ISSN: 2522-3429 (Print)
ISSN 2616-6003 (Online)

International Journal for Electronic Crime Investigation

(IJECI)

Vol. 3 Issue: 4
ISSUE: Oct. - Dec. 2019

Email ID: ijeci@lgu.edu.pk

Digital Forensics Research and Services Center
Lahore Garrison University Lahore, Pakistan.

LGU International Journal for Electronic Crime Investigation
Volume 3(4) October - December

CONTENTS

LGU International Journal for Electronic Crime Investigation
Volume 3(4) October - December (2019)

Sountra et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 4, Oct. - Dec. 2019

Cryptocurrency as a Modern Technique of Money Laundering and Terrorism Financing

Malik Amir Shahzad Sountra
Deputy Prosecutor
aamirshahzad00510@gmail.com

Abstract:
Virtual currency (VC) has become a currency of choice for money launderers, terrorists, kidnappers for ransom and other cyber criminals, especially for its two distinct features i.e. decentralization & fictitious-anonymity. Its usage in terms of criminality is not only increasing day by day but it possesses a huge potential of money laundering (ML) and terrorism financing (TF) in future also. Its probability to become mainstream component deserves a widespread familiarity and exposure to criminal justice circles. This article will encapsulate general awareness of cryptocurrency and its nexus with money laundering and terrorism financing specially with reference to Pakistan. It will also analyze the legal frame work of different countries of the world as well as Pakistan along with recommendations.

Keywords: Crypto currency, Money Laundering, Terrorism Finar

1. Introduction

Once Bill Gates said" the future of money is digital currency"[1]. Cryptocurrency[2] was said to be firstly formulated as facilitator-money for global trade without any centrally controlling authority and without disclosure of personal information of the parties[3]. The records of transactions are maintained in Block chain, and their truthfulness can be verified with the "private key" of the party only[4]. However, this decentralized universal currency is associated with sensitive substantial fiscal and criminal challenges. For instance, investigators may not reach to the identity of sender or receiver without having their "private key"[5]. Its feature of anonymity has made it a foremost choice for cybercriminals and underworld business transactions[6]. Many of the high-profile cases of ransomware[7] and terrorism[8] were found their footprints into the trail of such virtual currencies[910]. It is now said that modern digital world has provided an ideal shelter for all types of cybercriminals specially, money launderers and terrorists[11]. In the recent year, a gang of kidnappers in Lahore, demanded ransom money to be paid in bitcoin while trading in cryptocurrency is currently banned in Pakistan[12]

An old saying enunciates "for every level, there is new devil", in the same way cyberworld is new level where cybercrime is new devil[13]. This devil has become now a versatile facilitator to other crimes. Accordingly, cryptocurrency is now a helping friend of terrorists and money launderers i.e. our engrossed zone of this article. Money laundering has upsetting economic influences on an economy as it adversely affects direct foreign investment by distorting international capital flow. It is also closely linked with terrorist financing; so, it has become a grave global concern[14].

The world is witnessing an expansive growth in use of cryptocurrency especially during past four years and many of the countries are now handling this issue with their customized legislations[15]. Obviously, this alarming threat cannot be left unaddressed but unfortunately, our homeland is with empty hands up till now and no legal framework has been constituted to regulate this virtual giant[16], even we are facing the peril of Financial Action Task Force (FATF) black list. The nature of this pitfall is transnational[17]; accordingly, it is a need of time to keenly observe the regulations formulated by our allies and developed countries, to establish our own legislation within prompt time frame.

At first, this paper aims to create an understanding about "cryptocurrency" for the general public and the quarters concerned. At second, it looks at the

use of such currencies for the purpose of money laundering and terrorism financing. At third, by putting a glance on current scenario in Pakistan, this article evaluates the different laws made by different countries of the world to regulate cryptocurrencies. Finally, this research will propose some recommendations and measures to deal with this modern devil.

2. What is Cryptocurrency?

In 1990 Digital currency was firstly introduced in the market and remained a subject of discussions, but in 2013, growth and popularity of cryptocurrency made such deliberations a serious concern for policy makers and investigation agencies[18]. Cryptocurrency is type of virtual currency. Traditional commercial venders as well as companies like Wikipedia, WordPress, Tesla and Bloomberg are accepting the famous most cryptocurrency namely "Bitcoin"[19] which is one of the most recognizable and best trading cryptocurrencies i.e. more than 1400 cryptocurrencies in circulation all around the world[20]. In 2014, Financial Action Task Force (FATF, USA) defined the term cryptocurrency as:

"A digital representation of value that can be digitally traded and functions as: -

1. ***Medium of exchange and/or***
2. ***A unit of account and/or***
3. ***A store of value but does not have legal tender status…. issued nor guaranteed by any jurisdiction"[21]***

This currency is multifaceted in its roles and features. On one hand it is a facility to make easements for the domestic as well as international trade, while on another hand, its features of anonymity and decentralization make it a potential facilitator for the criminals[22], at the same time it is a pitfall for the legitimate investors[23]. Recently many of the researchers enunciated the fact that Bitcoin is being used for Ponzi fraud[24],[25] and payment for ransomware[26].

Anonymity is glittering characteristics of the cryptocurrency, attractive most for money launderers and terrorist groups. It works as double edge weapon, shielding the privacy of people, nurturing the freedom of trade and democracy in line with the human fundamental rights in an oppressive regime, is optimistic side of its picture[27]. Potentially, cryptocurrency can become a game-changer, it can universally redesign the financial trading mechanisms and modern business models[28]. However, it operates similar to the dark web[29], as it does not need a centralized server. Cryptocurrencies like Bitcoin[30],Ethereum[31] empower the parties to trade peer-to-peer without central authority, resultantly identity of the trading parties is hard to discover. Thus, it is a reported fact that almost all dark market commerce is transacted by means of cryptocurrency[32]

This currency has become approximately billions dollar market[33] however it is very important for general public as well as for investors to know the complexities and risks collateral to cryptocurrencies i.e. volatility, high cost, difficult practical operation, associated multiple hazards and particular complications. Thereby, Stat Bank of Pakistan itemized in May 2017, that it does not recognize virtual currencies[34]. In the same way on 06-04-2018, SBP issued a caution through a press publication for the general public on the risk of cryptocurrencies as under:

"[The] General Public is advised that Virtual Currencies/Coins/Tokens (like Bitcoin, Litecoin, Pakcoin, OneCoin, DasCoin, Pay Diamond etc.) are neither recognized as a Legal Tender nor has SBP authorized or licensed any individual or entity for the issuance, sale, purchase, exchange or investment in any such Virtual Currencies/Coins/Tokens in Pakistan. Further, Banks/ DFIs/ Microfinance Banks and Payment System Operators (PSOs)/ Payment Service Providers (PSPs) have been advised not to facilitate their customers/account holders to transact in Virtual Currencies/ Initial Coin Offerings (ICOs) /Tokens vide BPRD's Circular No. 03 of 2018"[35].

However, it's an alarming notion that in "Anti-Money Laundering and Terrorist Financing Measures, Pakistan Mutual Evaluation Report", Financial Action Task Force (FATF) found that, State Bank & Securities and Exchange Commission of Pakistan have uncleared and limited understanding of Money Laundering (ML) & Terrorist Financing (TF) risks and both institutions need to apply risk-based approach[36].
This digital devil has opened countless gates for cyber thieves, hackers, scammers and robbers. The

report (2nd quarter 2019) of Cipher Trace Cryptocurrency Intelligence July 2019 on "Anti-Money Laundering" reveals[37]:

- ***"Thieves and scammers stole more than $4.26 billion from cryptocurrency exchanges, investors, and users in the first half of 2019.***
- ***Users and investors lost approximately US$2.9 billion as "South Korean" Plus Token app and exchange went offline; Chinese police arrested six Chinese nationals in Vanuatu as the alleged perpetrators.***
- ***Hackers used advanced cyberattack to steal $44 million from world's largest cryptocurrency exchange, Binance.***
- ***Update from Canadian court on QuadrigaCX collapse reveals long history of misappropriation of user funds by QuadrigaCX founder.***
- ***Japanese exchange BITPoint hacked for $30 million.***
- ***BestMixer mixing service seized by law enforcement authorities***
- ***European authorities seized three dark web markets and assets.***
- ***CFTC charged Control-Finance in $147M Ponzi scheme.***
- ***Facebook shook up crypto economy and woke up policy makers with Libra announcement.***
- ***SIM Swapping victim won $75.8 million judgement against hacker.***
- ***More sophisticated exchange hacks used advanced simultaneous takeovers of user and admin accounts.***
- ***SEC sued Kik over $100 million unregistered ICO.***
- ***CipherTrace research shows Bitcoin still dominates payment method in dark markets despite advent of privacy coins.***
- ***Hack may have caused Bitcoin flash crash on Kraken.***
- ***European authorities made arrests in two major typosquatting scams that cost exchange users tens of millions.***
- ***$23 million in Bitcoin lost and co-owner found dead after Polish exchange Bitmarket shutters due to "liquidity issues.***
- ***Iran accused US of attempting to block its virgin Bitcoin as means to compensate for financial hit from sanctions.***
- ***UN published report on North Korean government hackers stealing $571 million from Asian exchanges to fund WMD and compensate for sanctions".***

3 Nexus of Cryptocurrency with Money Laundering (Crypto-laundering)

Money laundering is a procedure of "cleaning" a "dirty" money received from unlawful commotion so that offenders can use that money without apprehension of getting its source traced by investigating agencies. This method can be categorized into three steps i.e. placement, layering, integration.

3.1 Placement

Placement can be done in different ways, for instance criminals can channelize their money into the lawful financial system, by exchanging their money against foreign currency and can hide the identity of their incomes with the technique mingling foreign and domestic banking system. They can use "smurfing and structuring" technique where they split their money into multiple smaller individual deposits into various accounts and then after a reasonable period of time they get back all that money after its cleaning or they can establish cash intensive companies as front man with small amount transactions to avoid detection of larger sums. Smaller the amounts, lesser the risk of detection in any banking system[38].

3.2 Layering

It is a process to mask the illegal origins of dirty money by placing that money into a financial system at first as aforesaid, then by revolving the money into various domestic and offshore accounts and series of transaction, by falsification of fake sale-purchase invoices. Corrupt employees of financial institutions and law enforcement agencies also play their roles by allowing their transactions go through and through[39].

3.3 Integration

This is a final stage of money laundering. It's all about the spending of "cleaned" money which is done very wisely by the criminals i.e. cash purchases of real estate or luxurious articles. Still they do not let the law enforcement or banking system get alert with precautionary measures[40].

3.4 Crypto-laundering

It means money laundering by using cryptocurrency. Crypto-laundering is much faster and easier to pass through the aforementioned three stages. Therefore, cryptocurrency is going to be the foremost choice of money launderers, terrorist and other criminals. Bitcoin facilitates its users with pseudo-anonymity to launder their criminal proceeds with minimum risk of disclosure. Although they have to afford the risk of trust and face to face meeting at some stage for getting their cryptocurrency exchanged with cash. But now it has become a common practice of criminals to use bitcoin or any other cryptocurrency for their illegal business to avoid such apprehensions[41]

Crypto-laundering simplifies the **"placement"** stage as follows: -

- Criminals can deposit large amount of cash into crypto-currency through local cryptocurrency exchanges.
- Illegal business transactions can be done by accepting payments directly into bitcoins e.g. drug traffickers, pornographers etc. can where customers can make payments in bitcoins by concealing identities.
- Their illicit proceeds can be exchanged into bitcoin and can also be stored[42].

For the **"layering"** purpose, smart criminals are using cryptocurrency instead of traditional methods as criminals can create as many cryptocurrency accounts as they need without disclosure of personal identity. For instance, bitcoin blockchain publishes all the transactions between the wallets and smart criminals consciously layer their series of multiple transactions by using their numerous accounts, hence hiding the true origin[43].

Now the stage of getting fiat money against cryptocurrency comes, what we call **"integration"** as a final stage of money laundering. Criminals can cash out their bitcoin into their local currency from where they started cleaning their money or into any other currency they wish to have in any other country of the world. This is how cryptocurrency facilitates the money launderers in terms of minimum time, with less effort and more personal privacy in the process of cleaning their dirty money[44].

As encapsulated in my previous research article on "Cyber Terrorism Laws, implementation and Ways Forward", money laundering has close nexus with terrorism financing[45]. Every terrorist organization needs funds to operate and according to Financial Action Task Force (FATF) 2008[46], funding sources of terrorist groups can be categorized into two heads:

1. Earnings from transnational crimes
2. Funding from sponsors

Such sponsors do money laundering to finance terrorism i.e.

1. To establish long-run infrastructure of terrorist organization in order to recruit and train members, to obtain new sponsors 'and to propagate ideology.
2. Direct operational costs of terrorism e.g. bomb blasts, attacks etc. This is the reason; it is said that money laundering is a global danger for the world's economy and security. So, if we need to stop the terrorism, we need to disrupt their financial resources, we need to stop money laundering[47], we need to stop "crypto-laundering".

Statistics of Law enforcement agencies of Pakistan since 2014 shows that[48]:

- Money laundering investigations initiated 2420
- Out of which 354 prosecuted
- Only one person convicted for corruption based self-laundering
- It is vehemently observed by Financial Action Task Force (FATF) that the level of money laundering risks is much higher than the level of efforts made by law enforcements of Pakistan[49]

4. Terrorism Financing.

In 2015, Financial Action Task Force (FATF) added a specific section regarding use of virtual currencies for terrorism financing[50]. Obviously, cryptocurrency is very attractive to the ghost armed groups to secure and enhance their funding from donations of their sponsors, criminal proceeds e.g. extorting people, abductions for ransom etc., state funding, NGOs and profitable enterprises. Cryptocurrency is used by terrorist to meet all types of multi-challenges collateral to aforementioned sources to ensure an effective flow of such funds to terrorist organizations[51].Researchers summarize that terrorists need cash to operate and their scattered establishments required huge funds flow around the world which is now very easy due to virtual environment in addition to the benefit of concealing their identities, donors and crimes[5253].

Pakistan is continuously facing a threat of terrorism financing. Out of 228 registered cases of TF, only 58 individuals are convicted (49 in Punjab & 9 in rest of the provinces)[54]. About 7600 individuals and 66 entities are proscribed by Pakistan[55] and NACTA has taken some significant steps to improve counter terrorism strategies pertaining to better control over terrorism financing. However according to recent alarms of Financial Action Task Force (FATF), measures taken by Pakistan are not consistent with the TF risks in Pakistan[56]. Our homeland is geographically linked with Iran and Afghanistan which increases the risk of huge cash smuggling. Reportedly many terrorist groups are operating and raising funds in Pakistan[57] i.e. Tehrik-e Taliban Pakistan, Haqqani Network, Quetta Shura Taliban, Lashkar.e.Taiba, Falah-e-Insaniat foundation, Jamaat-ud-Dawa[58], ISIS Khorasan[59], Da,esh, Al-Qaida, Jaish-e-Muhammad[60]. Usually they use formal as well as informal channels for their funds flow like hundi, hawala, cash smuggling etc.[61]

It is said that, all types of terrorist groups around the world are not using crypto currencies at a scale up till now. In 2015 United States assessed that cash & banking system are two main sources of terrorist's funds flow[62] while VC is evolving as a potential threat of TF[63] as most of the terrorist organizations are mainly operating in such areas where infrastructure is very poor and modern telecommunication tools are not available[64]. So, what the key notion for policy maker is to prevent this from happening[65]

A report of US officials tells us that "ISIS is one of the best funded terrorist organizations[66] which holds territory across Syria & Iraq[67] and in 2015 it earned $1 billion approximately[68] including funds inflow from their wealthy donors as well as their external ally fighter groups[69]. Once a user posted a call for donations for some Syria fighter group by giving an account with a German bank[70] and terrorists are using social media for crowdfunding networks as a modern technique for inviting funds as it facilitate a user to set up a page on crowdfunding websites and raise funds from all around the world[71]. It demonstrates that any one who has access to the internet can do so easily beyond traditional podiums.

As for as movements of funds for terrorism operations are concerned, using banking system have become risky for the terrorist groups after 9/11 attacks as Al-Qaida used US banking system widely to orchestrate 9/11 possible[72]. In 2015 a terrorist namely Elshinawy was arrested by FBI, who allegedly transferred $8700 to ISIS through Western Union and PayPal[73]. Hence all types of digital payment services like Google Wallet, PayPal, Amazon Pay etc. can be abused by terrorists for their funds transfer[74].

Virtual currency is appealing to the terrorist for its decentralized structure, anonymity, rapidity with minimum cost and global reach. ISIS followers' have revealed the potential for terrorist groups to use virtual currencies on a global scale. Financial transactions agency of Indonesia, in 2017 announced that Bitcoin and online payment services are being used by terrorist to operate in Middle East[75]. Few of the occurrences are enlisted below: -

- As a first instance, it was reported in January 2015 by Haaretz that an ISIS cell is raising funds on dark web by using Bitcoin. An alleged fundraiser namely Abu Mustafa raised 5 Bitcoin (about $1000) when his account was blocked by FBI[76].
- A suspect on dark web namely Abu Ahmad al-Raqqa placed an appeal to ISIS supporters for donations in Bitcoin. May 2015[77].
- A boy 17 years old arrested and confessed his guilt in Virginia for supporting ISIS. He conveyed instructions to the donors of ISIS to use Bitcoin for an untraceable financial support. June 2015[78].
- A computer burglar with user name "Albanian hacker" demanded 2 Bitcoin for removing bugs from an internet retailer. He also put an "ISIS kill list" of 1351 names of U.S Government and military personnel. August 2015[79]

There is other perspective of some scholars that the velocity of using VCs among the terrorists is slow as compare to the overall expansion of VCs[80] as terrorists want fiat currency most of the time to fulfill their operational expenditures and they might have to face complications when they require their virtual currency converted into fiat money[81].

