 32, See review in The New York Times, Inside Terrorism, Available on http://www.nytimes.com/books/first/h/hoffman-terrorism.html. Retrieved on 11 February 2012. Cited in "Cyber-Terrorism: Finding a Common Starting Point" by Jeffrey Thomas Biller, to The Faculty of The George Washington University Law School.

Siddiqi e*t al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 1 issue 1 Dec 2017

Crypto Currency in Cyber world

Mohsin Ali[1]
Digital Forensics Research and Service Centre
Lahore Garrison University, Lahore, Pakistan
mohsinaly@lgu.edu.pk

Abstract:

The Article covers the key aspect of the evolution of Cryptocurrency as a future mode of payment for merchant and consumers, the paper will highlight all the key elements that plays a pivotal role in influencing the market value of the Cryptocurrency, with respect to the acceptance of Cryptocurrency within general people, government regulations for this means of transaction, the security aspect of the currency, and where, how and who is using this currency, the perks and the disadvantage that have taken birth due to the advent of this currency which includes bitcoin, ethereum, and other alt-coins. More over the paper concludes with author's analysis on digital currency.

Keywords: Cryptocurrency, Security, transaction, bitcoins, ethereum, Government regulations, payment.

1. Introduction

The evolving trends have change people lives to great extent, every day every instant our standards of living is changing because of the acceptance of new improved items that are arriving the market. These items have not only brought comfort to our lives, but is also source of revenue generation for many individuals. There was an era when all our capital was the gold or silver coins that we had in our hands, then paper money came into existence, then banker's cheque, and then online payments, and now the emerging currency is crypto currency.

It's certainly not wrong to say that over the recent years, the production and the usage of digital currencies also known as crypto currency has increased a lot. The famous among these electronic currency is Bitcoin [1], because of the great market worth, usage and merchant acceptance. There are numerous currencies available in market which are functioning primarily on the same principles as Bitcoin. All these crypto currencies are collectively termed as "altcoins". During the past few years, the altcoins have gained monetary worth and acceptance to great extent.

The total value of crypto currency worth billions of dollar, in a survey conducted in 2015 the total net worth of this industry was $3.8 billion, in which only bitcoin worth was $3.3 billion alone. This shows the acceptance of crypto currency among the people during the recent years [2]. Many of the altcoins available within the market are the replica of the functionality of Bitcoin, it's because of the code being open source, the slight difference in these altcoins, and Bitcoin is of the tweaks, which can be easily enhanced by anyone who has fundamental skills of programming. Though undoubtedly the adoption of crypto currency is increasing day by day, and the market worth of these digital currencies are touching the sky, there are many factors that are issues of concern for developing world, which includes the fragility of the value of this currency, and anonymity. The biggest threat to the world is anonymity of this currency at the moment, where hackers are asking for ransom as an amount to be paid in these crypto currency, where the identity of a hacker is unknown to the victim, and it's a source for them to easily flee the scene. There was a time when the many of the cybercrimes were related to the physical ransom, and the crime end scene had somehow connection with the physical world, but due to the presence of cryptocurrency now this factor has moved more into to virtual world, and has increased the anonymity of the person online to great extent [3].

The mechanism of a crypto currencies like bitcoin, and other same kind of altcoins is just based on "a chain of digital signatures" where for every transaction the owner of the coin must digitally enter the hash value of the last transaction and must generate public key for the next coin holder of crypto coin, which is to be attached at the end portion of the coin, to complete the process of transfer of transferring coin ownership dynamically. Now after purchasing coin there is an additional process of storing these coins either there is an option of storing it on physical hard drives or to store online using wallets available online like coinbase. As every invention has some pros and cons, cryptocurrency has negative features too, Since everything is done online or saved in hard drive there are chances of these currency to be stolen or loss or destroyed, as happened to Mt. Gox in the incident where approximately $ 350 million worth of bitcoin were stolen which caused the company to declare bankruptcy and this has made the concern of money lost in cryptocurrency more prominent, though its matter of 2014 but till the date people are very conscious when it comes to transaction through bitcoins. Apart from the risks within this industry there are more than 5 ton of cryptocurrencies that are available in market, and the success ratio is high, though not as high as bitcoin, but certainly they are playing role in giving boast to this industry. Still there is a lot to be researched of this industry as most of the research focuses on Bitcoin, and research on other altcoins is not done as effectively as done on bitcoin. The advent of this cryptocurrency has not only brought new way to digital payments, but has brought significant development in technological progression, and alarming factor for government entities, for the issuance of new laws for carrying out transactions legally. According to many experts even after these years of Bit coin within the global market there are still mixed perspectives about the future of bit coin and currencies related to this industry. According to [4] he believes that the ratio of electronic

transactions will increase. Block chain mechanism will be greatly used by the stake holders for handling digital transactions [5]. Considering all these elements, the paper will give a brief yet comprehensive analysis on the industry of crypto currency.

2. Literature Review:

This topic of research is taking great strength over the years, the crypto currency is a matter of concern that's been highlighted in most of the research write ups, and the top among all these is Bit coins. There have been several researches done on Bitcoin value, some researchers have actually tried to compare the value of this "moneyless" digital currencies with the actual available currencies like 'digital gold' [6][7]. According to another study carried out by Yermack there are several weakness in Bitcoin currency which can cause fluctuation in the value of this currency. Even though, the value of Bitcoin can change because of many reasons.

Yermack believes there are many weakness in the bitcoins currency which can easily alter its price on a given day. Even though, the price of bitcoins can vary over various exchanges but the bitcoins price in dollars is a bit too high considering alt-coins are not exactly money in the traditional sense and there will be issues of acceptance by people of these crypto currencies [8]. Crypto currency track has been wild over the last half decade even though the traction it has got at the moment. The hype it had at the time it was publically emerged in 2009 was more than the performance of anarchic crypto currency. The future of crypto currency and how it will affect us in future is still unknown, though the demand of alt-coins have increased over the years but when it started in 2009 it was only traded for pennies. It was later that when a slight alteration was made to the code by a community of coders and its value rose from $1 in February of 2011 to $30 after just four months to roughly $290 in 2015 [9]. The remaining portion of this article will highlight the factors which influence the price, and the repute of this digital currency.

