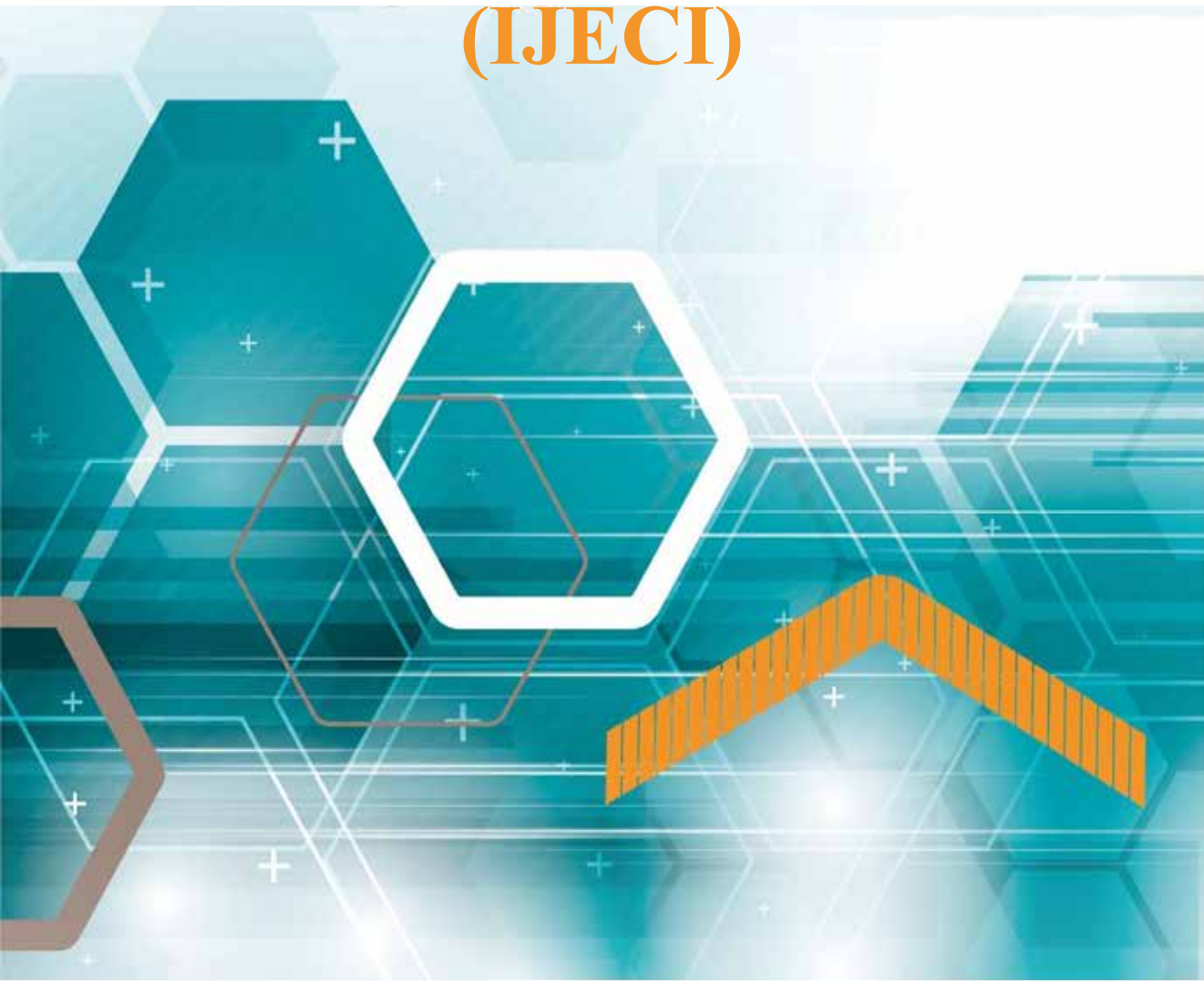
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for Electronic Crime Investigation

(IJECI)



VOL: 2
ISSUE: 3 July-September

Email ID: ijeci@lgu.edu.pk

Digital Forensics Rcscarch and Service Center
Lahore Garrison University, Lahore, Pakistan.

LGU International Journal for Electronic Crime Investigation
Volume 2(3) July-September (2018)

SCOPE OF THE JOURNAL

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

SUBMISSION OF ARTICLES

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

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

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

LGU International Journal for Electronic Crime Investigation
Volume 2(3) July-September (2018)

CONTENTS

LGU International Journal for Electronic Crime Investigation
Volume 2(3) July-September (2018)

Malik *et al.LGU (IJECI)* 2018

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Procuring Confessional Evidence of Criminals, Its Significance As Compared To Forensic, Digital and Other Oral Evidence of Witnesses

Aftab Ahmad Malik[1] ,Mujtaba Asad[2] Waqar Azeem[3]
Professor Department of Computer Science, Lahore Garrison University (LGU), Pakistan[1]
School of Electronics Information & Electrical Engineering
Shanghai Jiao Tong University, Shanghai China[2]
Senior Lecturer, Department of Computer Science (LGU), Pakistan[3]
dr_aftab_malik@yahoo.com[1],asadmujtaba@sjtu.edu.cn[2] ,waqar.azeem@lgu.edu.pk[3]

Abstract:

The work presented in this paper concentrates on the significance of confessional statement of the criminal and particularly how it is procured; using what methodology and tactics. The significance of voluntary confession is more effective evidence in court of law. The question that merely a confessional statement of the accused is sufficient for punishment or it must be coupled, conjoined and amalgamated with other types of evidence such as forensic, digital forensic, documentary or oral evidence tendered by prosecution witnesses. The reasons for voluntary confession must be recorded in writing in court of law. Therefore, confessional statements obtained by torture or other third degree methods by police or investigating agency may jeopardize and endanger the administration of justice. A few third degree methods to obtain the confessional statement are exhibited. Sometimes, innocent persons admit their guilt and are punished in the absence of transparency. However, the significance other types of evidence cannot be ruled out in the presence of confessional statement of the criminal. The paper also presents the analysis of the authenticity of the confessional statement gathered using medication or methods of hypnotism.

Keywords: Admissibility of evidence, Forensic Evidence, Digital information, Prosecution.