5. How the World is Regulating Crypto-Currency? Trend Analysis

During last 4 years an expansive growth has been observed in use of cryptocurrency which got the attentions of policy makers of the countries and it has got various names in different jurisdictions[82]: -

Name of the	Name of the

Cryptocurrency being used	Country Using
Digital Currency	Argentina, Thailand, Australia
Virtual Asset	Honduras, Mexico
Electronic currency	Colombia, Lebanon
Cyber currency	Italy, Lebanon
Payment token	Switzerland
Crypto-token	Germany
Virtual commodity	Canada, China, Taiwan

By realizing the risks of TF and money laundering through cryptocurrency, many of the countries have issued notices to sensitized their general public and investors about this pitfall[83]. Some of the countries have updated their counterterrorism and anti-money laundering laws including their regulation regarding financial institutions to stop all types of organized crimes through cryptocurrency market. Some of the countries have imposed tax on cryptocurrency transactions while others have banned it completely. In this reference, a country wise overture is encapsulated below: -

A. Countries where cryptocurrency is taxed as an asset or profit from its sale proceed is considered as taxable income:
   - Argentina [84]
   - Austria [85]
   - Bulgaria[86]
   - Finland[87]
   - Iceland[88]
   - Italy[89]
   - Norway[90]
   - Poland[91]
   - Romania[92]
   - Russia[93]
   - Slovakia[94]
   - South Africa[95]
   - Spain[96]
   - Sweden[97]
   - United Kingdom[98]

B. Countries where Anti-Terrorism & Anti-Money Laundering Laws applicable on cryptocurrency:
   - Latvia[99]
   - Singapore[100]
   - Cayman Islands[101],[102],[103]
   - Costa Rica[104]
   - Gibraltar[105]
   - Hong Kong[106]

   ○

C. Countries where cryptocurrency is taxable and also falls under the ambit of Anti-money laundering laws as well as Counterterrorism laws:
   - Australia[107]
   - Japan[108]
   - Canada[109],[110],[111]

D. Countries where cryptocurrency is absolutely banned
   - Pakistan[112]
   - Nepal[113]
   - Algeria[114]
   - United Arab
   - Egypt[115]
   - Bolivia[116]
   - Iraq[117]
   - India[118]

E. Countries where there is an implicit ban on cryptocurrency
   - Bahrain[119]
   - Bangladesh[120]
   - Iran[121]
   - Taiwan
   - Saudi Arabia[122]
   - Qatar[123]
   - Oman[124]
   - Kuwait[125]
   - China
   - Colombia[126]
   - Dominican Republic[127]

F. Countries that have or in the progression of issuing their own regional or national cryptocurrency
   - China[128]
   - Dominica[129]
   - Ireland[130]
   - Marshall Islands
   - Saint Kitts and Nevis[131]
   - Venezuela[132]
   - Antigua and Barbuda[133]
   - Anguilla[134]

Legal Framework of Pakistan

Presently, no regulation or enactment to control cryptocurrencies or to administer the trade in cryptocurrencies in our homeland[135]. On one hand State Bank of Pakistan has clearly stated that any kind of token, coin or virtual currency is not recognized as legal tender in Pakistan and on other hand SBP directed all types of financial institutions

and money exchangers not to facilitate or participate any kind of virtual currency or token-based transaction. SBP further publicly negated any kind of impression of licensing any individual or institution to purchase, sale or doing investment in such type currencies[136].

Investigations are being conducted by the Federal Board of Revenue Pakistan against the individuals and institutions, involved in trading of digital currency for tax evasion and money laundering[137]. Furthermore, an exclusive operation by Federal Investigation Agency of Pakistan (FIA) has also been lodged against people dealing in cryptocurrencies[138].

Brighter Side of this Picture

Certainly, there is a brighter side of cryptocurrency, critics discuss. It is a technology revolution which cannot be stopped and scope of its benefits is broader than harms. Cryptocurrency is a global financial easement for business as well as for personal life. If this innovative piece is regulated under the law of the state and channelized by minimizing risks of its criminal use, it is full of fruits for its users[139].

While cryptocurrencies have their benefits and drawbacks, critics argue that the innovation of bitcoin technology that promotes a global free market and connects the globe financially is worth more than risks because it helps a lot more people than it harms. However, it is hard to balance the fostering of an innovative piece of technology, while deterring the crime that unsurprisingly is attached to it. If there was a way to mitigate the harms from crime association, then cryptocurrencies would be a lot safer for its users[140].

Recommendations

Financial system has provided an easy access to payment anonymity, at the same time social media is now providing more anonymous communication then ever before. Now it is caution of the time for law enforcement & intelligence agencies to coordinate closely more effectively, simultaneously private sector should be escorted into this picture to play its role to trap the TF and money laundering networks. It is vital that policy authorities must sensitize to all stakeholders of this issue that they must drastically extend their synchronization, along with an expanded legal alleyway with the responsibility to protect the information sharing and regulatory rewards for cooperation. This methodology will help in general to strategy against use of VC by terrorist and money launderers[141]. It is also important to formulate a strategy to unite private entities, state intelligence and regulatory bodies to understand the characteristics and pattern of VC users in a better way. Applying these principles together, would provide a systematic betterment in fight against criminal financial activity[142]. Followings recommendations offer steps to various stakeholders of counterterrorism and anti-money laundering to prioritize their focuses and improve their strategies in this reference: -

1. For a good solution of a problem, first step is to understand it in a better way by all its dimensions, perspectives, endangers and benefits along with its intensity and future apprehensions. Our policy makers are immediately required to do so about cryptocurrency. Only then we shall be able to go for the next steps in a fruitful way.
2. Against any crime, if there is no law, every strategy against that crime would be proved as hollow shadow. Hence Pakistan need to constitute an effective legislation at first as a top priority without any delay. Prevention of Electronic Crime Act 2016, Anti-Terrorism Act 1997, Procedural laws, Law of Evidence, laws related to financial institutions and other relevant laws may be updated immediately in this regard.
3. Mere imposing a ban and issuing few publications by State Bank of Pakistan may not serve the purpose against this huge increasing evil. People of the country may be sensitized to protect the legitimate investors from this trap. Awareness about the abuses of cryptocurrency may be publicized at large.
4. Unfortunately, we do not have a competitive infrastructure against this elite cyber devil to screen, identify and capture the offenders and even if luckily, we arrest the suspects, we are unable to procure the admissible evidence to be produced in the court of law for trial and getting convictions of the wrong doers. Hence a well-coordinated technological infrastructure between the law

enforcements, intelligence agencies and financial sector may be established along with digital forensic lab for procuring and analyzing the electronic evidence.

5. Infrastructure without man power is vague. Cryptocurrency is a common devil, facilitator of many types of crime including terrorism financing and money laundering. To operate effectively against them it is pertinent to understand for a state like Pakistan the nature and patterns of close nexus between both of the crimes. We have two separate law enforcements i.e. Counter Terrorism Department (CTD) having jurisdiction to counter the TF cases & Federal Investigation Agency (FIA) having jurisdiction to counter ML cases. As for as offence of use of cryptocurrency for the purpose of TF & ML the picture is very confused due to the absence of proper clear legislation, shortage of workforce, lack of coordination, knowledge, expertise and skilled manpower. At first, they must be equipped with modern infrastructure and their workforce may be recruited and groomed to the optimum level of this challenging crime. The important most is the active coordination between both the departments and intelligence sharing which is not possible without an effective legislation to regulate the procedures between them. To deal the cybercrime, FIA has established a special wing which may be updated in this reference. CTD may follow this model and should establish a specific wing for an effective operation against terrorism financing considering Financial Action Task Force (FATF) cautions and deadlines.
6. Mutual trainings of above-mentioned stakeholders of the issue including Judges, prosecutors and digital forensic experts may be arranged and SOPs among them may be drafted.
7. Cryptocurrency is worldwide issue. There is a dire need of nationwide regulation and efforts. Our homeland needs to be entered in treaties with other countries in this regard.
8. Rationally, we can not hide ourselves from such modern technological challenges. Ultimately, we have to cope such stranger uncontrolled products with the strength of creating our own competitive products, legislation and taxation system. Digital currency is a game changer step towards global market and a bigger facility to business and financial market. Legitimate investor, importer, exporter and government can take benefits in their jobs. Looking into the China model, Pakistan should issue its own cryptocurrency. This step will work as a strategy against abuses of ghost cryptocurrencies and would give all aforesaid benefits to the state including tax revenue and a better control over investment flow, financial sector and business market.
9. Last but not least, TF&ML are the curses to our homeland and cryptocurrency is able to become a potential friend of the both. It is time of “no more negligence”, hence both the issues should be prioritized as significant concern of public policy and focus of law enforcements. Incentives and protections should be offered to cooperating private sectors and simultaneously violators should be dealt with iron hands. We cannot compete such technological revolutions without technological development, hence we need to get developed our financial technology to face the challenge digital currency.

Conclusion and Future Work

Virtual currency is a technological devil as it has become a currency of choice for criminals, money launderers and terrorist groups by using which they can hide their identity and its worldwide approach has made it more challenging for all the countries of the world. Some of countries taxing it while some countries are in process to issue their own cryptocurrency. Pakistan has imposed a complete ban on it along with some other countries. Terrorism financing, money laundering and other financial criminal activities are very easy to do by using this type of currency. However, we cannot stop it as a future currency of global market. Our homeland is facing allegation and threat of Financial Action Task Force (FATF) pertaining to the terrorism financing and money laundering. So, our policy makers, legislatures, law enforcements, financial institutions, private sectors and all other stakeholders are required to work against both the issues more efficiently than ever before. As cryptocurrency is a common facilitator for both the crimes, hence it is an immediate significance to

focus on it and include it as urgent most issues of our public policy.

References

[1] https://images.app.goo.gl/m51vzGytQXq9iag9

[2] Wikipedia definition of Cryptocurrencies – https://en.wikipedia.org/wiki/Cryptocurrency

[3] Alqassem, D. Svetinovic, Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis, 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), 2014

[4] F. Dai, Y. Shi, N. Meng, L. Wei, Z. Ye, From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues 2017 4th International Conference on Systems and Informatics (ICSAI), 2017

[5] February 2018 https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/

[6] I. Rijnetu, A Closer Look at Ransomware Attacks: Why They Still Work,Heimdal Security Magazine, 8 August 2017 https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/

[7] FBI News: Incidents of Ransomware on the Rise, 29 April 2016 https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

[8] M. Viscuso, Why business is looking good for ransomware criminals, CSOOnline Magazine, 08 November 2017 https://www.cso.com.au/article/629705/why-business-looking-goodransomware-criminals/

[9] Why Cyber-Attackers are Using Bitcoin, RHEA Group Report, 10 July 2017 https://www.rheagroup.com/fr/news/why-cyber-attackers-are-using-bitcoin

[10] C. Duckett, Ransomware victims paying up and would do so again: Telstra, Research article by Australian telco Telstra, 10 April 2018 https://www.zdnet.com/article/ransomware-victims-paying-up-and-woulddo-so-again-telstra/

[11] C. Janze, Are Cryptocurrencies Criminals Best Friends? Examining the CoEvolution of Bitcoin and Darknet Markets, Proceedings of the Americas Conference on Information Systems (AMCIS), 2017

[12] http://www.techjuice.pk/gang-from-lahore-busted-for-demanding-ransom-in-bitcoin/

[13] Mabunda, Sagwadi. 2018. "cryptocurrency: The new face of cyber money laundering ." *Iternational Conference on Advances in Big Data, Computing and communication.* Durban, South Africa: University of Western cape. 1.

[14] National Drug Intelligence Center, "Money laundering in digital currencies," U.S. Department of Justice, No. 2008-R0709-003, June 2008

[15] Directorate, Staf of Global Legal Research. 2018. *Regulations of Cryptocurrency Around the World.* The Law Library of Congress. P. 1

[16] Ibid. P. 102

[17] Durrant, Sara. 2018. "Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations." New York: City University of New York, spring

[18] S.J. Hughes, and S.T. Middlebrook, "Regulating cryptocurrencies in the United States: current issues and future directions," WM. MITCHELL L. REV. 282 40, 2014, p 814

[19] Cao, Sesha Kethineni and Ying. 2019. "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity." *International Crimnal Justice Review.*

[20] Cryptocurrency market capitalization" https://coinmarketcap.com/all/views/all/ (accessed 23 January 2018).

[21] Financial Action Task Force. (2014). FAFT report: Virtual currencies key definitions and potential AML/CFT

risk. Retrieved September 29, 2018, from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtualcurrency-key-definitions-and-potential-aml-cft-risks.pdf

[22] Moser, R. Bohme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in eCrime Researchers Summit (eCRS 2013)

[23] de Balthasar and J. Hernandez-Castro, "An analysis of bitcoin laundry services," in Secure IT Systems. Springer International Publishing, 2017.

[24] Bartoletti, B. Pes, and S. Serusi, "Data mining for detecting bitcoin ponzi schemes," CoRR, vol. abs/1803.00646, 2018

[25] analyzing the bitcoin ponzi scheme ecosystem," in Bitcoin Workshop, 2018

[26] Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," CoRR, vol. abs/1804.04080, 2018.

[27] Akdeniz, "Anonymity, democracy, and cyberspace," Social Research: An International Quarterly, vol. 69, no. 1.

[28] de Balthasar and J. Hernandez-Castro, "An analysis of bitcoin laundry services," in Secure IT Systems. Springer International Publishing, 2017.

[29] Y. Kao and S. C. Hsiao, "The dynamic analysis of wannacry ransomware," in 20th International Conference on Advanced Communication Technology (ICACT 2018), 2018.

[30] Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." [Online]. Available: http://bitcoin.org/bitcoin.pdf

[31] Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." [Online]. Available: http://bitcoin.org/bitcoin.pdf

[32] Trace, Cipher. 2019. *Cryptocurrency Anti-Money Laundering Report, 2019.* Quarterly, CIPHERTRACE.

[33] Constantin, Mireea. 2018. "The Way of Cryptocurrrency." *Economy Information vol.18* 32.

[34] Mubarak Zeb Khan, *FBR Goes After Bitcoin Trader*, DAWN (May 25, 2017), https://www.dawn.com/news/1335184, *archived at* https://perma.cc/7VBW-LL6C

[35] Press Release, State Bank of Pakistan (SBP), Caution Regarding Risks of Virtual Currencies (Apr. 6 2018), http://www.sbp.org.pk/press/2018/Pr-VC-06-Apr-18.pdf, *archived at* https://perma.cc/L76H-PN8U.

[36] APG. October 2019. *Anti-Money Laundering and Terrorist Financing Measures* . Pakstian Mutual Evalution Report, sydny south Australia: Asian/Pecific Group on Money Laundering.

[37] Trace, Cipher. 2019. Cryptocurrency Anti-Money Laundering Report, 2019. Quarterly, CIPHERTRACE.

[38] Irwin, A.S.M., Choo, K.K.R., & Liu, L (2012b). Modelling of money laundering and terrorism financing typologies. Journal of Money Laundering Control, 15(3), 316-335.

[39] ibid

[40] Ibid

[41] Christopher, C.M. (2014). Wack-a-mole: Why prosecuting digital currency exchanges won't stop Online money laundering. Lewis and Clarke Review, 18(1).

[42] ibid

[43] ibid

[44] ibid

[45] Shahzad, Amir. 2019. "Cyber Terrorism Laws, Implementation and Ways Forward." International Journal of Electronic Crime Investigation.

[46] FATF (2008). *FATF Report.* Terrorist financing. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies %20Report.pdf

[47] Ibid

[48] APG. October 2019. *Anti-Money Laundering and Terrorist Financing Measures* . Pakstian Mutual Evalution Report, sydny south Australia: Asian/Pecific Group on Money Laundering.

[49] ibid

[50] FATF (2015). *FATF Report.* Emerging Terrorist Financing Risks. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

[51] ibid

[52] Irwin, A.S.M. & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control, 19*, 407-425.

[53] Salami, I. (2017). Terrorism financing with virtual currencies: Can regulatory technology solutions combat this? *Studies in Conflict & Terrorism*.

[54] APG. October 2019. *Anti-Money Laundering and Terrorist Financing Measures* . Pakstian Mutual Evalution Report, sydny south Australia: Asian/Pecific Group on Money Laundering.

[55] ibid

[56] ibid

[57] Source: https://www.business-standard.com/article/news-ani/jud-launches-political-campaign-in-islamabadseeks-donation-118062600965_1.html.

[58] Source: https://www.state.gov/j/ct/rls/other/des/123085.htm.

[59] Source: https://www.washingtonpost.com/news/worldviews/wp/2017/05/05/isis-is-on-the-decline-in-themiddle-east-but-its-influence-in-pakistan-is-rising/?noredirect=on&utm_term=.82ee2c421cd8. Also see:https://rusi.org/commentary/islamic-state-khorasan-nuanced-view

[60] APG. October 2019. *Anti-Money Laundering and Terrorist Financing Measures* . Pakstian Mutual Evalution Report, sydny south Australia: Asian/Pecific Group on Money Laundering.

[61] Based on Pakistan's NRA 2017 (page 6): "Bank accounts of over 4000 proscribed persons have been frozen."

[62] "2015 National Terrorist Financing Risk Assessment"(Department of the Treasury, June 2015), 47, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

[63] Ibid.,56, 57.

[64] K, Zachary. 2017. "Terrorist Use of Virtual Currencies." *Energy, Economic & Security*, May: 6.

[65] Ibid., 5.

[66] Kristina Wong, "Senators: ISIS Is 'Best Funded' Terror Group Ever," *The Hill*, August 26, 2014, http://thehill.com/policy/defense/216023-senators-isis-is-best-funded-terrorist-group-in-history.

[67] Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)" (FATF/OECD, February 2015), 10, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

[68] "Testimony of A/S for Terrorist Financing Daniel L. Glaser before the House Committee on Foreign Affairs Subcommittee on Terrorism, Non-proliferation, and Trade, and House Committee on Armed Services' Subcommittee on Emerging Threats and Capabilities," Department of the Treasury, press release, June9, 2016, https://www.treasury. gov/press-center/press-releases/Pages/jl0486.aspx; "Statement of Deputy Assistant Secretary Andrew Keller, U.S. Department of State, Bureau for Economic and Business Affair before the United States House of Representatives on Foreign Affairs Subcommittee on Terrorism, Non-proliferation, and Trade, June 9, 2016," Committee on Foreign Affairs. House of Representatives, statement to the Subcommittee on Terrorism, Non-proliferation, and Trade, 2–3

[69] "Financing of the Terrorist Organization ISIL," 18, 20.