2.1 Government Regulations for Cryptocurrency:

It is believed that there is still room for improvement when it comes to the government regulations, and because of this there is hesitation among the investors. Still there are a lot countries which doesn't accept the use these crypto currencies but Japan is one where it's is legitimately allowed to use Cryptocurrency as the legal means of transaction, after implementing changes in the Payment Service Act, which officially recognize the bitcoin and ethereum as legal medium for payment transactions, but it's not piece of cake to use it straight away, any organisation that wish to use this medium should register first with government by paying 10 million yen ($90,000), should ensure that they have proper Secure IT system, to avoid fraud and theft, and an every year audit by certified accountant. Apart from Japan, United States is also making use of digital currency as legal currency, but the process is lengthier, and difficult one needs to go through many channels before getting final approval, while in Japan it's only Financial Services Agencies FSA. [10]

While the growing cryptographic money popularity can possibly reform the mode of

transaction, its presentation into worldwide settings is full of challenges and possible problems linked to it. Since virtual currency standards are not generally perceived as legitimate methods for paying to merchandise and enterprises, creating systematic frameworks for their operation is fundamental. For the monetary reforms to be rational, their legal status must be built up. Administrative frameworks are blooming, with horde approaches being taken by different governments. Current administrative steps are in their initial stages and is changing with rapid growth of the industry [11].

Controls will highlight more prominent genuineness to a cash, which will result in increased mass acknowledgment. They will institutionalize mechanism of the market and limit in any events that can cause instability. While governments are trying administrative steps, their end objective is the same: to confine fraud, protect buyers, regard financial agreements, and create appropriate tax evaluation techniques [12].

2.2 Public Perception about Cryptocurrency:

The acceptance of virtual currencies among general public is growing day by day, according to a survey by Boston Federal Reserve in 2015 a negligible percentage of 0.87% of American consumers were estimated to have Cryptocurrency, which worth's approximately 2.8 million people in United States only. Carrying this calculation ahead, coin based and ARK Research projected that in 2016 roughly 10 million people around the world will own bitcoin. Their survey clearly shows that people have started to adopt digital currency, for business and transaction purposes.

According to another research conducted in America in April 2015 not many Americans knows about the crypto currency, what actually it is and how it works or how can be used. Only 4.5% of the surveyed people had used crypto currency weather in payment or transactions [13]. At that particular instance this stat show very discouraging depiction of how the crypto currency is useful and how only few people are using it.

There are few researcher who believes that the hike in the price of bitcoins is simply a marketing technique of making money, as there is no basic value to support this currency [14]. In contrast to his study Woo, and his fellow researchers states that bitcoin may have some rational value because of its money like properties and can be used in transactions and payments, without any fundamental basis [15]. The advancement in technological aspects can impact the bitcoin value. E.g. the blend of bitcoins in PayPal's instalment framework has brought issues into consideration and encourage a substantial measure of eagerness for advanced financial systems among many people. Besides, many new organisations have begun using crowd funding stages which recognize cryptographic forms of money, with Ethereum being one of the best case. Block stream is another progress that could provide enhanced functionalities to bitcoins, which will ultimately support their general esteem and cost. The purpose of stage was begun to develop better approaches for speeding up developments process in these kind of financial methods and particular contracts.

Only few large retailer have accepted crypto currency as a mode of payment during the initial 6 years of crypto currency. Many of the major vendors like Zhanga, Overstock.com and TigerDirect only used to deal in bitcoins [16]. This shows that there is a positive development of this industries and still it's in developing phase. A paper written by William J. Luther and Josiah Olson, in 2013 stated that hardly any retailers accepts Bitcoin as a type of payment because of the little client base; and many of the customers won't consider utilizing Bitcoin till the time that a critical number of retailers started accepting Bitcoin payments. Basically: arrange impacts support the status quo.... Bitcoin may neglect to gain broad acknowledgment regardless of the prospect that it was better than existing currencies [17].

Block chain technology is new to many of the business, and few of the businesses have already started to adopt this technology. NASDAQ proclaimed that it will launch a block chain-style digital record technology to manage equities with its Nasdaq Private Market stage [18]. The consultancy firm Deloitte has established the Deloitte Crypto Currency Community to direct instructions to its customers on the advantage of the block chain for trading funds and overseeing staff payments, among other things [19]. Even the Federal Reserve System in 2015 has considered the block chain or in other words "digital value transfer vehicle" to process interbank transaction. It is expected that more organisations will adopt this technology as more people will be more familiar.

2.3 Cyber Terrorism and Cryptocurrency:

Though the internet terrorism is not as intense deadly as the conventional terrorism like (bombings, mass killing, and other kind of violence), the reason why it's dangerous is because it's used as a medium to recruit, convert and to establish an easier medium of communication with terrorist cells, with greater degree of anonymity from Intelligence Communities and Law enforcement agencies. Now the question that arises here is that how these terrorist organisation do works? It is believed that they are terrorist groups that have created their websites that have information regarding the history of the group, details about the famous members, and the founder of the group, goals of the organisation and how they are going to achieve their set goals, it's not necessary that all the groups will write their goals directly, there is a possibility that they may not state it directly. The main way to identify their intention is the content they will write against their enemies. There are few groups like Hezbollah and Hamas discuss the operation they have been involved in. Moreover the news that's cited on their website is generally accurate in terms of their "enemies", attack, martyrs and the enemies they have killed in an attack [3].

There have been many cases were terrorist have tried to used crypto currency, for transferring money, Though they are not using it to great extent as they are using the "hawala" system, as they area where they are operating are not IT infrastructure wise as strong as other countries. According to Haaretz in January 2015 one of the support of ISIS Abu-Mustafa was able to raise five bitcoins (approximately $1000) at that time, his account was then shut by FBI, and he was not able to further proceed. Then in May 2015 one of the member Abu Ahmed al-Raqqa had appeal ISIS supporters to

submit their donations on dark web through bitcoins. Then in 2015 another member of ISIS from Virginia had instructed donors through social media to submit donation using bitcoins. It is further reported that one of the ISIS linked hacker "Albanian Hacker" had demanded to bitcoins in order to remove bugs from the system of an Illinois internet retailer, at that time the worth of bitcoin was app $250. In July 2016 a terrorist organisation had received 0.929 bitcoins in 2 different transactions after they have added option of donating those funds through bitcoin. Recently in January 2017 Indonesian financial agency has announced that Bitcoin and other online Services were used by ISIS militants to fund terrorist events in Indonesia [20].

2.4 Stability of Crypto Currency:

Another problematic issue with these virtual currency is that their value is unpredictable, which is one of the reason that plays critical role in user acceptability, just as happened in the case of ZCash where the value of one coin was over $4000 on October 28th, the day when it has launched, and a week later the value dropped to $1000, and now the worth of one coin is below $100 [21]. As happened recently when the rumor of the death of the owner of ethereum broke out, which resulted in loss of $4 million to the ethereum. Ethereum is the second leading crypto currency after bitcoin.

To keep user identity anonymous the efficient methods have been developed for bitcoins and other altcoins. Bitcoin is a digital currency which relies on a systematic set of mineworkers to mine coins, and a distributed system that is responsible for communicating the exchange. The character of Bitcoin clients are concealed behind the pseudonyms (keys) which changes time to time with a set target to increase the exchange. One of the significant feature of bitcoin design is the mining mechanism which involves the participants to solve the computational puzzles in order to gather payment. This helps in understanding the weak points and technical problems such as the inconsistencies in the crypto currency disrupted log data structure [19].