1. Introduction

The purpose of this paper is to highlight the admissibility and inadmissibility of evidence in court of law, with special emphasis and contrast to forensic, digital evidence, oral evidence by **witnesses before** Police and court. The philosophy of the right and wrong has been fully elaborated in Jurisprudence [11] which forms basis of various legal systems and their operations. The admissibility of evidence mainly depends on its veracity and reliability. The second important question is how the prosecution can make use of available evidence effectively in the court of law. The present authors have presented a detailed study [1] in the area of 'effective prosecution'. The supporting tools in the effective prosecution [1] are forensic and digital evidence, information contained in the Databases of the criminal Information Systems. The prosecution can only be effective [1], if the

evidence on record is authentic and consistent. The value of digital and forensic evidence in criminal cases cannot be minimized. The digital information is collected by the police or investigating officers has to be used by the prosecutor in the court. This information normally consists of [1] hard disk of computers, mobiles, databases and other sophisticated electronic Medias used by invoking into the networks to commit frauds. The criminals often transfer money into their accounts or fictitious accounts by illegal techniques.

Similarly, the unethical [9] and illegal practices and banking frauds are often committed and observed in banking transactions [1]. In the present time, it has become extremely useful to keep up the information such as and related to Iris, DNA, Fingerprints, modus operandi and facial prints of criminals in the Criminal Data Base System for future verification and retrieval. This requirement has been stressed upon by [2],[3],[4] and [5] giving detailed arguments. For example, the modus operandi in a previously committed offence can thus match to trace out Offenders in present offence during investigation. The biometrics technology plays a pivotal role in this situation.

2. Evidence

In this paper, both areas, the civil and criminal cases are under consideration, therefore, all the types of law of evidence shall be applicable such as Oral evidence by witnesses, documentary evidence, direct, secondary, and primary subject to the provisions of Law of Evidence, “Qanun-e-Shahadat” which was introduced and promulgated in Pakistan in 1984. As for as electronic crimes are concerned, there exist the law called prevention of Electronic Crimes Act (PECA) introduced in 2016; which also prescribes the manner to record evidence and what type of evidence [10]. This paper also considers another type of evidence tendered by the concerned criminal what is called confessional statement, admitting his guilt.

3. The Confessional Statement

In the confessional statement the offender admits and acknowledges his offence or legal wrong done. The admission may oral or in writing. The confession has different import, significance and meaning in Criminology, law, Psychology and religion. Often the confessional statement is tendered to claim some credit best known to sinner or offender. According to Law prevailing in USA, the voluntary confession is valid. It is described in [14] that “the distinction between "to do" and "to confess", between having thoughts of love and confessing one's love, between the indetermination of a feeling and its final definition", as a theme that "creeps into the various stories".

According to [15], Confession is basis of mental health and the confession is self-examination and practice of doing honesty with himself. Further, the confession is categorized as judicial confession and confession before police. The judicial confession is made before the magistrate or concerned court of law. It may be recorded by the court during the investigation of the case. The extra- judicial confession may not be as a strong evidence as confession made voluntarily before court. However, the valid confession is made with a promise or threat to accused. According to the legal provisions of Evidence Act, the confession made before Police by a person shall not be used against him as evidence. According to [17], in Nigeria, the evidence provided by police in a criminal

court is the confessional statement.

3.1 Duty of Prosecution

It is the duty of the prosecution to prove the veracity and reliability of the confessional statement. In this report contradictory and conflicting points of controlling crime have been discussed. The amendment have been made in Nigerian Law on confession has been made. The issue of confession being admissible or not admissible has been left over to the discretion of the judge. In US court the polygraph test is accepted. The polygraph test is carried out conveniently without torture, as explained at depth in [2], which may indicate whether the accused is telling a lie. The polygraph test can only be reliable if an expert technician is conducting it.

Figure 1: Polygraph Devices for Confession

4 Legal Position of Confessional Statement

The confessional statements procured under section 164,364 and 533 of the Criminal Procedure Code have special significance. It is essential that the oral confession ion civil cases must be recorded very carefully. The use of different words and phrases may change the meaning of the confessional statement. Therefore, a lot of care is required, for example, the while recording the confessional statement the court must sent the Police outside court room and order to remove the handcuff (Lahore High Court Rules & Orders Vol. III, Chap. XIII). The judges must tell the accused that there is no binding on him to tender the confessional statement. This rule of law has been reported in (DB) PLD 1958 Lahore 559 and also in PLD 1987 FSC 43. According to these rules, it is mandatory for

the Magistrate to ascertain and record that the accused has made the confession voluntarily as per injunction of the rule 1975 P.Cr. LJ 889. Further, the judicial confession recorded shall be ruled out not being consistent with High Court Ruling (Chap. 13 Vol. III and NLR 1987 Cr. 831).

5. Procuring Confessional Statement When the Accused is Under Intoxication

It is improper to record the Confessional Statement when the accused is served with intoxication material, which may hamper the physical and mental control on what is being said. The effect of alcohol are particularly worth mentioning. The alcohol apart from being poison shows the effects such as problems in breathing, vomiting, low body temperature, Seizures and especially it creates Confusion. It reduces the testimonial capacity and adversely affects the faculty of mind concerned with intelligence and truthfulness. The accused may be in the state of half sleep and the speech may be irrelevant.

In India, a drug is used which is prepared from wild Cannabis Indica having narcotics effect, which can be smoked or chewed and also named as "Hasheesh". A drink in water or milk is also used made for intoxication. The person taking it in the form of smoke or drink loses in control on mental faculties related to wisdom, which is temporarily hampered. Under such condition the person talks freely, even about his secrets. Therefore, sometimes this method is used for obtaining confessional statement or for the purpose of knowing facts of the case, by Police.

Figure 2: Police Tactics for Confession

6. Police Tactics to Procure Confessional Statement

Police employs various techniques [16] and third degree methods to procure the confessional statement. The degree of torture varies from situation to situation. The most notorious practices are the burning of abdomen and parts of the body and skin, hanging in inverted position for longer intervals of times, breaking bones and using red hot steel rods to burn the hands and feet. Apart from physical torture and intoxication, the Police also use other methods of investigation while the accused is under the custody, such as the Reid Technique, isolation, maximization, minimization, asking informal questioning and also lying.