[70] "Emerging Terrorist Financing Risks," 31.

[71] Ibid

[72] National Commission on Terrorist Attacks upon the United States et al. "The 9/11 Commission Report," 14

[73] Ralph Ellis, "Maryland Man Charged with Trying to Aid ISIS," CNN, December 14, 2015, http://www.cnn.com/2015/12/14/us/maryland-terror-arrest/.

[74] "Emerging Terrorist Financing Risks," 37–38.

[75] Resty Woro Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says," *The Wall Street Journal*, January 10, 2017, http://www.wsj.com/articles/bit-coin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198.

[76] Danna Harman, "U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests," *Haaretz*, January 29, 2015, http://www.haaretz.com/middle-east-news/.premium-1.639542.

[77] Adam Taylor, "The Islamic State (or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin," *The Washington Post*, June 9, 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamicstate-or-someone-pretending-to-be-it-is-trying-to-raisefunds-using-bitcoin/?utm_term=.17ae7b7b7221.

[78] "Virginia Teen Pleads Guilty to Providing Material Support to ISIL," Department of Justice, press release, June 11, 2015, http://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.

[79] Tim Johnson, "Computer Hack Helped Feed an Islamic State Death List," *McClatchy DC Bureau*, July 20, 2016, http://www.mcclatchydc.com/news/nation-world/national/article90782637.html

[80] Brantly, "Financing Terror Bit by Bit," 1; Baron et al., "National Security Implications of Virtual Currency," 19.

[81] K, Zachary. 2017. "Terrorist Use of Virtual Currencies." *Energy, Economic & Security*, May: 26

[82] Directorate, Staf of Global Legal Research. 2018. *Regulations of Cryptocurrency Around the World.* The Law Library of Congress.

[83] Ibid.

[84] Ley 27430 de Modificación del Impuesto a las Ganancias [Law 27430 Amending the Income Tax Law] art. 2,B.O., Dec. 29, 2017, http://www.telam.com.ar/notas/201702/180185-el-vacio-legal-del-bitcoin-es-o-no-esdinero.html, *archived at* https://perma.cc/M758-JEK

[85] *Steuerliche Behandlung von Kryptowährungen (virtuelle Währungen)* [*Tax Treatment of Cryptocurrencies (Virtual Currencies)*], BMF, https://www.bmf.gv.at/steuern/kryptowaehrung_Besteuerung.html (last updated July 25, 2017), *archived at* http://perma.cc/BU4Z-3BFY.

[86] Marin Marinov, Legal and Tax Treatment of Bitcoin in Bulgaria, RUSKOV & COLLEAGUES (Nov. 20, 2017), https://www.ruskov-law.eu/bulgaria/article/legal-tax-treatment-bitcoin.html, *archived at* https://perma.cc/ZA9H4RGF

[87] Press Release, Vero Skatt, Inkomstbeskattning av virtuella valutor [Income Taxation of Virtual Currencies] (Aug.28, 2013), https://www.vero.fi/sv/Detaljerade_skatteanvisningar/anvisningar/48411/inkomstbeskattning_Wav_virtuella_valuto/, *archived at* https://perma.cc/JEU5-BKLW

[88] Ríkisskattstjóri (RSK), *Leiðbeiningar Skattframtal einstaklinga* [*Guidelines on Tax Return for Individuals*] 15 (2018), https://www.rsk.is/media/baeklingar/rsk_0801_2018.is.pdf, *archived at* https://perma.cc/65VK-7N2K

[89] Paolo Luigi Burlone, *Dichiarazione dei Redditi e Bitcoin* [*Declaration of Income and Bitcoin*], COINLEX,

https://coinlexit.wordpress.com/2016/04/26/dichiarazione-dei-redditi-e-bitcoin/ (last visited Mar. 16, 2018), *archived at* https://perma.cc/QSN8-XSHV.

[90] As per income tax guidelines at *3.1.12 Annen inntekt* [*Other Income*], SKATTEETATEN, https://www.skatteetaten.no/person/skatt/skattemelding/finn-post/3/1/12/ (last visited Apr. 6, 2018), *archived at* https://perma.cc/96P3QXNK

[91] Konrad Krasuski, *Crypto Traders Protest Poland's Tax Decision*, BLOOMBERG (Apr. 9, 2018), https://www.bloomberg.com/news/articles/2018-04-09/crypto-traders-protest-as-poland-wants-tax-from-alltransactions, *archived at* https://perma.cc/2EUZ-GQM9

[92] *Romanians with Bitcoin Must Pay Tax and Social Contributions Despite Virtual Currency Not Being Regulated in Romania*, LIBERTATEA (Mar. 4, 2018), https://www.libertatea.ro/stiri/exclusiv-romanii-cu-bitcoin-datori-la-fisctrebuie-platit-impozit-pe-venit-si-contributii-sociale-desi-monedele-virtuale-nu-sunt-reglementate-in-romania2163395 (in Romanian), *Archived at* https://perma.cc/H966-59E4.

[93] Yevgueniy Gayva, *Cryptocurrency Transactions Will Be Taxed*, RG.RU (Jan. 25, 2018), https://rg.ru/2018/01/25/operacii-s-kriptovaliutami-oblozhat-nalogami.html (in Russian), *archived at* https://perma.cc/53VR-YLTG

[94] Methodological Guideline of the Ministry of Finance of the Slovak Republic No. MF/10386/2018-721 for the Procedure of Taxing Virtual Currency, *available at* http://src.bna.com/xod (in Slovak), *archived at* https://perma.cc/C897-ZS9T; *see also* Jan Sojaspal, *Slovakia to Tax Cryptocurrency Income*, BLOOMBERG (Mar. 28, 2018), https://www.bna.com/slovakia-tax-cryptocurrency-n57982090526/, *archived at* https://perma.cc/F34QU9V5.

[95] Press Release, South Africa Revenue Services, SARS'S Stance on the Tax Treatment of Cryptocurrencies (Apr. 6, 2018), http://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-ofcryptocurrencies-.aspx, *Archived at* https://perma.cc/2ET9-V3KX.

[96] José Trecet, *Declaración de Impuesto a la Renta: Cómo Tributan los Bitcoins en la Renta* [*Income Tax Reporting: How Are Bitcoins Taxed*], BOLSAMANÍA (Mar. 1, 2018), http://www.bolsamania.com/declaracionimpuestos-renta/como-tributan-los-bitcoins-en-la-renta/, *Archived at* https://perma.cc/G4Y7-A59M.

[97] Guidelines available at Skatteverket Dnr: 131 191846-15/111 Beskattning vid mining av bitcoin och andra virtuella valutor m.m. [Guidelines on the Taxation of Mining of Bitcoins and Other Virtual Currencies] (Apr. 24, 2015), https://www4.skatteverket.se/rattsligvagledning/338713.html?q=131+191846-15%2F111, *archived at* https://perma.cc/QVH3-H8AL; *see also* Elin Hofverberg, *Sweden: Tax Authority Publishes Guidelines for Income Tax on Bitcoin Mining, Suggests Prohibition of Bitcoin Use in Waste and Scrap Metal Transactions*, GLOBAL LEGAL MONITOR (May 20, 2015), http://www.loc.gov/law/foreign-news/article/sweden-tax-authority-publishes-guidelinesfor-income-tax-on-bitcoin-mining-suggests-prohibition-of-bitcoin-use-in-waste-and-scrap-metal-transactions/, *Archived at* https://perma.cc/ZR8B-UP8X

[98] HM Revenue & Customs, *Revenue and Customs Brief 9 (2014): Bitcoin and Other Cryptocurrencies* (Mar. 3, 2014), https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-othercryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies, *Archived at* https://perma.cc/MP2E-GQKV

[99] Amendments to the Law on Prevention of Money Laundering and Terrorist Financing, No. 222 (6049) of Nov. 8,

2017, OFFICIAL GAZETTE No. 2017/222.7, https://www.vestnesis.lv/op/2017/222.7 (in Latvian), *archived at* https://perma.cc/8GEV-DSF2; *see also* Dmitriy Kolesnikov, *Regulation of Virtual Currencies Came into Existence in Latvia*, NJORD LAW FIRM (Nov. 10, 2017), https://www.njordlaw.com/ru/latvia-introduces-regulation-crypto/ (in Russian), *archived at* https://perma.cc/8T7M-JE5U.

[100] MAS, Reply to Parliamentary Question on the Prevalence Use of Cryptocurrency in Singapore and Measures to Regulate Cryptocurrency and Initial Coin Offerings (for Parliament Sitting Oct. 2, 2017), http://www.mas.gov.sg/News-and-Publications/Parliamentary-Replies/2017/Prevalence-use-of-cryptocurrency-in-Singapore.aspx, *archived at* https://perma.cc/WXF6-GDPD

[101] Securities Investment Business Law (2015 Revision), EXTRAORDINARY GAZETTE No. 53 (July 17, 2015), https://www.cima.ky/upimages/commonfiles/1499349906SecuritiesInvestmentBusinessLaw2015Revision.pdf, *archived at* https://perma.cc/356F-5DBD.

[102] Proceeds of Crime Law (2017 Revision), Anti-Money Laundering Regulations, 2017, EXTRAORDINARY GAZETTE No. 79 (Sept. 20, 2017), https://www.cima.ky/upimages/commonfiles/1507843083Anti-MoneyLaudering Regulations2017.pdf, *archived at* https://perma.cc/F5MN-XM5

[103] Money Services Law (2010 Revision), EXTRAORDINARY GAZETTE No. 23 (Nov. 8, 2010), https://www.cima.ky/upimages/commonfiles/1499348940MoneyServicesLaw2010Revision.pdf, *archived at* https://perma.cc/Q7UCDB5G.

[104] Press Release, Banco Central de Costa Rica, Posición del Banco Central de Costa Rica (BCCR) y sus Órganos de Desconentración Máxima (ODM) con Respecto a las Criptomonedas (Oct. 9, 2017), http://www.bccr.fi.cr/noticias/historico/2017/Posicion_bccr_criptomonedas.html, *archived at* https://perma.cc/KD4P-WXX8

[105] *Distributed Ledger Technology Regulatory Framework (DLT Framework)*, GIBRALTAR FINANCIAL SERVICES COMMISSION (Jan. 2, 2018), http://www.gfsc.gi/dlt, *archived at* https://perma.cc/L753-37RN.

[106] Press Release, Government of Hong Kong, LCQ4: Regulation of Trading Activities of Bitcoins (Mar. 25, 2015), http://www.info.gov.hk/gia/general/201503/25/P201503250463.htm, *archived at* https://perma.cc/WK74-B453

[107] *Digital Currency Exchange Providers*, AUSTRAC, http://www.austrac.gov.au/digital-currency-exchangeproviders (last Updated Mar.13,2018), *archived at* https://perma.cc/X4DK-SJ8X

[108] 資金決済に関する法律 [Payment Services Act], Act No. 59 of 2009, *as amended by* Act No. 62 of 2016 arts. 63-2 & 63-3. *See also Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider*, FSA, http://www.fsa.go.jp/en/news/2017/20170930-1/02.pdf, *archived at* https://perma.cc/M36D-7BU3.

[109] Mariam Al-Shikarchy et al., Gowling WLG, *Canadian Taxation of Cryptocurrency ... So Far*, LEXOLOGY.COM (Nov. 14, 2017), https://www.lexology.com/library/detail.aspx?g=6283077e-9d32-4531-81a5-56355fa54f47, *archived at* https://perma.cc/H9ZW-47KB

[110] Tariq Ahmad, *Canada: Canada Passes Law Regulating Virtual Currencies as "Money Service Businesses"* GLOBAL LEGAL MONITOR (July 9, 2014), http://www.loc.gov/law/foreign-news/article/canada-canada-passes-lawregulating-virtual-currencies-as-money-service-businesses/, *Archived at* https://perma.cc/BQA6-K7MV

[111] Christine Duhaime, *Canada Implements World's First National Bitcoin Law*, DUHAIME LAW (June 22, 2014), https://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/, *archived at* https://perma.cc/Z3AQ-SKME.

[112] Press Release, State Bank of Pakistan (SBP), Caution Regarding Risks of Virtual Currencies (Apr. 6 2018), http://www.sbp.org.pk/press/2018/Pr-VC-06-Apr-18.pdf, *archived at* https://perma.cc/L76H-PN8U

[113] *7 Nabbed for Running Bitcoin Exchange Business*, KATHMANDU POST (Dec. 27, 2017), http://kathmandu post.ekantipur.com/news/2017-10-06/7-nabbed-for-running-bitcoin-exchange-business.html, *archived at* https://perma.cc/J4BY-4Q7E.

[114] Law No. 17-11 of 1917 (Dec. 27, 2017) art. 117, Official Gazette No. 76 of 2017 (Dec. 28, 2017), https://www.joradp.dz/FTP/JO-ARABE/2017/A2017076.pdf (in Arabic), *archived at* https://perma.cc/JE65-VFFF (translation by author). French translation of the Law *available at* https://www.mfdgi.gov.dz/images/pdf/lois_de_finances/LF2018F.pdf, *archived at* https://perma.cc/XP6A-8Q4A

[115] Press Release, Central Bank of Egypt, A Warning Statement (Jan. 10, 2018), http://www.cbe.org.eg/en/Pages/HighlightsPages/Bitcoin%20Press%20Release.aspx, *archived at* https://perma.cc/3X6D-WFEG

[116] Comunicado, Banco Central Bolivia (Apr. 2017), https://www.bcb.gob.bo/webdocs/11_comunicados/04_2017_COMUNICADO_Uso_monedas.pdf, *archived at* https://perma.cc/YW8G-2Z73

[117] Statement, Central Bank of Iraq, Bitcoin (Dec. 3, 2017), https://cbi.iq/news/view/512 (in Arabic), *archived at* https://perma.cc/JG54-PDHV.

[118] Press Release, Reserve Bank of India, Prohibition on Dealing in Virtual Currencies (VCs) (Apr. 6, 2018), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243&Mode=0, *archived at* https://perma.cc/EFW3HCXG

[119] *Al Maraj: We Do Not Recognize Bitcoin and It is Dangerous to Deal With It*, AL-WATAN (Jan. 7, 2018), http://alwatannews.net/article/752396/Bahrain/رطخ-اهب-لماعتلاونيوكتيبلاب-فرتعن-لا-جارعملا (in Arabic), *archived at* https://perma.cc/WDT3-7R9F.

[120] C entral Bank of Bangladesh, Cautionary Notice on Bitcoin Transactions, https://www.bb.org.bd/mediaroom/noticeboard.php (in Bangladeshi), *archived at* https://perma.cc/7VEN-LYD7; *see also* Abdur Rahim Harmachi, *Bangladesh Bank Warns Against Transaction in 'Illegal' Bitcoin, Other Cryptocurrencies*, BDNEWS24.COM (Dec. 27, 2017), https://bdnews24.com/economy/2017/12/27/bangladesh-bank-warns-against-transaction-in-illegalbitcoin-other-cryptocurrencies, *archived at* https://perma.cc/2APB-ZSZV.

[121] *Iran's Banks Banned from Dealing in Crypto-currencies*, BBC NEWS (Apr. 23, 2018), http://www.bbc.com/news/ technology-43865105, *archived at* https://perma.cc/TQD5-889D; *Iranian Banker Calls for Cryptocurrency Recognition*, FINANCIAL TRIBUNE (Jan. 7, 2018), https://financialtribune.com/articles/economy-business-andmarkets/79459/iranian-banker-calls-for-cryptocurrency-recognition, *Archived at* https://perma.cc/H9HS-AGWK;

[122] *SAMA to Launch Digital Riyals for Banks*, ARAB NEWS (Oct. 5, 2017), http://www.arabnews.com/node/1172906/business-economy, *archived at* https://perma.cc/XC72-Y8U5

[123] Circular No. 6/2018, Central Bank of Qatar (Feb. 2, 2018), http://www.qcb.gov.qa/sitelists/CircularsTo Banks/Lists/Circulars/Attachments/173/Circular%20no.%206-2018.pdf,*archived at* https://perma.cc/AKG5-TJLF

[124] Press Release, Central Bank of Oman (Dec. 12, 2017), http://www.cbooman.org/news/PressRelease18Dec17.pdf (in Arabic), *archived at* https://perma.cc/CL9W-F7VC.