The work that's done on Bitcoin can generally be divided into couple of streams. The main stream of studies are focuses on the strategy and the innovation fundamental decentralized foundation of Bitcoin, i.e. its convention and hazards developing on a specialized level. Different systems in light of system hypothesis have been connected to direct inquiries in regards to exchange irregularities and conceivable results of de-anonym zing single substances in the Block chain. For example, Reid and Harrigan in their study have validated that clients and Bitcoin addresses might be drawn latently by the use of focused administrations, for example, online wallets and money traders also, [20]. On the premise of an everyday utilization situation of Bitcoin on a college grounds, Karame and his co researchers have split their approach with a semi simulative approach the secrecy of Bitcoin-clients. They locate that 40% of the understudies can be profiled inactively which subsequently additionally drives them to dismiss the namelessness theory with respect to Bitcoin. Furthermore, [22] demonstrate that twofold spending is imaginable under the situation of a quick installment (i.e. an installment which is not checked in the Block chain) and in this way they suggest an

alteration of the current Bitcoin execution. Clark what's more, Essex use the Bitcoin-framework to explain a technique with safely timestamp [23].

Though there have been several researches carried out to monitor stability of this type of currency, but till the date its considered to be most fragile currency unlike international currencies like dollars, euros, pound etc. The graph (figure 1) clearly illustrates how the value of bitcoin has changed over the recent months.

Figure 1: Bitcoin Stats

The figure 1 shows the value of one bitcoin against dollar, over the time, according to the figure the value of one bitcoin in early September was around $3400, which was further dropped in mid-September to approximate $3200, and now recently it has achieved the maximum high price of all time of $6034 on 21st October. This shows that the price is never stable and there are always chances of ups and down like stock market prices.

2.5 Critical Infrastructure, and Cryptocurrency:

In 2007 Estonia's Critical Infrastructure (CI) was hacked, which is believed to be caused by Russian hackers or a group of hackers who were upset because Estonian government had moved the Soviet WWII memorial out of city center to their capital of Tallinn, they initiated Distributed Denial of Service attack (DDOS) on the CI of the Estonia, which includes communication systems, and few big name in banking industry there. It is said that most of the banking transaction (98% of the transactions) in Estonia are performed online, and due to this attack there was a huge impact on the financial system. [24]

The United State has initiated the initial steps to counter this threat, by following the Executive Orders (EO) 13.636, and Presidential Policy Directive (PPD) -21; "Improving Critical Infrastructure Cyber Security" and "Critical Infrastructure Security and Resilience" respectively. EO acknowledges the issues that are faced by the CI, and to priorities the national security, wellbeing of the digital world. This EO 13.636 strategies to successfully increase the degree of sharing information regarding cyber security. The plan is to come up with a process that can track, disseminate, record report, and deliver said reports to the necessary agency or agencies with the coordination of National Intelligence. Not only physically but virtually the amount of sharing information among agencies and security providers will improve by this order. The order also states that the information sharing objective will be further improved by temporarily hiring Subject Matter Experts (SMEs), who will provide information to the Critical Infrastructure Operators so that they can provide sufficient security to the CIs. The order further states that agencies will consider all action and courses to make sure that they comply with privacy standards. Annually all Sector Specific Agencies (SSAs) and Subject Matter Experts will spot the CIs by the risks level they are on, and shall work accordingly. [25]

The threat to CIs is inevitable to great extent, many of the banks in London have started to stock Bitcoins, so that if there is threat to their system they can pay in bit coins, it's because criminals prefer to have ransom in shape of virtual currency, which is difficult to be traced. [26]

2.6 Security for Cryptocurrency:

When we talk about online payment transfer procedures or virtual currencies among many other factors, security is one of the major factors that needs to be considered, people still have trust issues with this type of currency because it's something that doesn't exists physically. People still have doubts about the transaction being secure and real, and this is

exactly what people should understand that it's secure and real. There have been many mechanism developed in order to make sure that the digital transaction are secured. For digital transactions. Decentralized trusted Time stamping technique is used to store anonymous record for digital content transaction through online web based service. The service enables clients to hash records, for photographs, content, or recordings, and save the generated hashes in the Bitcoin square chain. Clients would then be able to retrieve and verify the timestamps that have been focused on the piece chain [27].

Crypto currency can work as decentralized trusted time stamping only if digital data of the transaction, and the hash values are embedded together, which keeps record in the block chains of the alt-coins or crypto currency [23].

In addition to all the techniques mentioned above another way of verification of-work in light of looking for prime numbers is presented in shared digital money plans. Three sorts of prime chains known as Cunningham chain of first kind, Cunningham chain of second kind and bi-twin chain are qualified as evidence of-work. Main quickest is connected to piece hash to protect the security property of Nakamoto's Bitcoin, while a consistent trouble assessment conspire is intended to enable prime tie to go about as customizable trouble evidence of-work in a Bitcoin like digital money [28].

3. Conclusion:

After discussing all the key elements above the author would like to conclude the article with the statement that certainly there is no doubt that Cryptocurrency will be the future global currency for the means of transaction.

4. References

1 Hayes Adam, "What Factors Give Cryptocurrencies Their Value: An Empirical Analysis". (16th March 2015) University of Wisconsin - Madison - Department of Sociology; The New School - Department of Economics. Available at SSRN: https://ssrn.com/abstract=2579445

2 Ujan, M., Anthony, S., Oluwakemi, H., Jon, O., Lu, Y. and Richard, B. (2017). " A brief survey of Cryptocurrency systems" - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: http://ieeexplore.ieee.org/document/7906988/

3 Jesse D. Bray, "Anonymity, Cybercrime, and the Connection to Cryptocurrency" (January 2016) Eastern Kentucky University [online] Available at : http://encompass.eku.edu/cgi/viewcontent.cgi?article=1342&context=etd

4 Luther, William J. and Josiah Olson. "Bitcoin is Memory." Journal of Prices & Markets, 3, 3 (2015): 22-33.

5 Nahorniak, I., Leonova, K. and Skorokhod, V. (2016). CRYPTOCURRENCY IN THE CONTEXT OF DEVELOPMENT OF DIGITAL SINGLE MARKET IN EUROPEAN UNION. 3(1).

6 Gertchev, Nikolay. "The Moneyness of Bitcoin.", Available at: www.mises.org (2013).

7 Harwick, Cameron. "Crypto-Currency and the Problem of Intermediation." Available at : SSRN 2523771 (2014).

8 Yermack, David. “Is Bitcoin a Real Currency?”. No. w19747. National Bureau of Economic Research, 2013.

9 Luther, W. (2017). Bitcoin and the Future of Digital Payments. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631314

10 Boyd, J. (2017). “Japan Takes Lead in Legitimizing Digital Currencies”. [online] IEEE Spectrum: Technology, Engineering, and Science News. Available at: https://spectrum.ieee.org/tech-talk/computing/it/japan-takes-lead-in-legitimizing-digital-currencies

11 Raymaekers, "Cryptocurrency Bitcoin: distribution, challenges and opportunities," Journal of Payments Strategy & Systems, vol. 9, no. 1, pp. 30-40, Spring 2015.