7. Reid Technique

According to [19], the Reid technique consists of interviewing and arguing with the accused by two officers at a cup of tea. It is effective in the criminal cases. One playing "bad cop" and the other "good cop" and the session of questioning continues until the accused confesses his guilt. In the maximization technique the person interrogating the suspect begins with the assumption that the accused is guilty. In another method the accused is kept away from family and friends in isolation.

8. Hypnotic Technique

There are several techniques available in literature bur [23] gives explanation 31 Techniques to create hypnotic induction. A few of these are simple such as Eye Cues & eye contact, Arm "Levitation" Technique, Relaxation technique, Handshake technique, Visualization. Some images such as specially designed spirals pictures and other model are shown to the person being hypnotized and asked to visualize the situation. In recent years, this science is being extensively applied to cure people from addiction, fears, to change habit, cognitive behavior or pain management using relaxation method.

9. Hypnosis and its Applications in Criminology

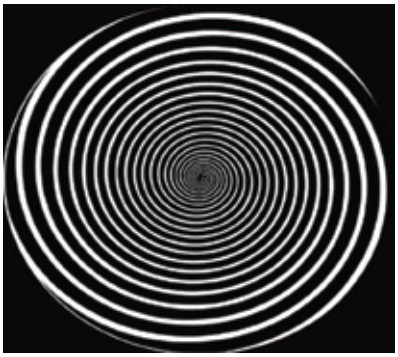
The offender's conviction or exoneration mainly depends upon the evidence other than that of hypnosis report. The report of hypnotist is supportive evidence. The hypnosis or mesmerism or hypnotism takes a person into state of consciousness, oblivion or sleep and the power of voluntary action is temporarily withheld but the person gives response to the commands of hypnotist. It is 200 years old psycho-technique. It is normally used to unfold the forgotten memory. People under the effect of hypnotic effect are regressed [20]. It is frequently used in criminology and crime investigations. In [21] its uses in Psychology have described to study the focused attention of mind. The discipline of hypnosis sometimes is termed as Abnormal Psychology or imaginative field or enactment. The procedure of hypnotizing a person is called art of mentalism or hypnotherapy. The hypnotism is applied to areas of music, stage performance and most importantly in crime investigations.
Why hypnosis is useful in Criminology, crime detection and investigation because the hypnotized person speaks out all the information automatically without caring or being concerned with people sitting around him. This characteristic makes the discipline useful for crime investigations and procuring confession of criminal.

Another characteristic of the hypnosis is the hypnotic induction, which makes it attractive for field of criminology. It is a technique to put the subject into a state called hypnotic trance. This is how the confessional submissions come out the mind of accused. The Braid's eye fixation method is most influential.

10. FBA Uses of Hypnotic Techniques

The Federal Bureau of Investigation (FBI) is using the hypnosis in crime investigation. In important criminal cases, the police, psychiatrists, physicians and lawyers separately conduct sessions of hypnosis induction to make the criminals confess. However, this is done without prejudice to the task of the investigating officers, which proceeds independently. The hypnotic induction works successfully on criminal involved cases such as bank robbery, rape and murder etc. The witnesses to offence may also be sometimes allowed to question during hypnotic session.

The hypnotist must have adequate training of hypnosis, knowledge of human behavior and medicine. While using hypnosis the Federal Bureau of Investigation (FBI) follows the rule of the government (Department of Justice) strictly for selective cases. The coordinators of hypnotists are trained personnel. The hypnotists are very well qualified in the requisite area. They also make video tape the whole procedure. The hypnosis is carried out phase wise. The hypnotist himself applies the procedure in the first phase; while in the second phase the witnesses also participate to ask questions from the criminal by mentioning the sight and scene of offence other circumstantial matters. The third phase is concerned with real induction followed by regression. The rate of success in obtaining the confession is 60-70%.



11. Forensic Hypnosis

According to [22] hypnosis is extensively being used in the criminal investigation producing positive outcome in various fields of criminology. One of the drawbacks of this method is loss of memory during the hypnotic process. The experimental results on patients are reported in [22]. The important issue is how much of outcome of hypnosis results are used in court as evidence.

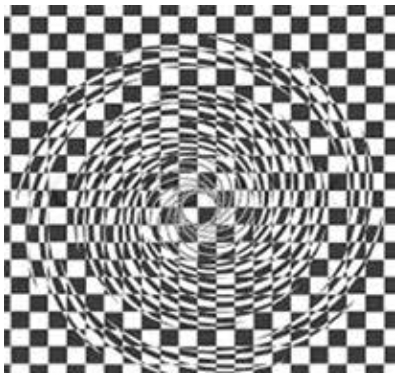
Figure 3: Hypnosis Techniques

12. Conclusions

The confessional statement from accused must procured without using brutal and third degree methods by police. The confession obtained forcefully by these methods and by use of intoxication is not admissible in court. However, the hypnosis may helpful to Police to further probing the matter, in spite of inherent drawbacks of hypnosis such as occasional memory loss and control of person performing hypnosis induction, it produces favorable results. The visualization, relaxation, eye cues and eye contact technique of hypnosis are effective in criminal investigation and obtaining confessional statement to support other investigation conducted by Police. The hypnotic approaches strengthen and protect the case witnesses and the victims. Forensic hypnosis technique is used successfully for restoration of memory of the witnesses or victims of serious crime.

13. Acknowledgement

The authors are grateful for the appreciation and encouragements of our work presented in this paper by Mr.Kaukab Zuberi Director DFRSC, Lahore Garrison University Lahore. He is Certified Consulting Hypnotist of National Guild of Hypnotists. He guided us to work on Confession and Hypnosis.



14. References

[1] Dr. Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2018), " Effective Prosecution to Support Digital Forensic Evidence During Investigation and Court Proceedings", International Journal for Electronic Crime investigation, ISSN 2522-3429;IJECI; Volume 3 ,April-June 2018; Lahore Garrison University, Lahore.