[125] Press Release, Central Bank of Kuwait (Jan. 18, 2018), http://www.cbk.gov.kw/ar/cbk-news/announcements-andpress-releases/press-releases.jsp?kcp=o8QTtSFuP5Ix5WoYWwA74iHHhdsnIQ

(in Arabic), *archived at* https://perma.cc/RXB3-F447.
[126] Superintendencia Financiera de Colombia, Carta Circular 52 de 2017, Riesgos Potenciales Asociados a las Operaciones Realizadas con "Monedas Electronicas-Criptomonedas o MonedasVirtuales" [Potential Risks Associated with Operations Related to "Electronic Currency-Cryptocurrencies or Virtual Money"] (June 22, 2017) *available at* https://actualicese.com/normatividad/2017/06/22/carta-circular-52-de-22-06-2017/, *archived at* https://perma.cc/V4MW-TNUD
[127] Banco Central de la Republica Dominicana, Comunicado (June 29, 2017), https://www.bancentral.gov.do/noticias/avisos/archivos/aviso20170628.pdf, *archived at* https://perma.cc/C2Y6-FD4G
[128] *Zhou Xiaochuan: Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now*, XINHUANET (Mar. 1, 2018), http://www.xinhuanet.com/finance/2018-03/10/c_129826604.htm (in Chinese), *archived at* https://perma.cc/2CW7-8F2T
[129] *Bitcoin Event in Dominica Cancelled*, DOMINICA NEWS ONLINE (Feb. 11, 2015), http://dominicanewsonline.com/news/homepage/news/business/bitcoin-event-in-dominica-cancelled/, *archived at* https://perma.cc/6T86-CC65
[130] Barry Flanagan, *Cryptocurrencies: 'Lack of Regulation Means Investors Can Make a Lot of Money Fast'*, THE JOURNAL.IE (July 2, 2017), http://www.thejournal.ie/readme/cryptocurrencies-lack-of-regulation-means-investorscan-make-a-lot-of-money-fast-3470179-Jul2017/, *Archived at* https://perma.cc/69UV-S86N
[131] Shiva Bissessar, ECLAC, *Opportunities and Risks Associated with the Advent of Digital Currency in the Caribbean*, ECLAC– STUDIES AND PERSPECTIVES SERIES– THE CARIBBEAN No. 46, at 32 (Jan. 2016), http://repositorio.cepal.org/bitstream/handle/11362/39860/S1501234_en.pdf;sequence=1, *archived at* https://perma.cc/F69E-MRTB.
[132] Decreto 3196 Mediante el cual se Autoriza la Creación de la Superintendencia de los Criptoactivos y Actividades Conexas Venezolana [Decree 3196 Authorizing the Creation of the Venezuelan Superintendency of Cryptoassets and Related Activities], GACETA OFICIAL [G.O.], Dec. 8, 2017, http://gacetaoficial.tuabogado.com/gaceta oficial/decada-2010/2017/gaceta-oficial-6346-del-8-diciembre-2017, *archived at* https://perma.cc/CSC3-BKBV
[133] Adam Reese, *Antigua and Barbuda to Support Ethereum-based 'ICO For Development'*, ETHNEWS (Feb. 28, 2018; updated Mar. 1, 2018), https://www.ethnews.com/antigua-and-barbuda-to-support-ico-for-development, *archived at* https://perma.cc/DD5P-6994
[134] Lonnie Hobson, *The Government of Anguilla Announces World's First Cryptocurrency Registration Process for "Utility Token Offerings"*, LINKEDIN (Nov. 15, 2017), https://www.linkedin.com/pulse/government-anguillaannounces-worlds-first-process-utility-hobson/
[135] Mubarak Zeb Khan, *FBR Goes After Bitcoin Trader*, DAWN (May 25, 2017), https://www.dawn.com/news/1335184, *archived at* https://perma.cc/7VBW-LL6C.
[136] Press Release, State Bank of Pakistan (SBP), Caution Regarding Risks of Virtual Currencies (Apr. 6 2018), http://www.sbp.org.pk/press/2018/Pr-VC-06-Apr-18.pdf, *archived at* https://perma.cc/L76H-PN8U
[137] Nozair Hanif Mirza, *FIA Springs Into Action Against Cryptocurrencies, One Held*, DAILY PAKISTAN (GLOBAL) (Feb. 10, 2018), https://en.dailypakistan.com.pk/pakistan/fia-swings-into-action-against-cryptocurrencies-one-held/, *archived at* https://perma.cc/P7KK-RK7G
[138] Ibid.
[139] Durrant, Sara. 2018. "Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations." New

Fatima et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 4, Oct. - Dec. 2019

Forensic Linguistics

Fatima Fatima
fatima.dfrsc@lgu.edu.pk
Lahore Garrison University

Abstract:
This study sheds some light on brief overview of the fundamental elements of forensic linguistics covering the discipline, its history and development. Forensic linguistics is comparatively new field within applied linguistic that describes the nodes between language and legal proceedings. It explores distinctive forms of linguistics evidence as forensic texts including emergency calls, threat letters, ransom and suicidal notes, final statements prior to execution, and public denial or confessions etc. Moreover, it explains different forensic applications of linguistics such as author identification, forensic stylistics, discourse analysis, forensic phonetics, linguistics dialectology, and plagiarism. Legal personals such as lawyers, judges, police officers, translators, and jury members should have awareness of linguistics principles for better understanding of legal issues for a fair and effective trial. With this perspective, this study also extracts importance of forensics linguistics in courtroom and as legal language.

Keywords: Forensic Linguistics, Forensics Phonetics, Evidences

1. Introduction

Language is a communication system that conveys messages with meaning in the form of code like those of communication systems such as human gesture and body language, animal sounds and movements, control signs and lights of traffic, and computer coding source. Human language distinguishes from above mentioned systems of languages as it combines sounds with meanings to yield words or larger structures which are then mutually associated with meanings to particular language and social context by speaker and listener (4). As language is a medium of expressing internal ideas and thoughts of an individual in the form of speech acts, therefore it is important to take into account not only what is said but also its meaning and effects on the listener. Such as impacts of a suicidal letter or ransom note or a threatening letter on the listener. So crime can be committed through written or spoken language. For example, perjury, solicitation, bribery, conspiracy, defamation, warning, and plagiarism etc. (5).

The scientific study of language in the form of structure and function as a human activity is known as linguistics (1,2&4). One of the increasingly prominent and developing applied subfield of linguistics is forensic linguistics which deals with linguistic evidence analysis to elucidate the suspicions in the legal issues (1,2). This discipline has made an important contribution to criminal justice system by implicating scientific knowledge to language with prospect of criminal and civil law (5). It further applies scientific mechanisms resulted from other subfields of linguistics such as stylistics, pragmatics, phonetics, semantics and dialectology. Such mechanisms are used to target and resolve legal disputes during police investigation process (1,2).

There is no law without language as it is codified and mediated through language. Therefore, linguistic is an interface between language, crime and law where law refers to law enforcement, legislation, judicial issues and disputes that seek to a legal remedy. As the language of the law is very different from everyday language so it creates

problem for an ordinary user to criticize the shades of meaning of legal language which often reviewed by linguistic experts known as forensic linguists who perform linguistic knowledge to forensic context of law. The duty of forensic linguist to see what might not be evident to the naked eye in any forensic investigation case, and should have strong background in respective areas of linguistic analysis to identify either a speech act or crime was committed or not (5). Forensic linguists are more concerned with use of language in forensic procedures by understanding language of the written law, its complexity and origin. Such as legal process from point of arrest to interview, charge, trial and finally sentencing stages. They are also interested in understanding of language used by police and lawyers during interviews with witnesses and suspects, and witnesses in cross examination respectively (1,2&3).

2. History and Development of Forensic Linguistics

Linguistic professor Jan Svartvik in 1968, for the first time introduced the term "forensic linguistics" in his book "The Evans Statements: A Case for Forensic Linguistic" (1,2&7). In addition, linguistic and sociolinguistic application to legal matters was debated by Australian linguists in 1980s. Further seminars and conferences regarding to forensic linguistics were also held such as in 1988 two-day conference was organized by German Federal Criminal Police Office (1,2). The most single effective development during the past decades in the field of forensic linguistics was in 1994 when the University of Birmingham initiated "The International Journal of Speech, Language and the Law" edited by Malcolm Coulthard and Peter French (4,6). Likewise, Cardiff University introduced first MA course in forensic linguistics in 1999, and Forensic Linguistics Centre was established at Aston University of Birmingham in 2008 to deal with increasing skills demand in forensic linguistics (1,2).

Scope of forensic linguistics has grown noticeably since it began to establish as a discipline in the recent years. Forensic linguists have been called on to provide evidence in several different types of cases from the beginning of questioning witness and defendant statements such as authorship attribution in terrorism, contamination of products and suspicious deaths. It further follows meaning interpretation in legal and other documents such as establishing time of death from the analysis of mobile phone text messages and the list continues so on (7).

3. Areas of Study

Widely accepted broader definition of forensic linguistics has many aspects with following major areas of study:

3.1. Language of Law / Legal Text

Language of law refers to legal language, its relation to law and legal process (8). Legal text is any text or item of spoken language potentially called forensic text when used in a criminal or legal context (8, 9). It includes the study of text types and forms analysis. Legal text may also encompass a wide range of legal documents that an ordinary person deals with on a regular basis such as end-user license agreements, lease agreements, contracts, real estate, Medicare forms, military disability forms, wills, deeds and other policies (5,8). Other legal texts include legislative texts with domestic statutes, international treaties and multilingual laws, judicial texts produced by judicial and other legal authorities in judicial process, and legal scholarly texts written by legal scholars or academic lawyers (8,10).

When the term 'legal language' is heard, it immediately points to a sparingly punctuated, over lexicalized, opaque and grammatically complex written text (9). Therefore, legal language often ends up being extremely user-unfriendly for its non-expert consumers. A considerable amount of research carried out by forensic linguists shows that legal language is only limited to a reduced number of the population. Such as those of pension plan documents and credit cards analysis with lengthy and complex texts are unintelligible to most people (5).

Forensic linguists when comparing to judges, prefer their definition to be based on observation of actual usage of said words, whereas judges often provide official definition of words from dictionaries which are used in legislation. There so, everyday common words have very different meaning when used as legal jargon. Like the case of a man in which restraining order was lodged against him. He was accused for molesting, interfering and menacing her partner on slipping an apology letter under his partner's door. The issue was that the man was unaware of the legal definition of those terms and never thought that an innocent apology can be considered as an act of molestation or menacing by the law. After this case,

researchers conducted a study in which they provided the restraining order to ordinary readers with four different scenarios if these could violate the order. But most of them failed to determine if it was violated, in fact it was violated (5,10). At this point, the speech act should be referred as it has social function. Therefore, we should know how to demand, ask, suggest and thank or simply we should learn how to use language knowledge as communicating with language is more than grammatical, semantic and lexical knowledge (15).

Complexity and faulty comprehension of language to layperson in jury instructions can and have resulted in many fatal consequences. As many death penalties have been reported by forensic linguists as expert testimony who demonstrate that how the majority numbers of jury could have misunderstood the central points of law that were essential for such cases to be applied (5,6). For this purpose, the defendant accused of a crime not only have the right to remain silent but also the right to be advised of their right to remain known as *"Miranda Warning"*. It is one part of the language of legal text and is being embodied in Police Caution in UK, USA and Australia. This right is of warnings that let know the defendant to be remain silent from the point they are in police custody else whatever they say can and will be used against them in the court of law. Recipients claiming this right must have certain level of competency in English language to completely understand these warnings (6,15).

3.2. Language of Courtroom

Other than written laws and legal documents, language is also a source of communication between law enforcement authorities and witnesses/suspects, and legal argumentation in the court room (4,5). Court room is a sanctified legal institution to promote justice by giving fair hearings of legal trials and judging the crimes. It involves on oral presentation of evidence where words are used as weapons. This leads to a trial as a war of words where the opposing parties use language as their weapons to defeat each other. The verbal exchange used as courtroom interaction differs from ordinary conversation. This area of study, examines the usage of language in cross-examination, evidence presentation, police interviews and testimony, interview techniques and, the questioning process in court room (11,13). Researches have been reported on following courtroom interactions:

3.2.1. Interaction between Police Officer and Suspects

Specific language and linguistic tactics are used by police officer to provoke firm responses from civilians. The social appearance of police officers and the way they often phrase requests as commands, confuse people to know their rights when they are being questioned by them (5,11). The suspects while appealing their right to a lawyer, should request in a direction so that the request may not come off as ambiguous to the officer else it is unacceptable in courtroom. Even a victim cannot receive the right for guidance if the request is not stated in a clear way (4,5&8).

Language plays a significant role in presenting a story to the courtroom during an examination process. The lawyer uses specific tactics to construct the story to stimulate specific reactions and emotions from the witness and jury. Such as examining a hostile witness, lawyers often use language to avoid conflicting evidence from the witness by limiting responses from them. For this purpose, they target yes/no questions and avoid WH-formation questions. WH-questions are targeted by the opposing parties where a defendant lawyer interviews a friendly witness whose testimony could strengthen the constructed story (5,8&11).

Using articular language tactics like dialects and slang, allows both lawyers and witnesses to be more or less truthful to the jury and people in the courtroom. Lawyers may refer to first or nick name of witness and slang to humanize the witness and create non-social situation in the courtroom respectively. However, lawyers also avoid slang and use complex law lexicon in the courtroom to set him apart and define his status. Similarly, specific witnesses may respond differently to constructed legal language of lawyers by using direct or indirect speech which can be based on their past social experiences

and differences, gender differences or education differences (5,11).

3.2.2. Vulnerable Witnesses/Suspects/ Defendants

Communication difficulties have been reported when dealing with vulnerable witnesses in general and, children and juveniles in particular. People with cognitive and mental disorders are more prone to surrendering their rights, changing statements and making false confessions or accepting appeal agreements (5,6).

The word Miranda warnings are worthless to mentally retarded suspects as they simply do not understand them. Most of the interrogators use manipulative methods of psychological interrogation that often lead an innocent person in a vulnerable group resulting in false confession. Linguistic tactics and interrogative techniques applied to suspects with limited language capacity in cross examination, are useless. 70% to 100% of juveniles with diagnosable disorders are still being questioned as healthy adults in judicial proceedings that leads to more false confession (5). People with mental disorders are not only vulnerable in a case where they are suspects but also when they are witnesses or victims of abuse (5,8).

3.2.3. Court Interpretation

Interpreter plays a significant part in fair trial of a legal process where language is used to cause responses. Anyone charged with a criminal offense has the right to an interpreter where she/he cannot speak the language of court. This right is derived from the right to a fair trial with minimum procedural guarantees including the right to have free assistance of an interpreter to understand the concerned court's language (8,11).

Interpretation problems also have been reported in courtroom interactions mainly due to lack of well-trained interpreters and insufficient trained police and legal professionals. It is stated sadly that unprofessional interpreting is truly academic with poor reward of work for field attraction. However, forensic linguists need to train both interpreters and legal professionals more actively. Police and legal professionals should have short course on working with an interpreter as their integral part of training to face a large proportion of non-native speakers in jurisdiction system (5,6).

4. Forensic Linguistic Evidence

Forensic text type or any type of text used in a criminal investigation as evidence in court either spoken, signed or written is termed as forensic linguistic evidence. Forensic text includes emergency calls, ransom notes, unknown letters/calls, suicide letters, text messages, police records, and confession statements etc. Forensic linguistics as expert witness undertaking task other than author identification, also investigate the crimes of language including threats, bribes, conspiracy or perjury (5,12).

In order to check the genuine or simulated texts, some of the main features and aspects are compared with respect to situations pertaining to above listed texts as following (12):

4.1. Emergency Call

The call to emergency services is the first stage of collecting evidence in criminal investigation process which involves a voice conversation between a telephone operator and a public member either witness/victim (9). It is crucial for emergency operators to complete a successful emergency call by extracting primarily linguistic evidence in threatening situation. In an emergency call, it is important to notice voice pitch, accent and cooperation between the caller and recipient. Frankly and timely responses are based only on full cooperation (9,12).

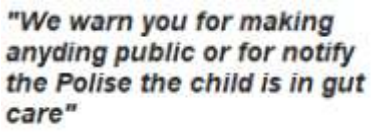
Hesitations, ambiguousness, and incomplete or short answers are indication of making hoax or false call as urgency is important during emergency calls whereas distinct interconnecting and slight overlap of turns shows a genuine call. Both recipient and caller trust each other for correct information and relevant question. Rising pitch of the caller at the end of every turn, might indicate a lack of commitment/assurance, and rising pitch of the recipient represents doubt or desire for further explanation. On the part of the recipient, the call ideally starts from zero to a maximum amount of knowledge in a minimal short

period of time, differentiating emergency call from other kind of service encounter (12,14).

4.2. Ransom Note/Demand

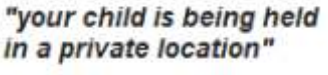
Threat is an important feature of ransom notes which are counterpart of promises in which one person threatens another to cause death/injury if any condition 'X' is not fulfilled. The conditional promise makes the ransom demands so complex that by doing 'x' or paying 'y' will return 'z' to you. Therefore, it is very important to consider the wording of conditions carefully because in most of the cases the kidnaper has no plan of returning back hostage alive or death.

Threats either genuine or false can be identified in analysis of Lindbergh kidnapping case where the primary ransom note stated as follow (12):



Forensic text 1: Ransom note (12)

In this note, the claim that the child is in good hands, can be only made before the culprit enters the location. Therefore, the claim is false as the kidnapper had not even encountered the child at the time of writing note. The claim sometimes, can end up true later when the statement being written ahead of time as in following note (12):



Forensic text 2: Ransom note (12).

The styles of written text have been noted in many ransom demand cases. Forensic linguists examine the style of writing used in ransom notes to determine the true intent of written note and who wrote it. When analyzing ransom notes, writing style may include factors such as syntactic structures, stylistic patterns, punctuations and also spelling (5,12). For example, in analyzing of a ransom note, dialectic variation and misspelling of words identified the suspect. The forensic linguist noticed that the author of the note was trying to show himself less educated than he was by writing daughter as '***dautter***', cops as '***kops***', though he wrote correct spelling of more difficult words such as precious, diaper or watching. However, the uncommon use of term 'devil strip' determine the author of note as it denotes the strip of grass between the side walk and the curb which is only used in surrounding area of Akron, Ohio. It did not take much long the police to find other clues that convicted the suspect who was the only educated man from Akron (5,6).

4.3. Suicide Letters

In forensic linguistic, suicide note being a forensic text is as important as other linguistic evidences. Main purpose of suicide note analysis is to decode the intention or motive of the writer through words as a text. (20,21). Atypical suicide note is brief, concise and propositional with an amount of indirectness whereas a reliable/sound suicide letter in situational context must make a certain clear proposition. A genuine suicide letter has a thematic proposition which is directed to the addressee and relevant to relationship between them. However, it is short typically in length less than 300 words (12).

Generally, content in suicide notes refer to the act of killing oneself, method of suicide that was undertaken and to make the addressee feel guilt. One cannot totally rely on the surface structure of the suicide text to interpret the real intention or the genuineness of suicide note (12,20). The reason and thoughts that lead to self-killing can be uncovered through in-depth semantic and pragmatic linguistics analysis of notes. Various results obtained from the analysis of suicide text indicate that both positive and negative adjectives of emotion can lead to commit suicide. These adjective emotional markers reveal the stated tone and meaning. Positive adjectives include emotional marker with positive meaning of thankfulness and praise to the addressee with positive meaning such as ***strongest*** *mother*, ***greatest*** *father*, ***best*** *mom*, and ***lovely*** *people*, whereas, the negative adjectives appear with negative meaning such as ***arrogant*** *son*, ***angry*** *at you* and *might* ***not*** *be* ***able***. However, there are some adjectives that appear positive but lack the positive meaning or show unfulfilled achievements, failures or hopelessness such as ***biggest*** *sacrifices*, *I am* ***sorry*** and *to make you* ***proud*** etc. The difference in adjectives with positive appearance but with negative meaning is that here the negative meaning is implied

whereas in negative adjectives, the negative meaning is clearly stated (19,21).