12 Gabi Stern. (2015, April) Bit post. [Online]. Available at:http://bit-post.com/players/bitcoin-regulation-around-the-world-the-current-state- 5627

13 Ryan Farell, “An Analysis of the Cryptocurrency Industry”, pp. 15-28, (2015), Available at: http://repository.upenn.edu/cgi/viewcontent.cgi?article=1133&context=wharton_research_scholars

14 Woo, D. Gordon. I., Vadmin. I., “BITCOIN, A FIRST ASSESSMENT. FX and rates” (2013) Available at : https://www.smithandcrown.com/open-research/bank-of-america-bitcoin-a-first-assessment/

15 Robin Arnfield, Royal Canadian Mint Conducts Crypto-Currency Trial, MOBILE PAYMENTS TODAY (Feb. 7, 2014), Available at : http://www.mobilepaymentstoday.com/articles/royalcanadian-mint-conducts-crypto-currency-trial

16 Orcutt. M, “Leaderless Bitcoin Struggles to Make Its Most Crucial Decision” (May 19, 2015) Available at : https://www.technologyreview.com/s/537486/leaderless-bitcoin-struggles-to-make-its-most-crucial-decision/

17 King, R, “By reading this article you are mining bitcoins” (December 17, 2013) Available at: https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

18 Rizzo. P, “Crypto 2.0 in 2015: Turning Bitcoin Theory Into Big Business” (Jan 3, 2015) Available at: https://www.coindesk.com/crypto-2-0-2015-turning-bitcoin-theory-big-business/

19 Joshua A. Kroll, Ian C. Davey, and Edward W. Felten “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries” (June 12, 2013) Available at:

http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf

20 Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "TERRORIST USE OF VIRTUAL CURRENCIES", (May 2017) Available at: http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf

21 Peck, M. (2016). The Crazy Security Behind the Birth of Zcash, the Inside Story. [online] IEEE Spectrum: Technology, Engineering, and Science News. Available at: https://spectrum.ieee.org/tech-talk/computing/networks/the-crazy-security-behind-the-birth-of-zcash

22 Reid,.F . Harrigan,.M "An Analysis of Anonymity in the Bitcoin System" (2013) Available at : http://www.item.ntnu.no/_media/studies/courses/ttm4546/bitcoin_article.pdf

23 Karame. O. G., Androulaki. E., Capkun. S, "Double-Spending Fast Payments in Bitcoin" (October 16 - 18, 2012) Available at: https://dl.acm.org/citation.cfm?id=2382292

24 Clark, J. and Essex, A. (2012). Commitcoin: Carbon dating commitments with bitcoin. In Financial Cryptography and Data Security, volume 7397 of Lecture Notes in Computer Science, Springer

25 James, R. (2009, June 01). A brief history of cybercrime. Retrieved from http://content.time.com/time/nation/article/0,8599,1902073,00.html

26 Obama, B. Office of Press Secretary (2013). Executive order -- improving critical infrastructure cybersecurity (EO 13.636). Retrieved from The White House website: http://www.whitehouse.gov/the-pressoffice/2013/02/12/executive-order-improving-critical-infrastructure cybersecurity

27 Doward J, "City banks plan to hoard bitcoins to help them pay cyber ransoms" (22 Oct 2016) Available at: https://www.theguardian.com/technology/2016/oct/22/city-banks-plan-to-hoard-bitcoins-to-help-them-pay-cyber-ransoms

28 Gipp, Bela. Gernandt, Andre, Meuschke, Norman (2015). Decentralized Trusted Timestamping using the Crypto Currency Bitcoin Available at: https://arxiv.org/ftp/arxiv/papers/502.04015.pdf 1502/1

28 King. S. Ritchie., Williams. S., Yanofsky. D., "By reading this article, you're mining bitcoins" (December 17, 2013) Available at: https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

Nizami e*t al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 1 issue 1 Dec 2017

Electronic Crimes and Prevention

Syeda Marrium Nizami[1] and Gulfraz Naqvi[2]
Lahore Garrison University
mariyum002@yahoo.com[1], gulfraz.naqvi@gmail.com[2]

Abstract:

The basic purpose of this article is to make provision for provision of electronic crimes where as it is expedient to prevent unauthorized acts with respect to information systems, and accommodate related offenses, as well as mechanisms for their investigation, prosecution, trail and international cooperation.

Keywords: Electronic crime, Internet, Hacker, Victim

1. Introduction

"Our pursuit of cyber security will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish." [1] .

Internet and World Wide Web works as a backbone for all online services and activities These online services can be accessed anytime from any place where internet service can reach. Internet provides opportunities of significant social benefits but also opens door of crimes for criminals. Websites and emailing in present era are preferred as medium of sharing data and communication as well This communication is not only restricted to personal data but it also includes sensitive data of organizations for whom information security is very important.

Now days, the technology rests with the devices like mobile phones tablets computers, MP3 players' smart watches and other electronic gadgets that can be used to track daily activities of users Most of these devices share internet via wireless devices or share data through Bluetooth to the devices that enable internet. These changes have dramatically changed the affect of nature of crime in the modern world.

A man is linked with crime and criminality since his failure. Crime remains puzzling and ever scrambles to hide itself in the face of advancement. Depending on the nature and extent of crime different democracies have adopted different plans to pact dispute with crime. This one thing is obvious; it is that a nation with high percentage of crime rate cannot benefit , that is so because crime is directionally proportional to the development. This increase in crime rate will leave an adverse social and economic effect on the

environment. Electronic crime is defined as crimes committed (on the) using electronic devices or internet utilizing the personal computers as either a device to accomplish criminal targets or to target a victim. It is very difficult to classify crimes in general, into distinct groups as many crimes evolve on a daily basis. The crimes like rape, murder or theft need not necessarily be separate, in the real world today. However, the computer and the individual behind it as casualties both are similarly involved in electronic or cyber crime; it all depends on the main target and the criminal. Hence, the computer will be looked at as either a target or tool for creating loss.

The term 'cyber crime' is a misnomer.. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Before evaluating the concept of cyber crime it is obvious that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms may be discussed.

2. Cyber Crime Includes

Following are the few examples of cyber crime:

2.1 Cyber Stalking

Stalking is a termed used to define online harassments and abuses of all soughts.It includes acts like unwanted attention of someone, harassment or intimidation, unauthorized monitoring of someone's activities. Mostly the stalker is motivated by a desire to control his victims.