[2] Dr Aftab Ahmad Malik, Asad and Waqar Azeem (2018); "DNA Fingerprints, Facial Prints and other Digital Forensics as Evidence in Criminal Investigation and Court Proceedings", International Journal for Electronic Crime investigation, ISSN 2522-3429;IJECI; Volume 2, Issue: 1 ,PP 01-09; January-March 2018; Lahore Garrison University, Lahore.

[3] Dr. Aftab Ahmad Malik, Asad and Waqar Azeem (2018)," Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed", International Journal for Electronic Crime Investigation, ISSN 2522-3429 ; IJECI ; Volume 1, Issue :1 , October-December 2017; Lahore Garrison University, Lahore (Printed and published in 2018).

[4] Dr Aftab Ahmad Malik, Asad and Waqar Azeem (2017), "Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed", International Journal for

Electronic Crime Investigation, ISSN 2522-3429 ; IJECI ; Volume 1, Issue :1 , October-December 2017; Lahore Garrison University, Lahore.

[5] Dr Aftab Ahmad Malik and Mujtaba Asad (2017), "Algorithm for using Codes in place of facial Images during image processing in large databases/warehouses to reduce storage and enhance efficiency and processing speed"; LGURJCSIT: Lahore Garrison University Research Journal of Computer Science and Technology; Vol 1, Issue 2, April-June 2017, PP:1-9, ISSN 2519-7991.

[6] Dr Aftab Ahmad Malik, Asad and Waqar Azeem (2017), "Algorithm for coding person's names in large Databases / Data warehouses to enhance processing speed, efficiency and reduce storage requirements Lahore Garrison University Research Journal of Computer Science and Information Technology, Volume 1, Issue 1, January-March, 2017; ISSN 2519-7991.

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

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

[9] Dr Aftab Ahmad Malik (1995), "Business Ethics in Banking Sector", Book Published by Institute of Banking Sector, Karachi.

[10] Prevention of Electronic Crimes Act (PECA)

[11] John William Salmond,"Jurisprudence", Ebook: ww.ebooksread.com/authors-eng/john-william-salmond/jurisprudence-mla.shtml

[12] Roger W. Shuy, The Language of Confession, Interrogation, and Deception(1998), p. 2

[13] Jorge J. E. Gracia (1995), A Theory of Textuality: The Logic and Epistemology, p. 94–95.

[14] Giulio Marra, Shakespeare and this "imperfect" World: Dramatic Form and the Nature of Knowing (1997), p. 69.

[15] Wilkes, Paul (2012). The Art of Confession: Renewing Yourself Through the Practice of Honesty. Workman Publishing. p. xi. ISBN 9780761168720.

[16] Ave Mince-Didier, "Tactics Police Use to Get a Confession", Criminal Defence Lawyer.com https://www.criminaldefenselawyer.com/resources/criminal-defense/defendants-rights/tactics-police-use-get-a-confession

[17] AdedoyinAkinsulore, A Jurisprudential Analysis Of Confessional Statement. https://www.researchgate.net/profile/Adedoyin_Akinsulore/publication/311201890

[18] Fr. Titus Ik. Nnabugwu, LL.M, BL, JCD; "Confessions in Nigeria Evidence Act, 2011"; http://titusnnabugwu.blogspot.com/2012/06/confessions-in-nigeria-evidence-act.html

[19] F Inbau, J Reid, J Buckley, B (2011), " Criminal Interrogation and Confessions" , Fifth Edition Jayne - 2011 – Book Published by Jones and Barlett.

[20] What Is Hypnosis? - How Hypnosis Works? https://science.howstuffworks. com › ... › Science Vs. Myth › Extrasensory Perceptions

[21] What Is Hypnosis and How Is It Used In Psychology? - Verywell Mind https://www.verywellmind.com/Psychology/Psychotherapy

[22] William S. Kroger &Richard G. Deuce (1979), "Hypnosis in Criminal investigation", International Journal of Clinical and Experimental Hypnosis, Volume 27, Issue 4, PP:358-374

[23] [23] Thirty one hypnotic Techniques, https://britishhypnosis-research.com/hypnosis-techniques/Birkbeck University of London, Malet Street, London WC1E 7HX. United Kingdom

Sumra *et al.LGU (IJECI)*2018

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Security in Vehicular Ad hoc Network (VANET) using Trusted Platform Module (TPM): A Survey

Irshad Ahmed Sumra[1], Zahid Adeel Hashmat[2]
Computer Science Department
University of South Asia
47-Tufail Road, Lahore.
Sector C, DHA Phase-VI Lahore.
zahidadeelhashmat@gmail.com[2] ,irshad.ahmed@usa.edu.pk[1]

Abstract:

Vehicular Ad hoc Networks (VANETs) are gaining more attention from automobile industries due to user safety on highway. However, security and safety critical issues need to be resolved before deployment of VANET in real environment. In this paper, we are providing a comprehensive survey on the usage of trusted platform module (TPM) in VANET. VANET is a open wireless environment where vehicle can communicate with other vehicles and also with roadside unit where any infected rogue vehicle can perform malicious actions on fellow vehicles. Security threats caused by rogue vehicles can endanger life of passengers. Trust is an important key factor and it can be introduced inside VANET environment using TPM hardware. The core purpose of this survey is to highlight the security threats in VANET and provide security architecture built upon TPM to mitigate all discussed threats.

Keywords: Vehicular ad hoc network (VANET), Security, trusted platform module (TPM), dedicated short range communication (DSRC).