4.4. Death Row Statement

Death row statements or final/last statements of a sentenced person, are recent addition to forensic text types allowing to say few words proximately prior to execution. For long, it is followed in American tradition and has not been practiced in the Australia, UK or other English speaking world. Despite the death row statement represents small set of texts, great variation and similarities can be found by making it a distinct and important class of text. The accused person in final statement either admits the crime with impression of honesty and bluntness or deny with an impression of innocence for the witnesses. Such as a fairly unspoken admission of crime is shown in following statement:

I am so sorry for what y'all had to go through. I am so sorry for what all of you had to go through. I can't imagine losing two children. If I was y'all, I would have killed me. You know? I am really so sorry about it, I really am. I got to go sister, I love you. Y'all take care and God bless you.
Gracie was beautiful and Tiffany was beautiful. You had some lovely girls and I am sorry.
I don't know what to say.
All right, Warden, let's do it.

Forensic text 3: Death row statement of Dennis Dowthitt (Texas death row prisoner) (12).

Here in this statement, Dennis admits the crime indirectly by saying that if he had been the family of victim he would have had killed himself, though the sentence 'I would have killed me' is very direct and brutal. However, they also criticize the witnesses as dishonest, law enforcement as corrupt or death row process as inhumane/cruel to portray them innocent and to distract attention away from the moment of pain for revenge in their last moments as in following examples:

(a)

Arizona's death row has become a swamp of inhumane treatment with men driven to various degrees of madness and suicide. Isolation, noise, mistreatment by guards and public indifference take a terrible toll on the human psyche.

(b)

I owe no apologies for a crime I did not commit. Those who lied and fabricated evidence against me will have to answer for what they have done. I know in my heart what I did and I call upon the spirit of my ancestors and all of my people and I swear to them and now Iam coming home.

Forensic text 4: (a) Final statement of Jose Jesus Ceja, (b) Last statement of Basil McFarland (12).

Regardless of same circumstances of death row statements production, initially these do not represent single style, instead form several types of text of denial, admission, public condemnation, and appeals for forgiveness. However, particularly two common features of these statements override the differences, first they all know that they are about to die which they cannot resist, and second they want to die with dignity or some kind of virtue. These statements are within great established settings of death row prisons and forensic linguistics institutes holding an amount of these documents, are conducting researches (12).

4.5. Confessions and denial of Public Persons

Public figures also respond to their accuser in public and sometimes in private in the form of statements. These texts are diverse and different from those of death row statements as they are written or spoken by public figures as in following example, Francis Bacon wrote:

I am ready to make an OBLATION of myself to the King, in whose hands
I am as Clay, to be made into a vessel of Honour or Dishonour. . . . Yet
with respect to this Charge of Bribery I AM INNOCENT. I never had Bribe Or Reward.

Forensic text 5: Letter to the Duke of Buckingham, 1617 (12).

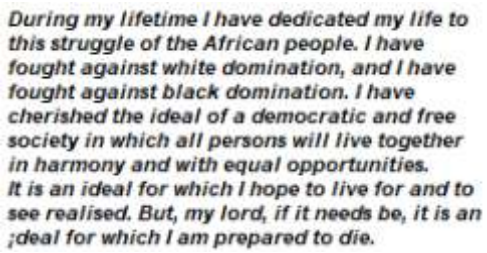
In this text, Bacon prepared his sacrifice to save the king's honor as he believes that a loyal subject should do this while maintaining his innocence as matter of principle. Similarly, Henry Garnet who was head of the Jesuits in England, confessed in his last statement before execution to his part in the Gunpowder scheme as follows:

Good countrymen, I am come hither this blessed day of The Invention of the Holy Cross to end all my crosses in this life. The cause of my suffering is not unknown to you. I confess I have offended the King, and am sorry for it, so far as I was guilty; which was in concealing it, and for that I ask pardon of his Majesty.

Forensic text 6: Confession of Henry Garnet in his last statement (12).

Garnet knew that the Gunpowder Plot was to take place and confessed only for saving people of his own religion from prosecution. Finally, let the closing words of Nelson Mandela be viewed which he stated at the end of his treason trial when he was sentenced to

life imprisonment on Robben Island. In this statement, he states that he is prepared to die for his beliefs as follows:



Forensic text 7: Closing statement of Nelson Mandela take from the British Library National Sound Archive (12).

All of these three statements have linguistic similarities specifying struggle of Mandela for African, suffering of Garnet for people of his religion and Bacon sacrifices for king. All these statements have different idioms with different meanings but with similar communicative purpose, making them a separate class of texts for study (12).

5. Forensic Application of Linguistics

According to Malcolm Coulthard, Linguistic can help court, as if not always, most of the time evidences are in form of text document, text reports, letter or any text format, their interpretation and authorship is always in question. In this regard, disciplines of linguistics can describe the texts through skills and procedures includes phonetics (study of speech/phonology), lexis (words used associated with person or group of people), syntax (words arrangement of sentences), semantics (meaning of words in language context), pragmatics (meaning of words in particular situation), discourse (expression of thought in term of text or talk) analysis (5) as in following explanations:

5.1. Author Identification (Forensic Stylistics)

The question documents text, audio or any material related to language in term of authorship and interpretation can be investigated by another tool of forensic linguistics i.e. forensic stylistic by which authorship of the text or material related to language can be access. These authors have their own distinctive style and language, stylistics can recognize authors attributes by looking into average length of word, average syllables numbers in a word, frequency of article or determiner, punctuation, and ratio of type to symbol (5,6&17).

There are many cases in literature that are solved by forensic stylistics as case of Prinzivaili told by Labov & Harris, 1994, the Prinzivaili was inhabitant of New York working in Pan American Airlines, alleged for threatening his Boss by telephone bomb in Los Angeles as he was thought as unhappy worker and accent of call was supposed as belong to New York. Labov investigated the content by comparing original call for threat with the samples taken from suspect on the basis of vowel patterns and found the caller was not New Yorker but belong to Eastern New England (5,6).

Authorship analysis is performed as sociolinguistic profiling and comparative authorship analysis. Sociolinguistic profiling includes analysis of an email or text messages, statements or postings on social media which are specific context with highly subjective interpretation and when the author is unknown by evaluating his age or education or examination of slang terms, dialect words and spelling mistakes (15,16&18). In comparative analysis, linguists compare the disputed piece of texts with known authorship samples by assessing similarity and uniqueness such as repeated spelling errors etc. This is based on opinion of the likelihood either the texts were written by the same author (3).

In most of criminal cases, there is rarity of some documents with too little texts for a reliable identification but they may provide adequate information to narrow down an author from a group of suspects (1,2). Such case of linguistic evidence, as text messages, was of a girl name Danielle Jones, abducted in 2001. Two mobile text messages were found important in this respect, to detect probability of her kidnapper. Linguistic analysis and stylistics of last two message, sent after her disappearance, and 65 sent prior to 3 days when compared, concluded that last two sent messages do not seem to have connection with previous messages and showed that someone else (abductor/culprit) had sent them (5).

Author identification also depends on the analysis of particular language patterns used like vocabulary, association, pronunciation, spelling, and grammar etc. (2,17). Based on style, there is linguistic variation at group level and also at individual level. Group level

includes inter-author variation in which texts of two authors differ from each other whereas individual level variation includes different texts of same author. Nobody found with homogenous data in style or idiolects, making it difficult to provide such evidence (1,2). Language is not inherited and acquired socially as acquisition lasts life-long. However, education can leave homogenous influence on language use (2,3). Language is always liable to variation such as media and macro-social changes, and following other factors:

- A considerable amount of variation is observed when texts are measured in different genres even though they are written by the same author.
- Text type in personal letters have more inter-authorship variation as compared to academic papers.
- When talking of fiction and non-fiction texts, some of fiction authors are journalists who differ from one another resulting in intra-author variation due to different demands of each medium.
- When it comes to private and public writing, a political speech which is a public text, varies from a private text of friend or family member.
- Anonymous written data can be published by a writer by disguising the result from recognition (1,2&4).
- Language changes as time passes on, influencing author's exposure to language changes. More time lapse results in greater variation for example in murder case of paperboy, tools of linguist played role to determine the reality of confession made by one of the suspects, name Patrick Mollo, who denied his confession and told that he confessed under pressure. The matter was to evaluate the recording of interview, provided by the police, as a proof of his confession, taken before confession whether it is real or fabricated. Coulhart analyzed the recording on the principle of uniqueness, according to which same story told twice by the same person at different time must have overlapping words but told in different style. He concluded that the confession was not real as both contents although belongs at different times but sharing same vocabulary and style that must be different if belong to same person which means that written confession was not real (5,8).

Authorship identification is now observed to be deterministic and researches are being conducted (1,2). Forensic linguists should have strong linguistic background for authorship analysis, to identify either speech act was committed or not, and to transfer conclusion to the audience in a simple and non-technical manner (5).

5.2. Discourse/Pragmatics Analysis

Discourse or pragmatics is the study of written, oral words or study of signs or symbols language or study of a word with different Semiotics (meanings) (1,2&5). Analysis of concealed tape recording between an athlete who was accused of selling drugs and drug dealer, can come to useful conclusion that use of singular pronoun 'I' despite of plural 'W' highlights wrongful act in scheme by showing individual capacity (5).

Similarly, semiotic analysis involves meaning determination of words or phrases either jargons or local terms on form of text or speech. Forensic linguists look at its regional origin and then interpret on its relative meaning which further can be used in investigation procedure for intelligence gathering (3). Such as the utterance of 'yeah and uh-huh', indicates understanding of suggestions by suspect but yeah and uh-huh does not show any agreement to the suggestion (1,2&5). Similar case of a man Lawrence Gerenstein who was accused of killing his wife in a conspiring and soliciting manner. Though there was not any direct request for blaming other man to kill his wife, he discussed about different types of weapons for committing the crime that pointed the figure indirectly towards himself (5).

5.3. Forensic Phonetics (voice or speaker identification)

Forensic linguistics would be incomplete without mentioning the science of forensic phonetics which deals with speaker identification, determination of disputed recorded content, and procedural settings of voice and ear line-ups etc. Forensic phonetics along with forensic linguistics are more established and advanced in legal forum that have been assisted by advance acoustic

engineering. Forensic phoneticians analyzing the distinct characteristics of speech with relation to speaker, makes inquiry easier than 20 years ago. Forensic phonetics has an important principle that there is proper source of reliable identification of an unknown speaker in legal proceedings such as prank bomb threat caller to an emergency service. Like other sciences, Forensic phonetics offer opinions based on examination and observation from the analysis of recorded speech (7,8).

Forensic phonetics involves accurate transcription of what was being said which reveals social and regional information about speaker (1). Phonetic experts use highly trained ear and specialist software to build up speaker profile as local or to a certain region by listening to the speech samples and analyzing accent features (3). Further speaker profiling can be processed by comparing speech samples of known and uncertain origin. The comparison involves assessing the similarities and distinctiveness, useful to indicate either the recordings are of the same or different speakers. The voice recording is an additional and strong qualitative support transcription include or exclude suspects (1,3). Transcription could be written documents, video and audio records. Transcription of text data should be reliable and accurate as it will be used as evidence. Failure to full and accurate transcription leads to altered evidence unconsciously. Text must be emphasized being as an evidence and never should be assumed to be accurate completely. Problem or alteration depends on types of transcription such as disputed utterance of a police officer and a suspect with one of the conversation topic was a third person known as 'Ernie'. Presence of acoustic problems in the investigation tape, sounded the 'Ernie' as 'Ronnie' due to poor signaling. Invasive sounds like that of car engine, playing of the car radio, and target vehicle movement noise overlapped with the first syllable of the disputed name 'Ernie'. Therefore, handwritten, video and audio documents may contain infrequent spellings, repetitions, illegible handwriting, difficult illustrations, speaker mumbling, and irrational talks or jargons that may be difficult to understand and comprehend. However, other sounds such as crying and laughing which are non-linguistic, also included in audio and video recordings. As these are not easily transcribed, interrogations of major criminal cases should be recorded and both the recordings and transcription must be kept safe as evidence (1,2&19).

6. Conclusion

Science has developed researches importantly in relation to the law and language. Forensics linguistics is one of the applied linguistics area where increased advancements lead to solve crimes. This extant study scrutinizes the use of linguistic evidence with respect of forensic linguistics in legal proceedings. It includes forensic application of linguistic disciplines relevant to forensics linguistics that interpret the connection between lawyers and linguist. This study suggests that lawyers and linguist should work thoroughly to flourish forensic linguistic growth. More future research studies are recommended for better tackling of forensic linguistics interpretation with more focus on forensic discourse analysis pertaining to linguistic investigation particularly.

7. References

[1] M.H. Alhumsi, "Key Aspects in Relation to Forensic Linguistics," *International Journal of Linguistics, Literature and Translation (IJLLT)*, Vol. 2(5), pp. 83-86, 2019.

[2] M. G. Ariani& F. Sajedi, "Forensic linguistics: A brief overview of the key elements," *Procedia - Social and Behavioral Sciences,* Vol.158, pp. 222 – 225, 2014.

[3] "Forensic Language Analysis," The Parliamentary Office of Science and Technology, Westminster, London, POST Note 509, 2015.

[4] G. R. McMenamin, "Forensic Linguistcs: Advances in Forensic *Stylistics," Library of Congress Cataloging-in-Publication Data*, ISBN 0-8493-0966-2, 2002.

[5] M. Correa, "Forensic Linguistics: An Overview of the Intersection and Interaction of Language and Law," *KALBỊ STUDIJOS; Studies about Languages*, Vol. 23, 2013.

[6] M. Coulthard, "Forensic Linguistics: the application of language description in

legal contexts," Language at Societies, Vol. 132, pp. 15-33, 2010.

[7] J. Olsson, "What is Forensic Linguistics?" School of Law, Forensic Linguistics Institute, Bangor University, Wales.

[8] M. Coulthard& A. Johnson, "The Routledge Handbook of Forensic Linguistics," Taylor & Francis e-Library, ISBN 0-203-85560-4 Master e-book ISBN, 2010.

[9] M. Coulthard & A. Johnson, "An Introduction to Forensic Linguistics; Language in Evidence," Taylor & Francis e-Library, ISBN 0-203-96971-5 Master e-book ISBN, 2007.

[10] J. Gibbons & M. T. Turell, "Dimensions of Forensic Linguistics," John Benjamins Publishing Company, *Library of Congress Cataloging-in-Publication Data*, ISBN 978-90-272-0521-6, 2008.

[11] S. O. Oluwatobi, "The Role of Forensic Linguistics in Court Room Cross-Examination," Journal of The Department of English, OBAFEMI AWOLOWO University, ILE-IFE, Nigeria, Vol. 12, NO. 2, 2016.

[12] J. Olsson, "Forensic Linguistics: Second Edition," Continuum International Publishing Group, ISBN: 978-08264-9295-1, 2008.

[13] A. Leonard, "Forensic Linguistics; Applying the Scientific Principles of Language Analysis to Issues of the Law," International Journal of the Humanities, Vol. 3, 2005.

[14] N. Momeni, "Fraud in Judicial System" as a Language Crime: Forensic Linguistics Approach," Theory and Practice in Language Studies, Vol. 2 (6), pp. 1263-1269, 2012.

[15] C. S. Michell, "Investigating the Use of Forensic Stylistic and Stylometric Techniques in the Analysis of Authorship on a Publicly Accessible Social Networking Site (Facebook)," University of South Africa, Dissertation, 2016.

[16] V. Guillén-Nieto *et al*,. "Exploring State-of-the-Art Software for Forensic Authorship Identification," *International Journal of English Studies,* vol. 8 (1), pp. 1-28, 2008.

[17] C. E. Chaski, "Linguistic Authentication and Reliability," *NCJRS.*

[18] M. W. Corney, "Analyzing E-mail Text Authorship for Forensic Purposes," Queensland University of Technology, Dissertation, 2003.

[19] G. Oxburgh *et al*,. "Communication in Investigative and Legal Contexts; Integrated Approaches from Forensics Psychology, Linguistics and Law Enforcement," *Wiley Blackwell: The Psychology of Crime, Policing and Law*, 2016.

[20] M. F. Cabanaa *et al*,. "Linguistic analysis of suicide notes in Spain," *Eur. J. Psychiat*. Vol. 29 (2), pp. 145-155, 2015.

[21] R. Alfian, "Meanings in a Suicide Note: An Analysis of Linguistics Pragmatics in Nusadi's Suicide Note," ResearchGate, 2018.

Nazir et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 4, Oct. - Dec. 2019

Cloud Forensics: Challenges and Evidence Collection

Jaleel Nazir[1] ,Mohsin Ali[2], Tahir Ilyas[3]
jaleel@lgu.edu.pk[1], mohsinaly@lgu.edu.pk[2], tahirilyas@lgu.edu.pk[3]
Lahore Garrison University

Abstract:

Cloud computing without any doubt has been one of the major key players in the present and upcoming era of digitization. The concepts of IT Governance, transparency through digitization has been pacing the present world with an accelerated velocity that has never been assumed or thought of before. With the advent of cloud computing, many businesses are using cloud for deployment and services. But with this paradigm shift subjects like digital crimes and vulnerability have also taken birth. With such scenarios it is need of an hour to have frameworks which can detect and solve crimes related to cloud deployment. There have been several frameworks that have been implemented and there are several frameworks that have been proposed by different researchers but still there is a large room for improvement especially in standardizing frameworks and procedure for Cloud Infrastructure (Gayatri S Pandi, 2018). This paper focuses on the scenarios and discusses the various aspects of the Digital Forensics Frameworks and challenges faced by investigators using existing conventional frameworks. One of the major challenge that is faced by the investigators and researchers is the absence of Physical machine from the actual crime scene. After detail discussion and analysis a model is proposed in later part of this paper the author has proposed a model which can be used for collecting evidence from cloud environment.