2.2 Bot Network

A Bot Network is a cyber-crime where a hacker remotely overtakes computer by using malware. The botnet's originator can command and control the system remotely. Systems can be co-opted into a botnet when they execute malicious software.

2.3 Hacking

The wall street journal has reported that computer hackers have accessed the imagined systems containing designs for a new Air force Fighter jet and have stolen huge amount of information [2]

The journal has also reported that spies have infiltrated imagined the electric power grid and left behind malicious computer code. [3]

U.S intelligence agencies, which have developed capabilities to launch cyber attacks on adversary's information system, have made a move to sounded cautions about a determined adversary could do to critical information system in the United States [4]

In general words hacking means seeking and exploiting weakness and security of a computer system or a computer network by gaining unauthorized access. The person who does hacking is known as hacker. Hacker use computer expertise and some tool or scripts to hack any computer system.

2.4 Cracking

It is indeed very unpleasant feeling if the user come to know that a stranger has broken into his computer system without his knowledge or consent and has tampered precious confidential data and information. If

someone has done it to you, it means you have been targeted by a cracker.

Crackers are different from hackers because hackers may be hired to audit network security or test softwares but on the other hand, crackers do same for their own profit or to harm others

2.5 Phishing

Phishing is defined as the act of acquiring data or information such as user name password financial account details through electronic communication. Phishing is done by producing fake links, messages that possess nothing but address of infection/malware contaminated fake website. The website then lure user to enter their personal data and eventually the user will share his/her data once he enters his info on such websites.

2.6 Voice Phishing

Voice phishing is use to gain access of private, personal and financial information from the public. The term is a combination of "voice" and phishing that uses a landline telephone call to get information.

2.7 Carding

Carding is the act of stealing money using debit/credit card information of victim's bank account.

2.8 E-Mail/SMS Spoofing

A spoofed E-mail/ SMS may be said to be one that fakes its origin. It shows different origin from which actually it was originated. Attacker through that email or sms steals identity of another in the form of email address, mobile phone number etc. and via internet sends message.

2.9 Cross site scripting

Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. Reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc are use for Reflected XSS attack.

3 Cyber Squatting

Squatting is gaining possession of unused abandoned or unoccupied domain. Cyber squatting is the act of registering a famous domain name and then selling it to someone who may need that domain at high cost.

3.1 Cyber Crime & Social Networking

Social media is frequently used by cyber criminals to commit online crimes, not only that but it also serve as a platform for carrying out real world crime owing to "over sharing" of these online networking stages. The risk associated with information related to our identity is also high because of social networking sites. Identity information theft can strike anyone who is posting personal information without configuring proper privacy settings. It is estimated that approximately 39-45% of social network users have been victims of profile hacking scam.

3.2 Reasons for Electronic or Cyber Crime

According to "The Concept of Law" 'people are accessible so proper rules are necessary to provide safeguard to them'. Applying this to the cyberspace, we can say

computers are accessible so implementation of proper rules is necessary to provide security to the general population against cybercrime. Following are the reasons for the accessibility of computer:

3.2.1 Data Storage in Small Space

A computer is such a machine, in which very small space to store large amount of data. This makes easy to input or retrieve data or information.

3.2.2 Convenient Access

The reason for digital Terrorism is to assault basic framework, including sites, organizes, and to take data from these Critical Infrastructures to pressurize the legislature and its kin to accomplish political, social or money related goals.

3.2.3 Complicated

The operating systems are made up of millions of codes and the computers work on operating systems. Human personality is broken and it isn't possible that there viability not be a bungle at any progression. Since Human have outlined and composed these codes they are conceivable outcomes that there are some glitches inside the framework. The cyber criminals take benefit of these gaps and cracks into the computer system.

3.2.4 Carelessness

Carelessness is associated with human behaviour the same behaviour of humans serve as a tool to gain control of computer system.

3.2.5 Loss of Witness

Loss of witness is a very accepted & frequent issues as all the data are consistently ruined. Advance collection of information outside the sectional degree additionally crashes the entire course of action of wrongdoing examination.

4. Best Practices for Prevention of Cyber Crime

In an effort to improve security, the Government has developed and is deploying a new intrusion detection system called “Einstein 2.” [5] Einstein 2 will be deployed at participating Federal agency Internet access points. [6] The first full implementation was at the Department of Homeland Security (DHS). [7]

Below mentioned security guidelines and good practices may be followed to minimize the security risk of Cyber crime:

4.1 By updating the Computer

The cyber-attacks can be avoided by keeping operating systems and antiviruses updated because updated computer will be able to deal with latest viruses. However, it will not be enough to protect user from all attacks but it will make information framework security much secure and for hackers it will not be easy to access computer systems.

4.2 By choosing strong passwords

Choosing strong and unique password can ensure data security. Password is like a key to your account and the rule is simple that if your key is strong and secure your account is not an easy meal for any hacker. The user should avoid easy words like names of person city etc. while setting passwords. The password should be combination of upper lower case and alphanumeric letters in a way that no one could be able to guess.

4.3 By protecting computer with security software

Security software commonly includes firewall and antivirus programs. What can be communicated with computer online is controlled by firewall Anti-virus is a software that counters viruses to invade in to systems. A good antivirus software monitor all online activities and warns as soon as it detects any threat to system.

4.4 Online offers are not always too good

Free tool and softwares are also used at times to penetrate viruses into your system. The user must examine the credibility of website and software. Reviews and comments also can help to know the quality before downloading.

4.5 Regular review of bank and credit card statements

The online crimes can be controlled through educating people so they may recognize it after their data is stolen or tried to be hacked. Whenever user observes irregular activities. In such case, one should regularly check banks and credit card's statements.

4.6 Be Social-Media Savvy

Social networking sites like Facebook twitter etc. are prime source of getting information. The user should focus on security setting and it must be ensured that no sensitive data is posted on your profile.

4.7 Secure Mobile Devices

Mobile devices are soft target for hackers, as different application are required to be installed in mobiles for convenience. While downloading applications, always use trusted platform otherwise there is a fair chance of data theft as application could also contain hidden malware.

4.8 Secure wireless network

Wi-Fi networks are vulnerable to intrusion if security concerns are not addressed properly. Public Wi-Fi spots are also used by hackers to trap users by inviting them to free connection.

4.9 Call the Right Person for Help

If computer crime is suspected by a way of identity theft or a commercial scam then immediately report this to local police. If help is needed for maintenance or software installations on computer then consult with authenticated service provider or a certified computer technician.