1. Introduction

Traffic accidents impact our life directly or indirectly and are considered a major challenge in traffic management. According to the global status report on road safety 2015, it is indicated that the global road accident deaths has platitude at 1.25 million per year [1] and it will increase 60% more in next few years if it is not controlled somehow. An ideal solution to avoid road accidents and improve traffic management is VANET. It is a sub category of mobile ad hoc network (MANET) where nodes can be Road Side Units (RSUs) or vehicles [2]. It uses Dedicated Short Range Communication (DSRC) channels in vehicle to vehicle (V2V) and vehicle to road side unit (V2R) communication [3]. DSRC are short to medium range wireless communication channels which are specifically designed for automobiles to guarantee active safety applications [1]. In

safety applications, warning messages are sent to network vehicles to prevent road accidents. Non-safety applications may include comfortable driving experience of passengers and availability of parking slots. Inside VANET, trust is key importance parameter between vehicles and RSUs. So, information and data exchange happens between vehicles and RSUs assuming that security, trust, privacy triad is ensured. Vehicle is a private property of a user and it may disclose very sensitive information about its owner if somehow a malicious attacker exploits it. In short, VANET faces some serious security challenges where a malicious attacker can change the behavior of network nodes and launch attacks against safety and non-safety applications. Therefore, network security must be ensured before deployment in order to avoid any life critical situations. High mobility nature of VANET makes it very challenging task to monitor [4] and identify attacks. In order to make a reliable network these mobile nodes have to trust each other which is technically possible using trusted platform module (TPM). Trusted computing group (TCG) defines trust as "Any entity that behaves in an expected manner for that intended purpose"[5]. Core entities of VANET are user, vehicle and RSU where unexpected behavior from either of them can highly affect the behavior of other entities. So, in this paper we will discuss that how TPM can introduce 'TRUST' factor among VANET nodes and how it can help us to improve security against attacks.

The rest of the paper is divided into VI sections where section II discusses essential security requirements for VANET. Section III discusses the TPM architecture and proposed TPM model for VANET. Section IV discusses in details the about the nature of attacks on VANET. Section V discuss about possible usage of TPM and some other trusted hardware modules in VANET for defensive countermeasure of attacks and in the end section VI concludes the paper.

2. Essential Security Requirements

VANET infrastructure highly relies on communication and messages among its nodes. So, it is very important to make sure authenticity and integrity of the exchanged communication data. As VANET is a real-time network and little delay in communication messages can endanger the life of passengers especially when messages are meant for safety applications. So, it is very possible that a malicious intent attacker may try to delay or drop the safety concerned communication messages. Taking above mentioned scenarios into consideration, we need some proper security measures which may define and measure the security of VANET nodes [6]. So, we will discuss following five parameters to address all these security and privacy issues [13]. In simple words, a network will be considered well secured if it implements following parameters in its topology.

2.1 Authenticity:

Inside VANET, there may be legitimate and non-legitimate (malicious) nodes. So, first of all it is important to ensure that the communication nodes are authenticated by a trusted authority. A third party certificate authority (CA) module manages and verifies the identities of VANET nodes. So, it will ensure that the messages are received from legitimate users [7]. Authenticity will provide a trustworthy environment for exchanged messages by keeping un-authorized nodes away from private communication channels.

2.2 Confidentiality:

Confidential user data such as vehicle's

registration number, global position and route plan of VANET nodes is shared with concerned authorities for safety or non-safety applications [6]. Confidentiality parameter demands that the data must be shared and stored in secure way in order to avoid any un-authorized access. Confidentiality is achieved using encryption algorithms.

2.3 Availability:

VANET safety applications require real-time message exchanging. So, the network should be highly available and operational for authenticated users. VANET real-time applications exchange messages at very high data rate where there is not even a margin of milliseconds delay. In VANET safety applications, a milliseconds delay may endanger someone's life.

2.4 Integrity:

It makes sure that the message sent from sender side has been received successfully on receiver side without any alteration or modification on its way [10]. A malicious intent attacker can do attack against integrity in which case receiving node will receive tempered message which may cause serious problems. This kind of attack is used to spread misinformation. To ensure data integrity, sender node digitally signs its message with certificate before sending which is verified on receiving end to make sure that data is not tempered.

2.5 Non-Repudiation:

Nodes involved in message sending process must send that message at any cost and they must not be able to deny it. Similarly, nodes involved in reception process must receive it and should not have the ability to deny it. Non-repudiation is often used to detect and unveil the criminals. Particularly, it can be useful in accident's investigations by re construction of exchanged messages [10].

3. TPM Based Trust model for VANET

TPM hardware module is specifically designed for computing purposes where security and trust is main concern and now it is being integrated into many computer devices. In laptops, mostly TPM chips are being integrated for business class like Dell's latitude series [9]. The infrastructure on which TPM is deployed, a piece of software is needed to communicate with TPM. TPM communicates with this software to store data on secure locations. It has built-in cryptographic functionalities which are used to enforce trust. Though TPM seems quite good against software attacks but it doesn't have any mechanism to avoid hardware tampering. It can be introduced inside VANET to ensure a secure and trusted V2V and V2I communication. An architectural diagram of TPM is shown in Figure 1.

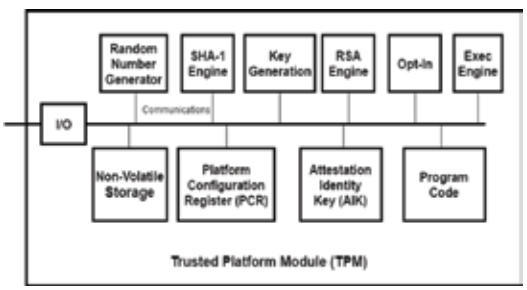


Figure 1. TPM Architecture [20]

F. Stumpf et al. [19] proposed a multi-layered C2C communication protocol named SRAAC for VANETs in order to ensure trust, security and privacy of nodes. Secure Revocable Anonymous Authenticated inter-vehicle Communication (SRAAC) protocol facilitate vehicles in inter-vehicle communication by sending or receiving safety messages. Proposed SAARC protocol will contain authentication authority (AA), inter-vehicle

communication certificate server (ICS) and onboard unit (OBU) components. Author discussed some potential attacks to SRAAC which are OBU collision attacks, false safety message injection and arbitrary validation time. Author not only discussed these attacks but also proposed a solution to prevent from these attacks which involves the usage of trusted inter-vehicle communication (T-IVC) certificate.

G. Guette et al. [20] discussed in detail that how TPM can be useful in VANET security. They highlighted some essential security parameters and proposed two applications [5] (event reporting and platoons) for VANET. Their research circles around some essential security parameters in VANET (authenticity, confidentiality, integrity) which are highlighted in section II of this paper. Their key objective was to ensure a secure and anonymous V2V communication using cryptographic keys. José María de Fuentes [21] highlighted some serious security issues in VANET and proposed some solutions related to those issues.