Keywords: Cloud Forensics, Cloud infrastructure, Framework, F

1. Introduction

Information and Communications Technology (ICT) has been revolutionizing our life, society and especially the business world but has also invoked the matters of security both at national and international level. Developed countries have taken edge of IT tools in full swing and thus embracing the ongoing pace of the present era and the world. Moreover, it's certainly not wrong to say that with the advent of cloud computing in recent years ICT has been revolutionized by two folds, due to its overwhelming advantages and benefits. The operational costs of Traditional computing are quite low as compared to Cloud Computing thus provides a best fit model for small and medium-large enterprises and modified versions of Cloud Computing for Large and big organizations. Thus, giving today's business a handsome cut in Capital, Human Resource while taking advantage of Speed, agility, flexibility and most important mobility of services. It is been predicted that there will a steep rise in the adoption of cloud infrastructure. A research survey by Market Research Media that cloud computing is expected to grow at a compound annual rate of 30% reaching $270 Billion by 2020 (Zawaod and Hassan, 2013). This is also because of increase in demand for computing power and desire for maximum optimization of business resources. Another study shows that opting cloud models can save up to 37% costs in the business expenses. Though the list of advantages of cloud is near to endless but certainly there every benefit comes with a price and some factors on which one has to compromise one way or the other. When talking about cloud computing like any other network cyber infrastructure is not exempted from frequent attacks by hackers or cyber criminals, cloud infrastructure developments are prone

constant attack threats too. As the design and infrastructure of network has changed the way of attack by cyber criminals have changed too, and this has led to change in investigation methods as well. Cloud computing though might be tough target but once penetrated, all the businesses being hosted by Cloud Service Provider (CSP) is on stake and exposed to hackers. One of the major issues in cloud security is its undefined geographical boundaries as once it's up on the cyberspace, it is a potential target form many hackers.

Though aspect of cloud computing is alarming on other hand adoption of cloud services is increasing day by day by the business community, and this is happening just because there are many benefits of cloud services and it's in trend as well. But with this it also raises the questions on the security and threats that are being developed at CSPs. Though the best but still vulnerable to cyber hackers. Cloud cannot assure you the exact security of the implementation underlying. And there have been several cases where companies like Microsoft have been fell victim to it. Thus, raises a new challenge for post incidence investigations. Once the breach has been reported the role of forensics investigations comes into action (Nhien An Le Khac, 2019). With new technological advancements the ongoing techniques as used in Digital Forensics are also revived and needs to be changed. Digital Forensics as defined by (Kent et. Al, 2006) "The application of science to the identification, collection, examination, analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data". Digital Forensics can also be inferred as a branch of Forensic Science comprising of recovery and investigation of digital evidence found in digital device usually invoked against any crime.

Whereas, Cloud Forensics can be defined as the use of Digital Forensics in Cloud Computing. As per NIST definition "Cloud Computing Forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events. This is done through identification, collection, preservation, examination and interpretation and reporting of digital evidence" (M.E. Alex, 2017).

With such technological advancements it's important to revamp the traditional Digital Forensics Structure in alignment to Cloud Environment, so that the evidence collected, formulated and analyzed is admissible and acceptable in the court of Law, to ease and assist the jury to give verdict on it.

This paper focuses on the single step of evidence collection from the cloud environment at first part discusses the challenges faced by the Digital forensics investigation team. Further the article discusses the Kent model of digital forensics in particular to cloud environment. After discussing different aspects of the Kent model frame work in accordance with cloud computing the author has proposed a model to overcome which aims to minimize the challenges that are faced by the forensic team while collecting the evidence from cloud environment.

2. Problem Statement

Currently the frameworks that are in use have a lot of complex issues, like data duplication, multi tendency to handle data and the unusual architecture design, all these attributes add ups in difficulties of investigating team, and makes investigation process more challenging.

In addition to all these problems there is issue of standardization with respect to government policies and methodology that should be adopted for investigating the cloud infrastructure. The standards should be developed in such a way that ensure integrity, privacy and security of data, and services in case of any mishap (Brandao, 2019).

Considering the technical and legal issues current evidence gathering frameworks does not cater these issues efficiently therefore, it is necessary to come up with a framework which can cater these issue efficiently.

3. Literature Review

Hichman, 2019 discussed almost 9000 breach events over the period of 2005 to 2018 which includes 12 billion records. During the data analysis phase he had specifically taken care of privacy and had an opinion that though there is huge number of records to be analyzed but the factor of privacy cannot be ignored.

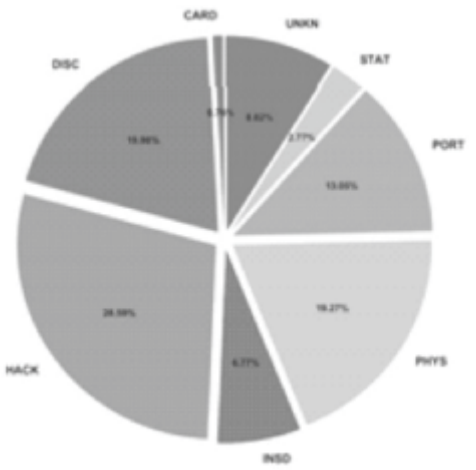


Fig 1. Breach type distribution
(Source: Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time)

Muhammad Tariq, 2013 reported several incidents that have taken place in recent years over the IT Infrastructure of Pakistan and in many cases, it remains unreported for years until and unless foreign Forensic Analyst intervened and reported the matter. Following table shows the data of websites hacked by foreign hackers.

Ser	Victim	Attacker	Date
1	20 websites hacked	Jagwar, India	26 Jan 2012
2	2000 websites hacked	Destroyer Army, India	15 Aug 2012
3	Google pk and 284 High Profile sites hacked	Eboz, Turkish	23 Nov 2012
4	250 Websites hacked	Indishel, India	8 Dec 2012
5	Punjab Assembly Website hacked	cr4ck-Br4in, Bangladesh	9 Dec 2012
6	60 website including gov pk and edu pk hacked	BGHH, Bangladesh	17 Dec 2012
7	Election Commission of Pakistan website hacked	NBOh7 F0x, India	29 Mar 2013
8	57 websites hacked	Afghan Cyber Army, Afghanistan	Jul-Aug 2013
9	Pakistan Army website hacked	GODZILLA, India	9 Aug 2013

Table I- Major Cyber Attacks on Pakistan
(Source: Cyber Threats and Incident Response Capability- A Case Study of Pakistan)

Further Cyber Espionage has also been an upcoming trend in the matter of national security where enemies are always looking for information and causing harm to national interests of the rival countries. As of evident from the major cyber espionage attack at public, private sector in 2009 which was reported by Norwegian Malware analysis in 2013 on request of Telenor Pakistan.

As far as cloud forensics is concerned; the challenges that are most important are related to architecture and technology, which needs to be addressed and there are different ways to addresse these challenges.

M. Yasar Arafat (2017) discusses the major challenges being faced by the Digital experts for collection of evidences from the inaccessible locations. He categorized the conventional Digital Forensic process in seven-step process 1) Identification 2) Collection 3) Preservation 4) Undertaking 5) Examination 6) Reporting 7) Close. Not only the process of Digital forensic are highlighted in his work, he has also highlighted the challenges that are faced by the expert in going through all these processes and has proposed solution for these challenges as well. Moreover, in his work he has also highlighted the scenarios of developed countries and their concerns about the growing cloud deployments and dealing with them.

Sheikh Khadar Manoj (2016) proposed a framework for the investigations of cloud deployed scenarios. He proposed the involvement of trusted third-party investigation team with computer forensics team to get assistance and to contact with them. He mainly focused on the validity and authority of the CSPs for integrity of data. The author uses Kent Model for evaluation of forensic activities in cloud.

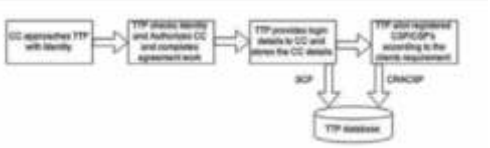


Fig 2. CC Registration Process with TTP
(Source: Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment)

Ameer pichan (2015) figured out Cloud Forensic process at three levels at following levels

1) Client Forensics: where artifacts for crime prints are being traced from client's machines.
2) Cloud Forensic: where evidences from CSPs are collected and are found in the form of Logs, and Authentication control
3) Network Forensic: traditional analysis of network where ISPs are involved and taken into account for any unusual behavior.

Emi Moroika (2016) proposed several possible solutions to overcome the challenges of cloud forensics at various level to collectively undertake cloud forensics. It also calls for a valid access to CSPs machines and have gain trust levels at their machines.

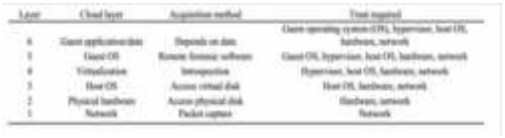


Fig 3: Trust Levels required at CSP by LEAs

Ben Matini (2012) though his work is bit old, but s proposed an effective solution for cloud forensics, and this is to use a framework which is blend of Kent and McKemmish conventional models to formulate a new methodology for the framework.

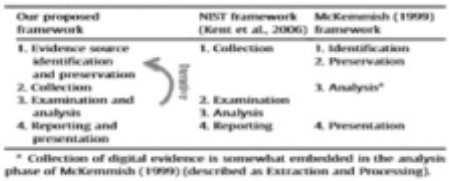


Fig 4: Proposed Framework by Matini 2012

Mark Scanlon (2016) proposed a solution to construct a solution by building a centralized DFaaS model by connecting the suspect device to forensic workstation using write blocker. This image is then stored to a device for later investigation.

Rahul Neware (2018) heighted multiple issues of cloud forensics. He has particularly showed concern over not having an appropriate tool for the cloud forensics. The other issues that have been focused in his write up includes Multi Tenancy, Volatile Data, Data Integrity, Evidence Correction.

4. DISCUSSION

The traditional Digital Models has been subject to wide discussions and several debates and discussions have been made in this regard, to evaluate each model in their particular area. Raza Monesari evaluates multiple models in his research and has concluded that computer forensics field triage model as the highest accepted model with in US Justice Department, with no or least errors being reported. But with these models physical evidence needs to be collected and taken into custody for further evaluation. But with Cloud Environment where data is scattered over multiple or beyond geographical locations traditional models needs to be extended and certain amount of support needs to be given in order to make evidence admissible and fruitful.

US state department conventionally follows Daubert Test in regard to evidence presentation in the court of law.

5. PROPOSED MODEL

The conventional methods as being proposed by many researches have limited applications on cloud environment. This model makes extension and blends concept of conventional Digital Forensics and Cloud Forensic to ensure the authenticity of evidence generated through. Along with this distributed nature of cloud also raises the need of third-party involvement to ensure proper standards as per laws and implicit implications of the SOPs over the CSPs. A new entity of Trusted Third Party needs to be introduced with in the geographical and Law Operational area of Cloud Customer where he needs to get himself registered with TTP before making any arrangements with Cloud Service Providers.

A. Registering With TTP

It should be made compulsory that any Cloud Service Seeker needs to get registered himself with TTP to ensure integrity of the CSP. The Government might setup such TTPs on their behalf to evaluate the workings of Organizational T&C and SLAs with CSPs.

B. Tracking of CC Data Activities

The TTP will keep track of all the important activities of CC in following two ways

1- Database Behavior
2- Log Database

This will ensure the maintaince of data in parallel with CSP and at local level as well. In case of any breach at CSP the TTP will be in a position to assist the Forensic Team at their level. Any incident reported at any level can be traced back with help of TTP tracking of Data.

Fig 5: Evidence Collection Proposed Framework

Data from real time environment of database is fed in to TTP monitoring layer to check for any out of behavior / anomaly data. This data is then further checked with Rules Management engine to check duly processed integrity of data. Output from behavior layer is further processed to Time Stamp for any further time stamping of the data.

Behavioral Database

Behavioral data is generated in response to CC engagement with business. Database behavior can be generated based upon the type of interaction a consumer is making with the cloud and thus can be of various benefit to the forensic expert. Based upon the data collected two types of behaviors can be inferred from it.

1) Rules inference: Any data that has been processed needs to pass some rules or privileges of the constraints applied before.
2) Monitoring: Data can be matched with monitored data base upon the rules applied earlier.

Log Database

1) Time Stamped: Any data / activity processed needs to be time stamped and has to be matched as per record.
2) Log Analysis: Any activity that fails to map with certain log entries or any log against that particular event is missing the entry will be considered fraudulent.

6. FUTURE WORK

Logs can be used in multiple scenarios, considering this, adoption techniques like machine learning can also be applied to enable the machines to learn and recognize patterns in evidence collection. Thus Evidence can be clustered and can be linked with any event that took place in past.
The model can also be made part of CSPs where each CSP can maintain record of each CC in separate apart from conventional methods and thus can extend its service as FaaS (Forensic as a Service) to other Cloud Service Providers.

7. CONCLUSION

Though many frameworks have been proposed and many framework will be proposed in future too, but the author believes that there should be a framework which should at least cater the challenges which author has presented, and has evidently proved from the work of different researchers that they have faced these challenges too, its just because this part of digital forensics investigation has still grey area, which needs to be properly figured out. Not only this but author believes that the solution should be a standardize solution, as there are set standards for computer forensics. In this regard author has proposed a model in this paper which has been designed specifically to address the challenges that are faced by the forensics expert and the investigator in conducting investigation on cloud platforms.

8. Referances

[1] Arafat, M. Y. (2017). Technical Challenges of Cloud Forensics and Suggested Solutions . International Journal of Scientific & Engineering Research.

[2] Brandao, P. R. (2019). Forensics and Digital Criminal Investigation Challenges in Cloud Computing and Virtualization. American Journal of Networks and Communications, 23-31.

[3] Gayatri S Pandi, D. K. (2018). CLOUD FORENSIC FRAMEWORKS, CHALLENGES,STATE OF ART AND FUTURE DIRECTIONS. Journal of Emerging Technologies and Innovative Research (JETIR), 712-721.

[4] Hammouchi, H. (2019). Digging Deeper into Data Breaches: An Exploratory Data Analysisof Hacking Breaches Over Time. procediaInternational Symposium on Machine Learning and Big Data Analytics for Cybersecurity andPrivacy .

[5] James, M. (2017). Jurisdictional Issues in Cloud Forensics. Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance .

[6] M.E. Alex, R. K. (2017). Forensics framework for cloud computing. Computers and Electrical Engineering, 193-205.

[7] Manoj, S. K. (2016). Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. International Conference on Computational Modeling and Security .

[8] Mantini, B. (2012). An integerated conceptual digital forensic framework for cloud computing. ELSEVIER.

[9] Martini, B. (2012). An Integratd Conceptual DF Framework for cloud computin. Digital Investigaion.

[10] Morioka, E. (2015). Cloud Computing: Digital Forensic Solutions. International Conference on Information Technology .

[11] Morioka, E. (2016). Cloud Computing: Digital Forensic Solutions . 12th International Conference on Information Technology - New Generations.

[12] Neware, R. (2018). Cloud Computing Digital Forensic challenges. International conference on Electronics, Communication and Aerospace Technology .

[13] Nhien➥An Le➥Khac, S. S. (2019). Security, Privacy, and Digital Forensics in the Cloud. Wiley.

[14] Picha, A. (2015). Cloud Forensics : Technical Challanges and Solutions. Digital Investigaions.

[15] Pichan, A. (2015). Cloud Forensics: Tehcnical Challaneges, soulutins and comparitive analysis. ELSEIVER.

[16] Ruwan, L. (n.d.). Cloud Forensics: An Overview. 2011.

[17] Sangho Park, Y. K. (2018). Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment. Sustainability, 1-24.

[18] Scanlon, M. (2016). Battling the Digital Forensic Backlog through Data Deduplication. Sixth internatonal Conference Innovative computing Technologies.

[19] Simou, S. (n.d.). Cloud Forensics: Identifying the Major Issues and Challenges . 2014.

[20] Simou1, S. (2015). Cloud Forensics: Identifying the Major Issues and Challenges .

[21] Tari, M. (2013). Cyber Threats and Incident Response Capability- A Case Study of Pakistan . 2nd National Conference on Information Assurance (NCIA).

[22] Zareen, M. S. (2013). Digital Forensics: Latest Challenges and Response.

Khan et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 4, Oct. - Dec. 2019

Cyber-Security Threats with Machine and Deep Learning

Rafaqat Alam Khan
Rafaqatalam@lgu.edu.pk
Lahore Garrison University

Abstract:

Machine learning can play vital role in cyber-security for the detection of an anomaly, risk analysis, and antimalware detection. The role of machine learning for privileged users in term of risk context is giving better precision through enabling of threat analytics. They are capable to generate real time risk activity notification and also have the capability of robustness against different cutting off sessions. They also add up other features including flagging and monitoring for further forensics follow-up. This paper gives an overview of how machine learning tools can be used to immediately identify the threat or attack associated with the system and instantly notified about the severity of the risk to the concerned user or administrator. The conclusion of this paper would be on the basis of extensive literature review and the different machine and deep learning techniques applied in cyber-security domain.

Keywords: Cyber-Security, Machine Learning, Deep Learning, Forensic

1. Introduction

The demand and usage of ML in a different walk of life is increasing day by day. The different techniques of machine learning addressing real issues are improving and their effectiveness is appreciated. The increasing demand for the adoption of machine learning has led them to their achievement in several domains. These domains compromise medical imaging [1], social marketing [2], computer vision [3] and gaming [4]. Though achieving a complete automated cyber defense system is an objective that is yet to be achieved. However, detection and analysis on the basis of machine learning tools one can benefit and operate on network and security operation centers.

This study analyzed the review literature and different real-time experiments performed on real large enterprise networks. The different surveys [5-10], that described the different machine learning approaches performed in the cyber-security field.

2. Machine Learning Categorization for Cyber Security

ML algorithms are divided into two main categorize for cyber-security. These two main categorize are namely shallow learning and deep learning. The two main categories are explained below.

2.1 Shallow Learning:

The traditional machine learning algorithms are known as shadow learning. These shallow learning algorithms for execution required engineered features from relevant data. The shallow learning algorithms are further divided into two main categorize i.e. supervised and unsupervised learning. Supervised learning required a pre-labeled training dataset while on the other hand unsupervised did not require. Supervised learning is composed of different machine learning algorithms namely Naïve Bayes, Logistic Regression, Support Vector Machine, Random Forest, Hidden Markov Models, K-Nearest Neighbors, and Shallow Neural Network. On the other hand

unsupervised machine learning algorithms in accordance with shallow learning are divided into two main classes i.e. clustering and association.