5. Conclusion

At present criminals have changed their method and have started using advanced technology. In order to deal with cybercrimes all the stakeholders of the society especially the legal and law enforcement authorities will have to take responsibility. Maximum cybercrimes are due to the lack of awareness. This is a duty of Government, print media to educate its public about the dangerous areas of the cyber-world because prevention is better than cure. Cyber Space Security Management has already become an important component of National Security Management, Military Security Management, Scientific Security Management and Intelligence Management all over the world. However, some countries like India has found a way to stop digital wrongdoings yet (No association with the procedure or past proclamation) the cyber law cannot afford to be

static, it has to change with the changing time.

Cybercrime cannot be fully eradicated from cyber space however; check on cyber irregularities can be kept. It is evident that no law is effective until enforced properly. The fear of being caught works as a barrier to get involved in such unethical activities. In short, prevention of cyber-crimes can be ensured through two steps. First is effective legislation so law enforcement agencies can act accordingly. Second is awareness of public that will not only stop the cyber-crimes in its very start but will also discourage the offenders to trap people.

6. Reference

1 President Barack Obama, Remarks at Release of White House Cyberspace Policy Review (May 29, 2009), available at https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

2 See Siobhan Gorman et al., Computer Spies Breach Fighter-Jet Project, WALL ST. J., Apr. 21, 2009, at A1.

3 See Siobhan Gorman, Electricity Grid in U.S. Penetrated by Spies, WALL ST. J.,Apr. 8, 2009, at A1.

4 See generally NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

5 Stephen. G. Bradbury, Principal Deputy Assistant Attorney General, Legal Issues Relating to the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) To Protect Unclassified Computer Networks in the Executive Branch, Jan. 9, 2009, available at http://www.justice.gov/olc/2009/ e2-issues.pdf. The memo concludes that operation of Einstein 2 does not violate the Constitution or surveillance statutes, and an opinion from the Justice Department's Office of Legal Counsel affirms that conclusion. Legality of Intrusion-Detection System To Protect Unclassified Computer Networks in the Executive Branch, Aug. 14, 2009, available at http://www.justice.gov/olc/ 2009/legality-of-e2.pdf.

6 It is unclear whether this means that Einstein 2 operates on privately owned and Operated equipment or on government equipment. More importantly, it is unclear whether The network points at which Einstein is deployed handle only government traffic or could Carry both government and private-to-private traffic.

7 See Hearing Before the Subcomm. on Tech. and Innovation of the H. Comm. on Sci. and Tech., 111th Cong., at 1, 5 (June 16, 2009) (statement of Dr. Peter Fonash, Acting Dir., Nat'l Cybersecurity Div., DHS), available at http://democrats.science.house.gov/Media/file/ Commdocs/hearings/2009/Tech/16jun/Fonash_Testimony.pdf.

Suleman *et al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 1 issue 1 Dec 2017

User Trust on Online Social Network on the basis of Security and privacy

Taseer Suleman[1], Hafiz Burhan-Ul-Haq[2], Sadia Zafar[3]
Lahore Garrison University, Lahore, Pakistan
taseersuleman@lgu.edu.pk, Burhanhashmi64@lgu.edu.pk, Zafarsadia73@gmail.com

Abstract:

Online social networks have become a popular medium of sharing information and also major source for connecting the people on a network. As we know that the threats related to online social network is affecting people to great extent, and is resulting in loss of trust among the people. The trust is basically the measure of confidence that an entity and entities will show in different manners, and privacy is basically a set of actions for controlling personal information. Our basic purpose is to improve user privacy and to build user trust on online social networks. For this purpose, we have conducted survey of users especially teenagers and have taken their views about their knowledge of maintaining privacy on social networks, whether they review privacy settings or leave it as it is, without knowing the importance of privacy. After getting survey result we concluded that most of teenagers are unaware of maintaining privacy so they did not review their privacy settings, resultantly they became a victim of different threats related to online social networks. For this purpose, the tool is designed for reviewing or checking the user's privacy settings and generating different alerts for achieving desired privacy level.

Keywords: Privacy, Online social networks, threats, Survey, response.

1. Introduction

We have seen that online social networks have become popular medium among the people during the past decade. The professor J.A Barnes was the first one to introduce the terminology of social network. By the term social network he described the association of people are brought together by family, work, hobby that is for support such as instrumental, informational, and emotional and also from low level to high level of nation. In 1979 two graduate student of Duke University Tom Truscott and Jim Ellis designed and built the first online social network called Usenet. Now, today we have many online social networks available like Facebook, twitter, Google+, and LinkedIn. As we know number of social media networks are increasing day by day, and eventually its opening doors for affecting users. In which one of major threat is

to the privacy of the user which include name, address, contact and email address, attacker steals this type of user's information and harm them in different ways.
Some of the major threats of online social networks are discussed:

Scams

Scams have been the most common threat used by criminals for centuries. In Facebook world, scam is simply a link that attracts the user. This link contains the information of winning of prizes, gift and cards which mostly attracts innocent people, when the user clicks on it, they get a form to fill their details, in this way scammers easily get their personal information like credit cards numbers etc.

Cyber bullying

This includes sending threatening text messages through online social media. Facebook users especially teenagers are mostly affected by cyber bullying.

Stalking

Cyber stalking is harassing a person with messages typically written threats, and also by adopting other ways online behavior that endangers people safety and can cause a serious problem.
Identity theft:

Due to presence of large amount of personal information on online social networks (OSNs) nowadays, it is not difficult for criminals to steal user's identities. Hackers often break into users e-mail account and then make fake online social media accounts. This happens when users are unaware to hiding their sensitive information by reviewing privacy settings.

Harassment

Harassment through online social networks is becoming common these days. If common user does not understand the way, how to protect his/her personal information this threat would continue to exist. Due to existence of these serious threats, there is an immense need to review privacy settings at the user end. There are many solutions available, in order to, minimize threat level.

However each solution can be better addressed, if we can create awareness among users. For this purpose, we have conducted an online survey. Through this survey the user's knowledge about security as well as privacy features of OSNs had been explored. Our survey was focused mainly on the teenagers because most of the users of OSNs belongs to this age group our society. Our results shows that most of the teenagers are unaware of reviewing their privacy settings and as a result their profile is exposed to the hackers. Hackers can steal their sensitive information easily. After analyzing through survey results we have developed our own feature related to OSNs privacy reviewing process, this feature will update OSN user about the exposure level to the public so that user can review his/her own privacy settings, in order to, achieve desired level of privacy. This feature will protect user from the existing threats on OSNs that we have discussed before.

The rest of the article is divided into following sections: Section III describes the

literature review, Section IV describes our methodology, and in section V we have proposed solution.

2. Related Work

2.1 Implicit trust:

Researchers [1] have defined the trust as one's belief towards the ability of others providing valuable rating. They also defined the properties of trust such as Asymmetry, Dynamicity, and Transitivity. At last they represent trust in two ways.