G. Guette et al.[22] proposed TPM based security and privacy solutions. Cryptographic key management was main focus point of their discussion. TPM module is used as an integrated part of the vehicle for all this solution. Privacy Certification Authority (PCA) is a third party modules which issues a certificate for Attestation Identity Key (AIK). AIK is used for attestation of current platform and its configuration. PCA also verifies different AIKs which are being used by different network applications. AIK certificates were proposed to be saved on a memory stick. The proposed mechanism creates some dependencies such as PCA and memory stick needs to communicate through a computer, and to connect with certification authority an internet connection is needed.

Sumra et al. [23] discussed in detail about a new card based scheme for VANET which focus on trust and security related issues. Sumra et al. [30] provided solution of security, trust and privacy using TPM in VANET.

For authentication purpose TPM used many key and here is mentioned two important keys which are given below:-

1) **Attestation Identity Keys (AiK):** This key generated by the TPM and the Privacy Certification Authority (PCA) authenticate the key and secure the end user information. AiK does not disclose the identity of the TPM and this is the main advantage of this key.

2) **Endorsement Key (EK):** this key is generated by the TPM manufacturer and unique feature of this key is securely stored inside the TPM.

A TPM root of trust architecture is showed in a Figure 2 and details about each module is given after that.

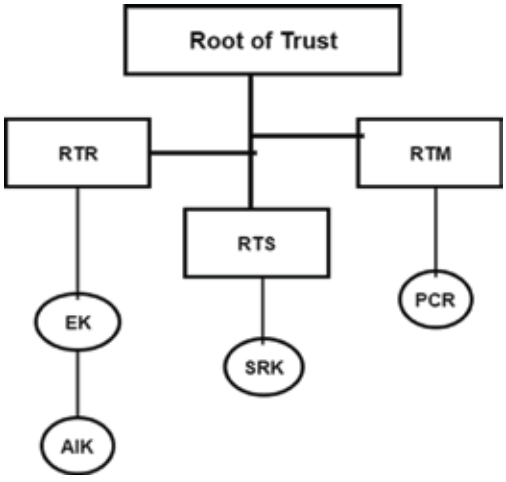


Figure 2. TPM based Root of Trust [24]

Root of Trust: TPM hardware provides following three types of root of trust [24]:

- Root of trust for measurement (RTM)
- Root of trust for reporting (RTR)
- Root of Trust for Storage (RTS)

TPM hardware communicates with onboard unit (OBU) and other embedded sensors of the vehicles and ensure root of trust. Figure 3 shows a high level working of TPM with OBU and other sensors and its application in VANET.

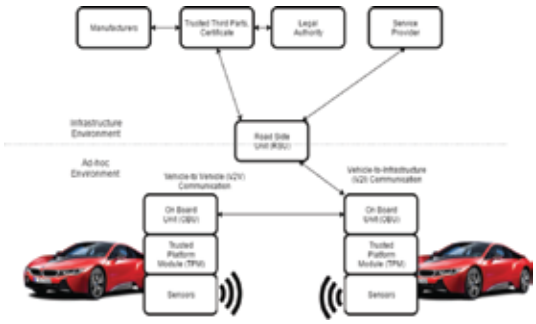


Figure 3. Trusted communication with TPM [28]

Root of Trust for Measurement (RTM): RTM is the module of TPM which measures current system state and saves it in Platform Configuration Register (PCR). TPM uses internal secure storage registers which are shielded from external attacks and data tampering attempts. So, PCR ensures data integrity of stored system state. PCR storage is non-volatile and it persists even when system is powered off.PCR basic purpose is storage of 20 byte digest hash values of system states and representation of hardware and software configuration metrics. Configuration Metrics are very important as they are defined before system is developed and then monitored in entire lifetime of system. If system finds any change in hardware and software configuration metrics, it logs it and takes appropriate actions.

Root of Trust for Reporting (RTR): RTR generates reports about current platform and securely provide generated reports to third parties. RTR ensures data integrity and privacy using digital certificates. RTR digitally signs PCR values with private key and send them to requesting third party. Third party can verify that digitally signed values using Endorsement Key (EK) [25] which is a public key.

Root of Trust for Storage (RTS): R T S does encryption and decryption of data and keys. Besides this, it also provides keys list and their respective unique functionalities. RTS utilizes a Storage Root Key (SRK) which uses asymmetric encryption to encrypt data and keys. RTS is embedded into TPM and its core purpose is to wrap TPM protected keys.

4. Attacks in VANET

A malicious intent attacker can launch different attacks in VANET. In this section, five major classes of attacks are discussed in VANET security perspective [24, 25]. In section VI, some proposed solutions to mitigate these attacks are discussed. Each attack class gives an insight to threat severity and attack type. The purpose of this section is to identify the attacks on based of their behavior or signatures and take appropriate measures accordingly. Figure. 4 lists down five classes of different types of attacks in VANET [29].

Figure 4. Classes of attacks in VANET [29]

First Class - Application Attack

This attack mainly targets VANET safety and non-safety applications. In this attack, attacker intercepts messages from one vehicle, tampers it and then spread it to other vehicles. In safety applications, warning messages are passed from one vehicle to other vehicles. If an attacker modifies it, it will give rise to some serious consequences. In bogus information attack [12] attacker spreads misinformation inside network which highly affects the behavior of network users.

In safety application attack, an attacker may spread wrong information that road is clear while there is a work zone ahead. So, in such case a road accident is obvious. In non-safety application attack, attacker may spread messages to other vehicles that parking slots are not available while actually there is parking slots are available [7].

Second Class - Network Attack

Network attack directly affect VANET infrastructure which in turn affect V2V and V2I communications. This attack is considered of high priority and might create serious problems for users.

a. Sybil Attack:

Sybil attack [16] belongs to the network attacks class. In this attack, attacker fabricates VANET communication messages with fake source identities and broadcast them inside network. When the fabricated messages [15] are received by legitimate users, they believe that there is more than one vehicle in the surrounding or there is some serious traffic jam situation. Attacker will benefit when other vehicles would believe that road is blocked because of traffic jam.

b. Denial of Service (DOS) Attack [32]:

DOS attack is attack on availability of some service. Inside VANET environment, all vehicles rely on network communication messages and if some attacker somehow jams this network, it will be serious problem. All V2V and V2I communication will get down, so authentic users won't be able to communicate with one another and it will create serious traffic jam or other life critical situations.