2.2 Deep Learning:

The recent advancement as compared to shallow learning in the field of machine learning is known as deep learning. Deep learning extract features automatically from the input data as compared to shallow learning which required domain expert i.e. engineered features. Deep learning is also divided into two main categorize i.e. supervised and unsupervised algorithms. Supervised learning has different machine learning algorithms such as fully connected feed-forward deep neural networks, convolution feed-forward deep neural networks and recurrent deep neural networks. Unsupervised learning algorithms are of two types i.e. stacked auto-encoders and deep belief networks.
Supervised deep learning algorithms are briefly discussed below.

► Fully Connect Feed Forward Deep Neural Networks

This type of DNN architecture works as that every neuron is connected to every neuron in previous layers. The computational cost for these deep neural networks is quietly high as there is no compromise or assumption on the input data given to the network. A fully connected feed-forward deep neural network is used by the study for malware analysis [11].

► Convolution Feed Forward Deep Neural Networks

This type of DNN works on the basis, in which every neuron depends on the subsets of different neurons in the previous layers. They performed very well on spatial data but their performance degraded when applied to non-spatial data. They have less computational power as compared to that of fully connected feed-forward deep neural networks. Convolution feed-forward deep neural network is used by the study for malware analysis [12].

► Recurrent Deep Neural Networks

This type of DNN working is such that output at each neuron can propagate its output to the neuron in previous layers. The training of such networks is quite difficult as compared to the other variants and they also work as a long short term memory as they are sequence generators. A recurrent deep neural network is used by different studies for the detection of intrusion [13-14] and malware analysis [15].
Unsupervised deep learning algorithms are of two types and are discussed below.

► Deep Belief Networks

This type of DNN has no output layer and is made up of restricted Boltzmann machines. They performed really well in pre-trained tasks because of their role in feature extraction function, but the data provided in that case is unlabelled data. The study shows an application of deep belief network for cyber-security in terms of intrusion detection [16], malware analysis [17] and spam detection [18].

► Stacked Auto-Encoders

In this type of DNN, the number of inputs to the network is the same as that of its outputs. They are composed of multiple encoders. Their training is the same as that of deep belief network but they performed well on smaller datasets. Studies show the application of stacked auto-encoders for intrusion detection [19], malware analysis [20] and spam detection [21].

3. Machine Learning Relevancy for Cyber Security

The relevancies of machine learning algorithms in accordance with cyber-security are in terms of spam detection, malware analysis, and intrusion detection.

► Spam Detection

Spam and phishing detection composed of different automatic machine learning techniques that reduce the waste of time and secondly security against unwanted emails. Machine learning approaches can improve the detection capability of spam detection. Spamming and phishing detection process is becoming very difficult as hackers are capable of bypassing traditional filters.

► Malware Analysis

The traditional rule-based approaches used for the detection of malware analysis fails because of the polymorphic and metamorphic capability of malware. Machine learning techniques can solve this problem for the detection of different variants of malware.

► Intrusion Detection

Intrusion detection systems (IDS) are mostly deployed in modern enterprise networks. These IDS work on the basis of know patter detection that is used for an attack within a computer or network. Nowadays different machine learning approaches are used for IDS. IDS are broadly divided into two main categories i.e. Botnets and domain generation algorithms.

4. Results and Discussion

This section discussed the current state of the art studies conducted so far in the field of cyber-security using the machine and deep learning. The study result shows that so far there is no fully automatic machine learning method available without manual intervention of the human. The common evaluation metrics used for classification are F1 Score, Recall and Precision. As in computer vision, deep learning outperforms shallow learning, but it is not the case in cyber-security. In cyber-security, the study shows [22] that the results obtained for shallow learning are better than that of using deep learning. The results are obtained through different evaluation metrics i.e. F1-score, Precision, and Recall. The results of random forest (SL) and fully connected feed-forward deep neural network (DL) are Fl-score [0.7985, 0.6085], Precision [0.8727, 0.7708] and Recall [0.736, 0.5027] respectively. So in case of cyber-security random forest results are better compared to deep learning when applied on the same dataset given in table 1. The other important point for consideration that can affect the results is the selection of features. Random forest classifier is applied to the same dataset as mentioned earlier by selecting different features from the dataset through the feature agglomeration process. The different features i.e. 5, 7, 10 and 12 on which random forest classifier is applied yields different results. The results obtained for recall through 12 features are quite better i.e. for 5 features recall value is 0.5734 and for 12 features its value is 0.7361. This shows that the selection of appropriate data can affect the results of different techniques.

Table1. Training Dataset for Intrusion Detection

Dataset	Benign Flows	Malicious Flows
1	100000	1000
2	250000	2500
3	500000	5000

5. Conclusion

The usage of machine learning approaches in different domain and applications are increasing with the passage of time. This increasing demand for machine learning is nowadays adopted for cyber-security. Analysis of these machine learning approaches can be applied to the different fields of cyber-security and these are namely spamming, malware analysis and intrusion detection. This study discusses the recent trend of different machine learning algorithms that are applied in the field of cyber-security. The different parameters are discussed that how these parameters can affect the performance of these machine learning approaches in the cyber-security domain. The results of different experiments performed by the researchers have certain kinds of limitations and those limitations, in turn, affect the cyber-security effectiveness. With the introduction of deep learning, a subcategory of machine learning can significantly improve the shortcomings of machine learning approaches. The outcome of this research base study is that machine learning approaches can automate the process of cyber-security, having pros and cons must be known. The main advantage of machine learning approaches is that it can automate the process and inhuman absence it can get rid of stealth of data, infiltration of attackers and last and the least enterprise sabotage.

6. References

[1] "Machine Learning in Medical Imaging," in IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 4, pp. 1361-1362, July 2019. doi:

10.1109/JBHI.2019.2920801.

[2] L. Deng and J. Gao, "An advertising analytics framework using social network big data," 2015 5th International Conference on Information Science and Technology (ICIST), Changsha, 2015, pp. 470-475. doi: 10.1109/ICIST.2015.7289018.

[3] S. M. S. Islam, S. Rahman, M. M. Rahman, E. K. Dey and M. Shoyaib, "Application of deep learning to computer vision: A comprehensive study," 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV), Dhaka, 2016, pp. 592-597.

[4] N. Justesen, P. Bontrager, J. Togelius and S. Risi, "Deep Learning for Video Game Playing," in IEEE Transactions on Games. doi: 10.1109/TG.2019.2896986.

[5] Torres, J.M.; Comesaña, C.I.; García-Nieto, P.J. Machine learning techniques applied to cybersecurity. Int. J.Mach. Learn. Cybern. 2019, 1–14

[6] Wu, S.X.; Banzhaf, W. The use of computational intelligence in intrusion detection systems: A review.Appl. Soft Comput. 2010, 10, 1–35.

[7] Sperotto, A.; Schaffrath, G.; Sadre, R.; Morariu, C.; Pras, A.; Stiller,B. "An overview of IP flow-based intrusion detection". IEEE Commun. Surv. Tutor. 2010, 12, 343–356.

[8] Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá -Fernández, G.; Vá zquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur. 2009, 28, 18–28.

[9] Nguyen, T.T.T.; Armitage, G. A survey of techniques for internet traffic classification using machine learning. IEEE Commun. Surv. Tutor. 2008, 10, 56–76.

[10] Buczak, L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security. IEEE Commun. Surv. Tutor. 2016, 18, 1153–1176.

[11] G. E. Dahl, J. W. Stokes, L. Deng, and D. Yu, “Large-scale malware classification using random projections and neural networks,” in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2013.

[12] G. D. Hill and X. J. Bellekens, “Deep Learning Based Cryptographic Primitive Classification,” arXiv preprint, 2017.

[13] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, “Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection,” in IEEE International Conference on Platform Technology and Service (PlatCon), 2016.

[14] P. Torres, C. Catania, S. Garcia, and C. G. Garino, “An analysis of Recurrent Neural Networks for Botnet detection behavior,” in IEEE Biennial Congress of Argentina (ARGENCON), 2016.

[15] R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, “Malware classification with recurrent networks,” in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2015.

[16] M.Z.Alom, V. Bontupalli, and T. M. Taha, “Intrusion detection using deep belief networks,” in IEEE National Aerospace and Electronics Conference (NAECON), 2015.

[17] Y. Li, R. Ma, and R. Jiao, “A hybrid malicious code detection method based on deep learning,” International Journal of Security and Its Applications, 2015.

[18] G. Tzortzis and A. Likas, “Deep belief networks for spam filtering,” in IEEE International Conference on Tools with Artificial Intelligence (ICTAI), 2007.

[19] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), 2016.

[20] W. Hardy, L. Chen, S. Hou, Y. Ye, and X. Li, “DL4MD: A Deep Learning Framework for Intelligent Malware Detection,” in International Conference on Data Mining (DMIN), 2016.

[21] G. Mi, Y. Gao, and Y. Tan, “Apply stacked auto-encoder to spam detection,” in International Conference in Swarm Intelligence, 2015.

[22] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 2018, pp. 371-390.

Khan et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 4, Oct. - Dec. 2019

Aspects of White Collar Crime

Syeda Marrium Nizami[1], Gulfraz Naqvi[2], Tayyaba Sultana[3]

Marium002@yahoo.com[1], gulfaraz.naqvi@gmail.com[2], tayyabasultana@gmail.com, tayyabasultana@gmail.com[3]

Lahore Garrison University

Abstract:

White-Collar crime is committed for centuries in world. It is not restricted in an area or country. It is a word wide issue that is increasing day by day with different means. White Collar Crime is included in daily NEWS but the agenda or the ways of committing is different every time. White Collar Crime is such a crime that is not only done by poor or needy people this crime is also done by rich people who have lust for money, or may be by young generation for the sake of fun or to tease someone, because there is no hard and fast rule or punishment for White Collar Criminals. This article describes White Collar Crime in simple terms by giving an over view on the prospective of different researchers. These researchers gave a new angle to white collar crime. Then the fraud triangle is described briefly which provides the reader with another angle of White collar crime.

Keywords: White Collar Crime, Fraud, Cheat, Tricky, Money, Victim, fool, innocent people.

1. Introduction

The white collar crime is a wide variety of offences. White collar fraud may identify various types of crimes, but they are usually all linked to crime committed through dishonest and financially beneficial activity. [1] Frequent white collar crime includes bribery, speculation, tax evasion and money laundering. There are many types of swindles and scams which are part of white collar crimes, including Ponzi schemes and secret services. The White Collar Crime also includes insurance frustration, tax evasion and other typical crimes.[2] Various scholars had different views on white collar crime. Sutherland was the first person to research and write a report on white collar crime, expanding the justice sector to study more than just traffic violence. [3] He has been researching the behaviour of 70 large US corporations and 15 utility companies for decades. He coined the term' white collar crime' in 1939, as he recognized that the violence was not limited to the streets of the city. Sutherland needed people to understand that even well trained and trusted people commit violence when they were creating the definition of white collar crime. [4] The sociologist and professor Edwin Sutherland was from the 20th century, whose doctorate in sociology was received by Chicago University in 1913.Most of his life has been learned and criminal behaviour philosophy developed by Sutherland.[5] .

2. Edwin Sutherland's view on White Collar Crime

Edwin Sutherland clearly defines the concept of white collar crime. He stated that white collar crime can be defined in different ways, but in general it is a crime of financial gain-motivated mistake. It is usually committed by a strong social standing and respectable individual.[6-7]. While these crimes of frustration are not what society calls violent crime, they can destroy lives. The US pays 300 trillion dollars worldwide for white collar crimes. And if a company loses revenue because of activities such as theft, it must somehow make up for its costs. Generally, work terminations, lower wages and/or price rises for goods and services are terminated. In other words, harm caused by

white collar crime always has a spinning impact. Top executives are not only affected but other employees in all layers of the organization are affected.[8]

2.1. Criticism on Edwin Sutherlands view on White Collar Crime

Theft has been a criticism from certain sources, in Sutherland's interpretation of white collar. Coleman and Moynihan the popular researchers pointed out that Sutherland's description of white collar crime was most problematic because of the lack of certain requirements for assessing men of respectability and status.' The Sutherland's significance is likely to be the lack of convictions for offences other than offenses with white collar. There is ambiguity also with the dimension of' high social status' used in the definition: it simply has a far narrower sense in ordinary use than that word. Commenting on this argument, Tappan a researcher argues that it is necessary to treat white collar criminals as criminals in that the moral interest of the administrator's actions is largely reinforced by the precise nature and consistency of legal provisions in the decision-making process. [9] . Nevertheless, Sutherland defends a special procedure of administrative agencies for the conviction of white collar criminals on the basis that it would protect the defendant from the court prejudice. A further critique of the concept of white collar crime by Sutherland is that it encompasses even such violations of law that are not committed in a career and are not usually perpetrated by the highest classes of society. Tax evasion, for example, is not only performed by people of high standing, but also by individuals belonging to the middle and even lower strata. Another argument against the concept of white collar crime is that mens rea, an essential component of the crime, does not necessarily require it. The mens rea doctrine based on common law does not extend to civil offences in India and the presumption of guilt mind can either be explicitly or implicitly omitted in such cases.[10] .

2.2. A Presumption of Guilt

Sutherland is relying on the argument that the presumption of innocence in criminal proceedings systematically deprives the convicted and the individual defendants. Nevertheless, nearly all legal and administrative lawsuits are his industry manifestations rather than actual criminal prosecutions. Sutherland can combine all enforcement efforts with criminal prosecution, even when no crime has ever been committed by a lack of substantial legal education (such as civil suits or settlement agreements). [11] For Sutherland there is no proof of business wrongdoing. He defends his mislabeling by claiming that the strong are favored in the legal system despite the lack of immunity from criminal proceedings that he respects and enjoys. Sutherland aimed to facilitate more convictions by re-conceiving crime with the term "white-collar crime" and initiated a match between regulatory agencies ' "adverse decisions" and criminal convictions.[12] Sutherland wanted to stress the presumption of innocence and the need to make the assessment of criminal liability easier for people involved in business. But Professor Sutherland also called an offense a regulatory infringement. Intention in such enforcement action is usually not taken into account, so many of the "crimes" of Sutherland might have been inadvertent and accidental. Sutherland was nevertheless sure that such activities be marked as offences. Within modern federal criminal procedure, the presence of Sutherland is evident. Instead of real crimes, many federal offenses prosecuted on the "white collar crime" label are regulatory or public welfare offenses. The founding architect in the United States Professor Sutherland's ' social science ' study, among others, clarified the need for guidance, i.e. "evidences of preferentiality for the white collar prisoner," were referenced in the sentencing guidelines of the Commission on prosecutions organizations.[13] .

2.3. About Crime

Sometimes people are tired with legal niceties if they are persuaded that an individual or class of individuals is guilty of a crime.[14] For the sake of other corporate cultures, Sutherland and others believe that common law protections must not extend to business people. However, in support of corporate defendants, civil-libertarian uproar is most possible. Professor Sutherland has dispensed with the basic (and often difficult to prove) aspects of wrongdoing and that those who are engaging in industry do not deserve the presumption of innocence culprit. While removing the presumption of innocence would be unconstitutional,

Sutherland is trying to avoid this by reducing the psychological condition.[15] .

By following his view that the law disproportionately stigmatizes the rich and powerful the poor, Sutherland has ignored the most fundamental principles of criminal law. Sutherland has not attempted to remove the stigma of crime (but ideally this aim should be accomplished by dispensing with the motive requirement).[16] He tried to expand it, instead. To pursuit of improved equity, the definition of "white collar crime" meant that the stigma of violence against a large part of the industrialized Americas had been introduced. Nevertheless, the rule of law demands that objective tests assess the guilt of the perpetrator until society stigmatizes and punishes the criminal defendant. Although it may be wished by some scholars, being rich or powerful is not a felony. In ignoring the culpability, Sutherland attempted to apply the stigma of criminal convictions usually in a non-criminal regulatory proceeding to business people and companies. But it is also likely that ambiguity proved that there was no criminal behavior in a particular case. [17] If the attorneys investigate federal crimes against the companies or their employees, comfortable evidence of motive leads to arrests where proven wrongdoing is "blurred and concealed." To Sutherland's view this conventional defense is an antiquated ethnicity. [18]The presumption of criminality historically, and for good reasons, often applies to those who have proven that they were "morally responsible" by doing so with the guilty mindset. [19]Alternatively, blame must include an externalized criterion that specifies whether the actions of the criminal breach the people's "moral feelings."[20] .

2.4. White-Collar's Sociological Echoes Today

In focusing on companies and individuals in the high social and economic classes, Sutherland and his predecessors have expanded the scope of criminality dramatically. A Sutherland lawyer-sociologist, Paul W. Tappan, has long pointed out that the definition of crime in Sutherland is different from that in law. According to Tappan, the concept of' white-collar crime' by Professor Sutherland involves "a boor, a sinner, a religious leper or a demon represented, and it doesn't become a crime by the sociological name of the person.' Tappan accused Professor Sutherland of this creation.[21] .

The phrase "corruption on the white collar" has grown to include such a variety of offenses that it is too amorphous for study. Some sociologists have "decreased the offender's class into an item," and even Sutherland's very vague definition of "too restrictive." Thus," White-collar "crime has become a corporate crime category. One is the Department of Justice, which is pressuring businesses, as a condition of pleading culpable, to waive their right from self-incrimination. Sutherland' s argument that "white collar" suspects do not have the same legal protections for other offenders, is in keeping with this emerging trend. This is sociological. Recently and rather interestingly, in recommending that the Commission on Sentencing ignore deviations from the criteria for the punishment of "white collar criminal offenders who usually have skilled lawyers," it followed a largely class based approach to the rule.[22] .

3. The prospective of FBI on White Collar Crime

A scam could destroy a company; devastate families, or save investors trillions of dollars for their life. Fraud is today more complex than ever and we are dedicated to finding the guilty and stopping scams before they begin. [23]

"White collar crime" is considered a "work, fraud, and burglary" by the Federal Bureau of Investigation (FBI). That's a white collar nutshell crime, says the FBI. The term was presumably coined by professionals and government employees in 1939 and is today synonymous with an enormous range of frauds and frauds frequently committed by white collar professionals. Crimes of white collars are not, however, usually violent. This crime can destroy a family's income, cost taxpayers billions of dollars, and ruin a good loan ranking. Today, the abuse of white collars is more complicated than ever with electronic technological breakthroughs. The FBI says the US has more than $300 billion in white collar crime. Although people caught up against a host of sanctions, firms can also be punished.