1. Trust representation
2. Trust matrices.

2.2 Privacy-Related Threats:

In this paper [2] the author describes, user requirements regarding privacy issues, user always like that their data must be kept private, but when the data is posted online on social network their data is not secure, ,and as a result they are exposed to threats like spamming, phishing and malicious attacks which causes harm to the users. The spammers send a link or message to victim and capture their personal data. These attacks are specially carried out by cyber criminals through social engineering. Author divided threats into two types in the paper i.e. Privacy related threats and Traditional Networks Threats. Privacy related threats includes user private profile information i.e. birthday, address, contact no, etc.

Author has also discussed the solution to these problems like creating awareness about the information disclosure, Encouraging awareness through educational campaigns, updating the existing legislation, and empowering the authentication.

2.3 Information Attacks on Online Social Networks

In this research [3] the researcher provides many solutions that can be used to increase security as well as privacy regarding use of OSNs. While the best long-term solution to the security problems is increasing the user's awareness, this may be unpractical because of the huge amount of user using OSNs and their perception is that they are in a safe environment, and they believe that there are many solutions and software available which can be used to improve the overall security.

2.4 Measuring Privacy Risk in Online Social Networks

The problem discussed by author in this research [4] highlight the difficulties in quantifying the amount of information revealed unintentionally and also discuss the privacy issue of online social networks. In order to, overcome this problem a tool has been developed namely as a Privaware to detect the unintentional loss of information. The goal of this tool is to recommend user information that should and also to report the loss of information to mitigate privacy threats.

2.5 Online Social Networks: Privacy Threats and Defenses:

The researchers in [5] explain the four causes that may lead to privacy leaks in OSNs. These causes are design or limitation flaws, clash of interest, implicit flow of information,

and user limitations. The user should have control on these flaws and protect themselves from threats. The information given by the user on online social network describes the users and it will be interesting for the hacker.

2.6 Privacy in Online Social Networks:

In this study [6] the researchers have discussed different problem related to OSNs privacy. Researchers have discussed that the risk of privacy is often ignored or underestimated due to lack of experience and awareness among users. The poorly designed tool made by the OSN and also the centralized nature of OSN make the User dependent on the services provided by the social media network, which at times is not as appropriate as required. The solution of this problem is also provided by researchers is that, the user should actually reveals minimum information which is required for basic functionality of OSNs, but at the same time he/she should keep in mind the consequences that might occur because of revealing personal information .So person must be careful while using these functionalities. The writer also discuss that many laws, including the Data Protection Act 1998 UK, focus on data controllers

2.7 Threats of Online Social Networks:

In this study [7] the researchers discussed that the sharing of the personal information is the one of major issue for users. They have also measured the privacy altitude and have criticized the current privacy setting in Online Social Network. Basically the privacy setting is incomplete without knowing that what the user want to share, For this purpose they have conducted an interview of different user of OSNs in order to know what type of, or what features in the privacy settings that user want. At last they concluded that the information must be categorized as it was categorized previously, but more advancement in this feature is needed.

2.8 Trust Management in Online Social Networks:

The problem discussed in this research [8] is the limited trust of users in Online Social Networks. Mostly the people leave the Social networks because of privacy concerns. Another reason of limited trust on online social networks is that, there is increase in privacy or security threats on online social networks like scamming phishing etc. A solution was suggested to control security threats or to develop user trust. He describes that the only way to find trust is the controlling access in which users grouped together into different categories and access all or limited to specify these groups.

3. Methodology

A step-by-step process was needed to address the privacy threat problem faced by end user of OSNs. It started with a survey that was used to gather information about the privacy related feature and its effects on users especially teenagers. Based on the result of the survey, an additional feature of OSNs privacy is developed which would be help to reduce privacy concerns of the OSNs users.

3.1 Survey results and Analysis:

Our first question was about selection of occupation. The responses had shown that most

of the person using online social networks are students as shown in Fig.01.

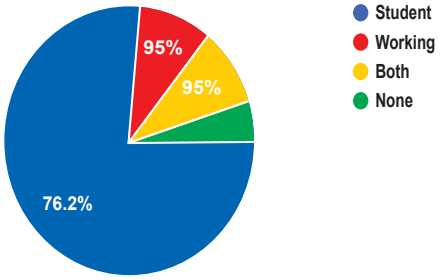


Fig.01. Survey result Question.01

In our next question of the survey, we have asked participants about the social media network that they use? We got to know that more than 70% of them have joined Facebook as their online social network as shown in Fig.02.

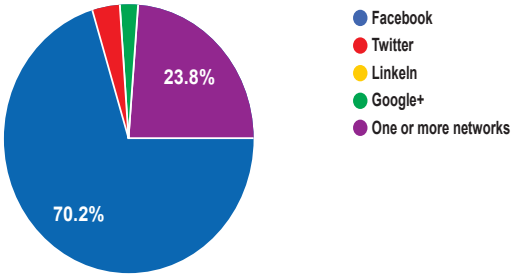


Fig.02. Survey result Question.02

In our proceeding question we had asked about what kind of information they want to include on social sites? Users share all of their vital information on OSNs as shown in Fig.03.

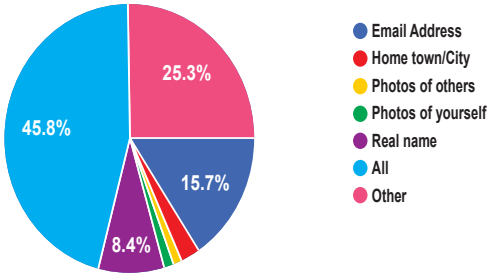


Fig.03. Survey result Question.03

In another question we had ask user about their familiarity about privacy concerns regarding third party applications. Their response was very strange as shown in Fig.04. Most of them had no concern of their privacy while using third party applications in any OSN.

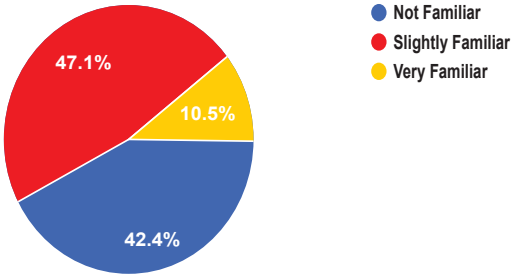


Fig.04. Survey result Question.04

In another question we have asked whether they had ever been victim to a cybercrime. Most of them said "No". Our analysis is either they had very little knowledge about the effects of cybercrime or they had actually made themselves save from such attacks. The result shows in Fig.05.