Third Class - Social Attack

In these attacks, social engineering attacks may be involved and it may also have attacks where immoral and abusive messages can be shared with network nodes. The main objective of this attack type is to create disturbance inside network. For example, a malicious intent driver send message to other vehicle death of his/her siblings. It will highly affect the behavior of driver which may lead to road accidents. Social attacks are totally based on social messages where one vehicle can lie to other fellow VANET nodes to create havoc.

Fourth Class - Timing Attack

This attack [31] is also on VANET safety and non-safety applications but in this attack warning messages are not altered by attacker. Instead, attacker creates a delay in message delivery. As VANET is a real-time network where warning messages should be sent and received in real-time otherwise it may cause some serious problems in life critical situations. For example, if a warning message is going to tell vehicle that there is a work zone ahead and user doesn't receive it in time, it may cause an accident.

Fifth Class - Monitoring Attack

In this class of attack, attacker only monitors or sniffs network traffic in passive mode without

creating any disturbance. In this attack, attack may find some valuable information from V2V and V2I communication which may be used for attacker's benefit. For example, if some police operation is going to happen somewhere inside VANET and attacker somehow intercept the operation details; he may use it for his benefit. Attacker may track user location in a specific region using ID disclosure attacks [17].

5. TPM based Proposed Mechanisms

VANET security threat has been under considerations in last few years and many solutions were proposed to mitigate those risks. In this section, countermeasures for attacks discussed in previous section are highlighted. In this section five basic trust entities will be discussed along with how they coordinate to create a chain of trust on platform. Figure 3 also elaborates that how TPM can be useful in VANET V2V and V2I communication. Trust entities (user, vehicle, application, routing, medium and infrastructure) are given below:[14]

a) Trusted User

There are basically two types of users inside VANET which are trusted users and non-trusted users. Trusted users are those who show the normal and non-malicious behavior. On the other hand, non-trusted users can tamper with VANET safety and non-safety applications. VANET warning messages are passed by trusted user to other users and data integrity is ensured while non-trusted users will tamper data on the way and compromise privacy of others. This way a chain of trust will be affected.

b) Trusted Vehicle

Vehicle is an important node of VANET so it is very important to make sure that vehicle is trusted or non-trusted (compromised) because vehicle is an integral part of V2V and V2I communication and if it is compromised, whole chain of trust will be affected. Trust factor in vehicles is introduced by integrating TPM with sensors and OBU. Figure 3 is elaborating this concept very well.

c) Trusted Applications

VANET safety and non-safety applications should have proper security measures within them so that an attacker may not use them to others and applications should perform their activities in the way they are designed to work. M.Gerlach et al. [11] proposed and discussed a model for trusted applications inside VANET. Proposed model discusses the situations where the attributes of the trust and trustee are relevant.

d) Trusted Routing

Routing is very integral part of network communications which involves hop to hop and hop communication. T. Chen et al. [26] proposed his own trusted routing framework which authenticates communication messages, ensures trust between vehicles and routing verification with depending on any third party CA. Trusted framework works on Optimized Link State Routing (OLSR) protocol.

e) Trusted Medium

VANET uses dedicated short range communication (DSRC) band for communication channels. It provides multiple channels on high bandwidth which ranges from 5.850 to 5.925 GHz. Attacker will try to monitor or tamper data of VANET nodes so there should be a secure and trusted communication channel. Communication channel should continuously hop to avoid any

data sniffing. C. Laurendeau et al. [27] discussed some security threats in DSRC which can be minimized to make communication channels secure and trusted.

f) Trusted Infrastructure

VANET infrastructure should be trusted and highly available to VANET nodes. V2I communication is an integral part of VANET applications and if somehow a malicious intent attacker performs a DOS attack against infrastructure and takes it down, it will raise some serious problem for VANET nodes because network nodes trust on infrastructure and if infrastructure is not responding it will break chain of trust.

6. Conclusion

Authenticity, confidentiality and availability are some essential security requirements and all of these can be achieved inside VANET if somehow 'TRUST' is introduced inside infrastructure and vehicles. TPM module is used to develop this trust. VANET safety and non-safety applications share messages in V2V and V2I communication so it is very important that all those messages are authenticated and generated by trusted network nodes. For this purpose, TPM digitally signs messages and receiving person verifies those with their key which verifies the authenticity of messages. TPM is integrated with onboard-unit and sensors of vehicle where it authenticates all incoming and outgoing communications. A chain of trust can be developed with trusted user, vehicle, applications and purpose of this chain of trust to handle with different types of attacks in VANET and secure the vehicle to vehicle and vehicle to road side communication.

7. References

[1] World health organization http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/.

[2] Samara, G., Al-Salihy, W. and Sures, R. (2010) Security Analysis of Vehicular Ad Hoc Nerworks (VANET). Proceedings of Second International Conference on Network Applications Protocols and Services (NETAPPS), IEEE, Kedah, 22-23 September 2010, 55-60.

[3] International transportation system http://www.its.dot.gov/factsheets/dsrc_factsheet.htm.

[4] Al-Raba'nah, Y. and Samara, G. (2015) Security Issues in Vehicular Ad Hoc Networks (VANET): A Survey. International Journal of Sciences & Applied Research (IJSAR) , 2, 50-55.

[5] B.Balacheff,L.Chen,S.Pearson, D.Plaquin,G.Proudler. In, S.Pearsoned, "Trusted Computing Platform: TCPA technology in context", Prentice Hall PTR, Upper saddle river, NJ, 2003.

[6] Engoulou, R.G., Bellaïche, M., Pierre, S. and Quintero, A. (2014) VANET Security Surveys. Computer Communications, 44, 1-13. https://doi.org/10.1016/j.comcom.2014.02.020

[7] Raya, M. and Hubaux, J.P. (2007) Securing Vehicular Ad Hoc Networks. Journal of Computer Security, 15, 39-68. https://doi.org/10.3233/jcs-2007-15103

[8] I.AhmedSumra, H.B. Hasbullah, J.AbManan,"User requirements model for vehicular ad hoc network applications", International Symposium on Information Technology 2010

(ITSim 2010), Malaysia.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[9] http://www.dell.com/us/business/p/latitude-laptops

[10] Mejri, M.N. and Hamdi, M. (2015) Recent Advances in Cryptographic Solutions for Vehicular Networks. IEEE Proceedings of International Symposium on Networks , Computers and Communications (ISNCC), Hammamet, 13-15 May 2015, 1-7.