White collar sentences include financial penalties, confiscations, fines, detention in state or federal custody, etc. Various types of theft and deception are known as a white collar crime and here are a few common examples:

3.1. Bribery

Bribery is an act of demanding money or other mental analysis under threat to do physical abuse, to damage wealth, to fault of a offence against the law, or to disclose unrevealed secrets. Duplication is an act that happen when someone clones something without permission of that and using the fake copy of original thing. Duplication is usually related to the finance but it can also be linked with branded products.

3.2. Credit Card Trickery and Computer Trickery

Credit Card Trickery is an act, when an unauthorized person permitted use of a credit card to buy valuable goods or can be used for wrong means too. Computer Trickery is an act of fraud done by the computer hackers who steal personal important information from personal computer. The data can be personal data, pictures, confidential data of any organization, information of bank credit cards etc.

3.3. Currency Arrangement

Currency arrangement is an act of thinking about deeply and theorizes on the future value of currencies. This can cause big loss to the currency.

3.4. Embezzle

Embezzle is done by a person who has given custody with the theft assets or money appropriates that assets. This act is done for some specific purpose that may benefit that person but harm others.

3.5. Environmental Tactics

Environmental Tactics is the most common white collar crime committed by almost every big firm. The practices or act of overbilling and deceptive done by huge organizations which implicit to clean up the environment.

3.6. Extortion

Extortion is an act of obtaining someone's personal property illegally by applying force, violence, use of intimidation, fear, blackmail or threat.

3.7. Counterfeiting

Counterfeiting is an act that involves in cheating for example using of using of false instruments like check that does not belong to you but you withdraws money. This act can badly harm a person financially.

3.8. Health Care Trickery

Health Care Trickery is a very dangerous white collar crime that can directly affect to a person's life. Health Care Trickery is done by false doctors and Health Care centers who are unlicensed but some service providers issues them false license, in return they demand large amount of money from the owner.

3.9. Insider business

Insider business is an act done by people classified in order to do business in shares of candidly held association.

3.10. Insurance trickery

Insurance trickery is an act done by the people associated with the insurance companies. Such frauds get profit from organizations providing insurance through misleading.

3.11. Investment Strategy

Investment Strategy is an act done by fraud people who commit false promises to return a large amount of money from a small investment.

3.12. Kickback

Kickback is an act that occurs when a buyer is paid a big part of the purchased money by the seller.

3.13. Crime of theft or steal

Larceny is an act that is done by a false person who illegally takes someone's property or money in order to theft it.

3.14. Black Money

The financing or transferring of money from racketeering, illegal drug business or other embezzlement systems, that it seems its real source either cannot be sketched or is authentic.

3.15. Racketeering

Racketeering is an act of establishing a business that is illegal for someone's own benefit.

3.16. Security Trickery

Securities Trickery is an act of unnaturally blowing up the rates of goods by stockbrokers so that the costumer can buy a stock on the rise.

3.17. Income tax Avoidance

Tax Avoidance is an act done by the people who do not pay the taxes to the government. This act is a big loss for the government of such country. Taxes are very important to be paid, and paid on time.

3.18. Telemarketing Trickery

Frauds arrange secret rooms and give telephonic calls to the innocent people and organizations. The Frauds ask charity to an asserted generous corporation where Fraud ask for the money or for the credit card number but unfortunately does not use the charity fund for the purpose they asked money for.

3.19. Welfare Trickery

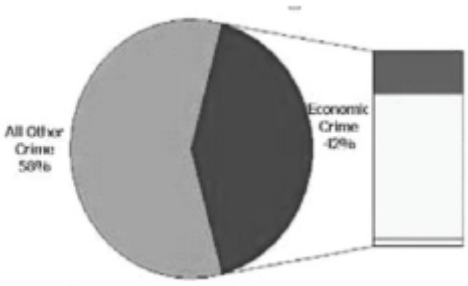
Welfare Trickery is an act of indulging in an activity where the aim is to get profit from the government of such country.

4. Federal offenses and White Collar Crime

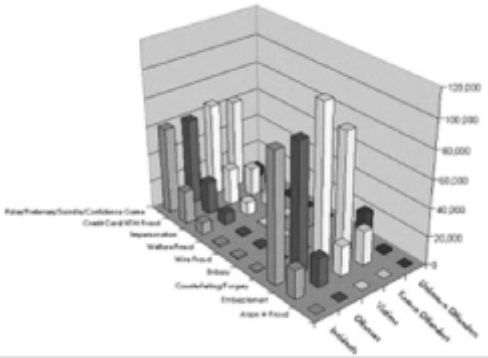
Based on State or Federal law or both, white collar crimes can be criminalized. Where the offense violates federal and state law, it is for the State and federal authorities to determine whether a state or a federal trial should be carried out. As a general rule, more penalties and longer prisons are imposed on federal crimes than on state crimes. Therefore, the situation is certainly more serious if your case goes to federal court. An expert Plano white collar criminal defense lawyer at the Zendeh Del Law Firm, PLLC, will clarify which of the protections are available if you're faced with criminal accused of a white collar crime. [24] .

5. FBI report on White Collar Crime

A survey conducted in the National Incident Reporting System (NIBRS) collection, the Federal Bureau of Investigation today released The Measurement of White-Collar Crime Using Uniform Crime Reporting Statistics (UCR). [25]Crime committed in his profession by a person of respectability and high social status, "accounted for 4% of the crimes reported in white-collar crime taken from NIBRS statistics. Four percent of all NIBRS arrests have been arrested for wrongdoing. Most white-collar criminals have been contacted, and are typically white men between the late 20s and the early 30s.[26].



The data element that notes the criminal has been suspected of using a computer or computer equipment for the crime can be extracted from computer crime, or techno-crimism, by NIBRS. [27] The NIBRS data show that 42% of code crimes concern white-collar crime. The larceny-theft crime accounts for the greatest number of these crimes.[28] The white-collar crime reflects, as opposed to other property crime cases, on average more dollar damages per occurrence, as shown in the figure above. The bulk of white-collar crime occurs in public areas, except wire fraud. The ability to collect information about non-personal individuals who are victims of crime is special to NIBRS. This is especially helpful in the context of white-collar crime, where NIBRS data show that companies are as likely to be victims as individuals. NIBRS provides information on incidents, crimes, vs. limited data previously available on white collar crime [29] .



6. Reasons of committing white collar crime

There are a few reasons why people make white-collar crimes. Financial gain is the primary motivator for these crimes. The search for influence and power is another matter. A crime of a white collar is a non-violent offense which needs some privilege on the part of the offender. It is better to know why people commit these crimes than to understand why. The level of privilege required for the offense of white collar distinguishes white collar crime from other forms of criminality. Many offences can be done by everyone, such as robbery and assault. In comparison, offences such as mistreatment and corporate fraud may only be committed when the perpetrator has access to certain financial and private records.[30] .

7. Motivations for White-Collar Crimes

Usually financial gains are the principal reasons for white collar crime. But if you really want to understand why people commit crime, the psychology which drives people to ignore morality and violate the law must be understood. Psychological justification for white-collar offences includes:

- Neglecting business Laws and rules.
- The craving that the decisions do not have a sufficiently significant impact.
- The feeling of not being caught because he's anonymous.
- The conviction that everyone engages in certain behaviours in the same industry, making them acceptable
- A sense of inventiveness because of career success.

The believe that the acts can be socially justified, such as being treated for what believes are immoral behaviour on the part of the victim as a valid retribution.A person can act by himself, or can work with a white collar crime with part of a group. A person convicted of this type of crime may face imprisonment, house arrest, penalties, restitution, the loss of business licenses or community service, depending on the offense.[31] .

7.1. Offenders of White-Collar

By fact, white-collar crimes are committed by offices with supervisors, consultants and contractors, hence the word white-collar. A white-collar criminal is typically a citizen with a bachelor's degree at least and a healthy, secure income. Persons in both the public and private sectors are responsible for the crimes committed in white collars. Amongst such criminals are judges, accountants, business vendors, financial advisers, professors of higher education and even clergy.

8. Theory of Fraud Triangle

The Fraud triangle is considered as a reflection of the structural foundation innate to a variety of fraud offenses within the field of investigation and analysis on fraud, which is defined as a criminal activity involving the deliberate and deliberate disappointment of other individuals in relation to their receive of financial gains.[32] The Fraud Triangle is a diagram that is implemented in a fraud analysis that represents fraudulent activity based on three components, these are the possibility, the rationalization and the pressure a common approach states in the analysis of the Fraud Triangle that the deletion of one or more of these components will be a deterrent for fraudulent activity.[33].

8.1. The Components of the Fraud Triangle

Three separate methodologies and ideologies within the three components of the Fraud Triangle are deemed contributing and inheriting to the bulk of fraud offenses.

Fig: This figure contains a brief description of the methodologies of Fraud Triangle.

8.2. Opportunity

In fact, the suspect targets persons believed to be vulnerable or outstanding for fraudulent activity; as a result, the "opportunity" is an aspect of the fraud triangle took place. Solicitation is an indirect, non-physical criminal offense involving a crime convict who gives another person or individuals, the possibility of a fraudulent opportunity to commit. A plan includes fraudulently giving out money to project the illusion of financial gains from investment projects unlawfully and disappointingly. A scam is an illegal, exhausting and organized scheme for deliberate defrauding the participants. [34]

8.3. Rationalization

Rationalization is the second step in the course of Fraud Triangle events. Following a successful request process, the offender usually seeks, through disappointment and misrepresentation, to instill a false sense of confidence and confidentiality within a victim. There is some common place in this aspect of the Fraud Triangle like misrepresentation. Misrepresentation is an act of presenting information which is considered fallacious and misleading in character. The reported false reports include fraudulent income, not only proliferating further investment but also drawing new investors eager to take part in the alleged said by albeit fraudulent on financial gains.

8.4. Pressure

The principle of intimidation is both perceived to be the final component of the Fraud Triangle and to be a key component of the fraud; the use of high-pressure manipulation techniques avoids a proper analysis and the use of an impulsive agreement to a situation. Within this portion of the Fraud Triangle, a high-pressure application process is commonly described as "pushy" and "bullying." [35]

9. Conclusion

White collar crimes are committed every year. Sometimes the perpetrator is discovered. Other times, such actions go undetected. In other cases, the defendant may be targeted by someone who actually committed the crime and is trying to avoid detection. White Collar Crimes is committed from ages in world but as there is no proper cat of law or punishment, people take this crime easy. Another issue with White Collar Crime is that people do not have the awareness. Not only the fraud but the victim is also unaware that the fraud happened to him is a crime and some serious action is to be taken against it, otherwise this act will be repeated by the fraud with the other innocent people.

10. References

[1] Liu, 'Rents for City's Cage Homes Rising.' South China Morning Post, 2010, April 28.

[2] Leung, 'Stifling Heat Piles on Misery in Cage Homes.' South China Morning Post, (2010), August

[3] Ng, 'Cage Homes Fuel Tuberculosis in Sham Shui Po.' South China Morning Post, 2011, August

[4] Chiu, Karen. (2014). 'HK Homes Still Least Affordable.' The Standard, January 22. http://www.thestandard.com.hk/news_detail.asp?pp_cat=1&art_id=141777&sid=41377698&con_type=1 (Accessed July 25, 2014).

[5] Vericia Miller, Edwin Sutherland & The Study of White Collar Crime, Working Scholars Bringing Tuition-Free College to the Communityhttps://study.com/academy/lesson/edwin-sutherland-the-study-of-white-collar-crime.htmlhttps://doi.org/10.2307/2572656

[6] Lee M. Brooks, White Collar Crime. By Edwin H. Sutherland. New York: The Dryden Press, 1949. 272 pp. $3.00, Social Forces, Volume 28, Issue 2, December 1949, Pages 215–216,

https://doi.org/10.2307/2572656
[7] Sutherland, E. H. (1941). Crime and Business. The ANNALS of the American Academy of Political and Social Science, 217(1), 112–118. https://doi.org/10.1177/000271624121700114
[8] Cressey D.R. (1964) Some Popular Criticisms of Differential Association. In: Delinquency, Crime and Differential Association. Springer, Dordrecht
[9] Pragati Ghosh, Essay on Criticism of Sutherland's Views on White Collar Crime, http://www.shareyouressays.com/essays/criticism-of-sutherlands-views-on-white-collar-crime-essay/121494
[10] John S. Baker, Jr., is Dale E. Bennett Professor of Law at the Louisiana State University Law Center
[11] Edwin H. Sutherland, White Collar Crime: The Uncut Version (1983).
[12] Mens rea is Latin for "guilty mind" and generally is used to identify the concept of criminal intent. Traditionally, criminal intent--that is, the requirement for a purposeful wrongful act--was a part of the very definition of a crime. See Paul Rosenzweig, The Over-Criminalization of Social and Economic Conduct, Heritage Foundation Legal Memorandum No. 7 (April 17, 2003).
[13] "The term `white collar' is used here to refer principally to business managers and executives, in the sense in which it was used by a president of General Motors who wrote `An Autobiography of a White Collar Worker.'".
[14] Julie R. O'Sullivan, Federal White Collar Crime 54 (2001).
[15] Ilene H. Nagel & Winthrop M. Swenson, The Federal Sentencing Guidelines for Corporations: Their Development, Theoretical Underpinnings, and Some Thoughts About Their Future, 71 Wash. U. L.Q. 205, 216 & n. 51. Co-author Winthrop M. Swenson "was responsible for the staff group that developed the basis for the organizational guidelines." Win Swenson, The Organizational Guidelines' "Carrot and Stick" Philosophy, and Their Focus on "Effective" Compliance (Sept. 7, 1995), in U.S. Sentencing Comm'n, Corporate Crime in America: Strengthening the "Good Citizen" Corporation: Proceedings of the Second Symposium on Crime and Punishment in the United States (1995), at 29.
[16] Paul W. Tappan, Who Is the Criminal? 12 Am. Soc. Rev. 96, 98-99 (1947) ("Apparently the criminal may be law obedient but greedy; the specific quality of his crimes is far from clear.").
[17] Id. at 98. In his foreword to the 1961 edition of Professor Sutherland's book White Collar Crime, Professor Donald R. Cressey commented that the book "clearly was not an attempt to extend the concept, `crime,' despite the beliefs of some reviewers." Edwin H. Sutherland, White Collar Crime iv (2d ed. 1961). He characterized the criticism of Tappan and another critic as "extraneous." Id. Professor Jerome Hall, however, has written that "Tappan's attack was devastating." Hall, supra note 30, at 276.
[18] Letter from Eric H. Jaso, Counselor to the Assistant Attorney General, Criminal Division, DOJ, to the Honorable Diana E. Murphy, Chair, United States Sentencing Commission (Oct. 1, 2002), at http://www.usdoj.gov/dag/cftf/sentencing_guidelines.htm (emphasis added).
[19] Edwin H. Sutherland & Donald R. Cressey, Criminology 51 (10th ed. 1978); Edwin H. Sutherland et al., Criminology 66 (11th ed. 1992) (emphasis added).
[20] Nicholas R. Mancini, Mobsters in the Monastery? Applicability of Civil RICO to the Clergy Sexual Misconduct Scandal and the Catholic Church, 8 Roger Williams U. L. Rev. 193, 195-96 (2002) (discussing application of RICO to Catholic Church and other corporations).
[21] This article is excerpted, with permission, mostly from Professor Baker's article, "Reforming Corporations Through Threats of Federal Prosecution." 89 Cornell Law Rev. 310 (2004).
[22] (January 24, 2020), White-Collar Crime: Lying, Cheating, and stealing https://www.fraudswatch.com/white-collar-crime-lying-cheating-and-stealing/
[23] White Collar Crimes,(June 20, 2016) ,

By The Zendeh Del Law Firm, PLLC https://www.zenlawfirm.com/law-blog/2016/june/white-collar-crimes/
[24] Washington, D.C. March 06, 2002 ,The Measurement of White-Collar Crime Using Uniform Crime Reporting Data https://archives.fbi.gov/archives/news/pressrel/press-releases/white-collar-crime-study
[25] Helmkamp, J., Ball, R., & Townsend, K., eds. (1996). Definitional Dilemma: Can and Should There Be a Universal Definition of White Collar Crime? Proceedings of the Academic Workshop, June 20-22, 1996.Sutherland,
[26] Edwin Hardin (1949). White Collar Crime. New York: Dryden Press.U.S. Department of Justice, Federal Bureau of Inves-tigation (1996). National Incident-Based Reporting System: Data Collection Guidelines. Washington, D.C.: Government Printing Office.
[27] U.S. Department of Justice, Federal Bureau of Inves-tigation (1990). National Incident-Based Reporting System: Supplemental Guidelines for Federal Par-ticipation. Washington, D.C.: Government Printing Office.
[28] U.S. Department of Justice, Federal Bureau of Inves-tigation (1992). UCR Handbook: NIBRS Edition. Washington, D.C.: Government Printing Office.U.S. Department of Justice, Federal Bureau of Inves-tigation (1989). White Collar Crime: A Report to the Public. Washington, D.C.: Government Printing Office
[29] Pearce, Cindi. "What Happens If Fraud Is Committed?" legalbeagle.com, https://legalbeagle.com/8352497-happens-fraud-committed.html. (24 January 2020).
[30] White-Collar Crimes -- Motivations and Triggers, Forbes, (February 22, 2018), https://www.forbes.com/sites/roomykhan/2018/02/22/white-collar-crimes-motivations-and-triggers/#49ca64b41219
[31] White-Collar Crime, FBI, (May 03, 2016), https://www.fbi.gov/investigate/white-collar-crime
[32] Understanding the Fraud Triangle, Fraud, (December 23, 2019), https://fraud.laws.com/fraud-triangle
[33] The Fraud Triangle Theory, Brumell Group, (March 25, 2015), https://www.brumellgroup.com/news/the-fraud-triangle-theory/
[34] What is the Fraud Triangle? , HRZone, (May 17, 2019), https://www.hrzone.com/hr-glossary/what-is-the-fraud-triangle

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 & Service Center, Lahore Garrison University