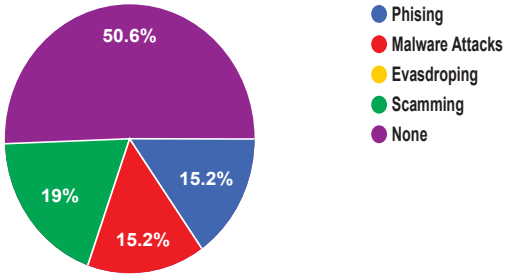


Fig.05. Survey result Question.05

These results show that users have very less knowledge about privacy. They are careless in reviewing their privacy settings, and ultimately they become victim to cyber-attack by hackers. Even OSNs does not provide such mechanism for generating alerts, in order to,

review user privacy settings, we have developed a new feature in which user will be informed about his current privacy settings, and if his/her privacy setting does not comply to the standards of privacy settings, he or she will be notified through our developed mechanism.

3.2 Privacy-alert Mechanism:

We have developed a feature to overcome these problems and to make the OSNs user data more secure, which is the novel idea in online social network. This is dummy tool or feature because online social networks like Facebook do not give the permission to integrate any tool. By using this tool or feature, teenagers set their password strong which is only for their safety purposes as shown in Fig.06.

Fig.06. A dummy Facebook page asking for strong password

Secondly, we have given the easiest or simplest format of security and privacy settings along with important security question which we have obtained after comparison of different online social networks. These privacy settings are quite similar to any other real online social network. It may include privacy features like showing email address and contact number, Blocking messages and third party applications, friend list hiding option etc. A user can adopt any of these settings; For example he or she can show his or her friend list to the public or hide it. In case of showing friend list chances of compromising privacy is higher. This developed feature will determine whether the user profile is secure or it's at risk.

4. Results and Discussions

This feature will create a graph and show the information to the user. The developed feature categorizes the provided information of user privacy settings in to three categories.

- Extremely risky
- Risky
- Secure

In case of "Extremely risky" the user is in red portion of the graph, and has to review his or her profile privacy settings, in order to, prevent from privacy-related threats. In case of "secure" mode, the user has taken all possible measure to ensure privacy. A user with excellent privacy settings is in "Secure" mode as shown in Fig.07.

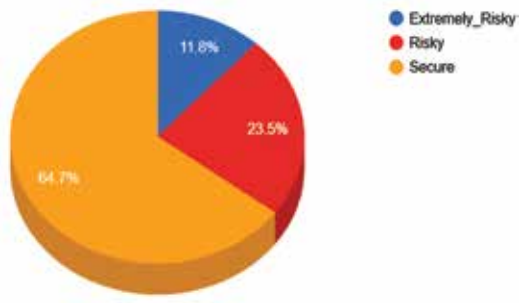


Fig.07. "Extremely risky" profile graph

A user with normal privacy settings is being warned of categorizing him/her in "Risky" mode as shown in Fig.08.

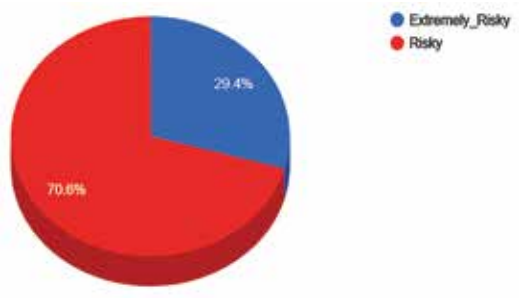


Fig.08. "Risky" profile graph

These pie charts are displayed to the user so that user can review profile privacy settings. This feature would help especially teenager, to, secure themselves form privacy-related threats. This is novel feature that is not included before in any online social network(s).

5. Conclusion and Future Work

In this paper, we have discussed privacy threats regarding OSNs privacy of users especially teenagers. Users are generally don't bother to review their privacy settings which results in the leakage of their vital information. Moreover, there is no such built-in mechanism that exists in any online social network. Which can enforce user to check and review their privacy settings. In our survey results we have also observe irregularities and unawareness at the user end regarding lose privacy settings. This would eventually lead to victimization of a cybercrime. Our proposed feature will help user to find out the level of privacy achieved by checking and reviewing privacy settings. This will help an OSN user to protect his/her profile safe from cyber-attacks.

In future, we will enhance our developed system of OSNs privacy features, and we will also work on security features of social network, that would eventually build user trust on online social networks.

6. Refrences

1 Yadav, A., Chakraverty, S., & Sibal, R. (2015, October). A survey of implicit trust on social networks. In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on (pp. 1511-1515). IEEE.

2 Gharibi, W., & Shaabi, M. (2012). Cyber threats in social networking websites. arXiv preprint arXiv:1202.2420.

3 Franchi, E., Poggi, A., & Tomaiuolo, M. (2014). Information Attacks on Online Social Networks. Journal of Information Technology Research (JITR), 7(3), 54-71.

4 Becker, J. L. (2009). Measuring privacy risk in online social networks. University of California, Davis.

5 Mahmood, S. (2013). Online social networks: Privacy threats and defenses. In Security and Privacy Preserving in Social Networks (pp. 47-71). Springer Vienna.

6 Beye, M., Jeckmans, A. J., Erkin, Z., Hartel, P., Lagendijk, R. L., & Tang, Q. (2012). Privacy in online social networks. In Computational Social Networks(pp. 87-113). Springer London.

7 Al Hasib, A. (2009). Threats of online social networks. IJCSNS International Journal of Computer Science and Network Security, 9(11), 288-93."

8 Fu, B. (2007). Trust Management in Online Social Networks. University of Dublin, Trinity College September.

Editorial Policy and Guidelines for Authors

IJECI is an open access, peer reviewed quarterly Journal published by Digital Forensics Research and Service Centre (DFRSC) LGU. The Journal publishes original research articles and high quality review papers covering all aspects of Digital Forensics and Cyber Security.

The following note set out some general editorial principles. A more detailed style document can be download at www.research.lgu.edu.pk is available. All queries regarding publications should be addressed to editor at email IJECI@lgu.edu.pk. The document must be in word format, other format like pdf or any other shall not be accepted.

The format of paper should be as follows:

- Title of the study (center aligned, font size 14)
- Full name of author(s) (center aligned, font size 10)
- Name of Department
- Name of Institution
- Corresponding author email address.
- Abstract
- Keywords
- Introduction
- Literature Review
- Theoretical Model/Framework and Methodology
- Data analysis/Implementation/Simulation
- Results/ Discussion and Conclusion
- References.

Heading and sub-heading should be differentiated by numbering sequences like, 1. HEADING (Bold, Capitals) 1.1 Subheading (Italic, bold) etc. The article must be typed in Times New Roman with 12 font size 1.5 space, and should have margin 1 inches on the left and right. Length of paper should not be longer than 15 pages, including figures, tables, exhibits and bibliography. Table must have standard caption at the top while figures below with. Figure and table should be in continues numbering. Citation must be in according to the IEEE 2006 style

LAHORE GARRISON UNIVERSITY

Lahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in the Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

VISION

Our vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

MISSION

At present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:
Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
Email: ijeci@lgu.edu.pk

Published by: Digital Forensics Research and Service Center , Lahore Garrison University