[11] M.Gerlach, F. FOKUS,"Trust for Vehicular Applications" IEEE Computer Society, Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, p: 295-304, year of publication: 2007.

[12] M. Raya,J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15,Issue no.1 January 2007, pp: 39-68.

[13] Razzaque, M.A., Salehi, A. and Cheraghi, S.M. (2013) Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. In: Khan, S. and Khan Pathan, A.-S., Eds., Wireless Networks and Security , Springer, Berlin Heidelberg, 107-132.

[14] Irshad Ahmed Sumra1,Halabi Hasbullah1,Jamalul-lail2,Masood-ur-Rehman1,Trust and Trusted Computing in VANET. Computer Science Journal 2011.

[15] J. Douceur,"Thesybil Attack", First international workshop on peer topeer(P2P) system,march 2002,pp: 251-260.

[16] G. Guette, B.Ducourthial," On the sybilattackdetection in VANET",

[17] M. Raya, P. Papadimitratos, J.P. Hubaux," Secure vehicular communications", IEEE Wireless Communication Magazine,specail issue on inter-vehicular communication, Oct 2006.

[18] Al-Raban'nah, Y. and Al-Refai, M. (2016) Toward Secure Vehicular Ad Hoc Networks an Overview and Comparative Study. Journal of Computer and Communications, 4, 12-27.

[19] F. Stumpf, L. Fischer and C.Eckert," Trust, Security and Privacy in VANETsMultilayered Security Architecture for C2C-Communication", Automotive Security, pp. 55-70, Wolfsburg, Germany, VDI-Verlag, 200.

[20] G.Guette,O.Heen, "A TPM-based Architecture for improvedsecuirty and Anonoymity in vehicular ad hoc networks" ,IRIS France.

[21] J.M. d. Fuentes, A.I. González-Tablas, A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks", Maria Manuela Cruz-Cunha, Fernando Moreira (Eds.), Handbook of Research on Mobility and Computing, IGI Global (2010)

[22] G. Guette, C. Bryce, "Using TPMS to securevehicular ad-hoc networks (VANETS)", in: Information Security Theory and Practices. Smart Devices, Convergence and NextGeneration Networks, 2008, pp. 106–116.

[23] IA,Sumra, H.Hasbullah, iftikharahmed, Jamalul-lail," New CardBasedScheme to Ensure Security and Trust in Vehicular Communications", Saudi

International Electronics, Communications and Photonics Conference Riyadh, Saudi Arabia April 23rd - 26th 2011.

[24] K. N. McGill.” Trusted mobile devices: Requirements for a mobile trustedplatform module”, Johns hopkinsapltechnical digest 32(2):544, 2013.

[25] S. Kinney,” Endorsement Key (EK)”,Trusted Platform Module Basics Using TPM in Embedded Systems , chapter No.04, , pp No.32.

[26] T. Chen, O. Mehani and R. Boreli, ”TrustedRouting for VANET” 9th International Conference on Intelligent Transport SystemsTelecommunications (20 October 2009), pp. 647-652.

[27] C. Laurendeau, M. Barbeau,”Theat to security in DSRC/WAVE”, 5th International Conference on Ad Hoc Networks and Wireless (ADHOCNOW). LNCS 4104, pp.226-279, 2006.

[28] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi,”Survey on VANET security challenges and possible cryptographic solutions , Vehicular Communications, Volume 1, Issue 2, April 2014, Pages 53-66, ISSN 2214-2096

[29] I. A. Sumra, I. Ahmad, H. Hasbullah and J. l. bin Ab Manan, "Classes of attacks in VANET," 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, 2011, pp. 1-5.

[30] I. A. Sumra, H. B. Hasbullah and J. l. A. Manan, "Using TPM to ensure security, trust and privacy (STP) in VANET," 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, 2015, pp. 1-6.

[31] I. A. Sumra, J.-L. A. Manan, and H. Hasbullah, “Timing attack in vehicular network,” in Proc. of the 15th WSEAS International Conference on Computers, Corfu Island, Greece, July 2011, pp. 151–155.

[32] I.A. Sumra, H.B. Hasbullah, J. lb. Ab Manan, ”Denial of Service (DOS) Attack and Its Possible Solutions in VANET”,WASET issue 65, april 2010 ISSN 2070-3724.

Ali *et al.LGU (IJECI)* 2018

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Role of Windows Registry Forensics in Digital Forensics Investigation

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

Abstract:

The research paper covers one of the most important aspect of the digital forensics investigation "Registry Forensics" as there are several components that are necessary for carrying out digital forensics investigation, one cannot overall the windows registry. The research paper is basically divided into two segments, where the first segment fully explains what registry is, how it works, and what important information stored in it. Moreover, the research paper covers the aspect of anti-forensics elements that are incorporated by different cyber criminals in order to wipe the traces of fraudulent activities, and finally the author has concluded the research paper by highlighting the importance of windows registry in digital forensics investigation.

Keyword: Digital Forensics, Forensics Investigation, Windows Registry, Windows Registry Forensics, cybercrime, cybercriminal.

1. Introduction

As there are many aspects that are examined by an investigator during the investigation of a criminal offence same goes with the digital forensics investigation, after seizing the crime scene the investigating officer has to take forensics image of the suspect system, after that it is taken to the forensics labs for the examination, the investigator here critically analyse every aspect of the image, and look for the foot prints that can help him in drawing his findings. One of the most important element that is analysed during the examination phase of the investigation is the examination of windows registry. To start with windows registry is the fundamental component of windows OS Operating system, which contains a lot of information regarding the configuration of the system. The information that is managed within the registry of the windows contains the history of the user activities, details about the program installed and details about the running programs. The storage of data is carried out in same way as it is done in log file [1]. Windows registry is explained in depth in proceeding parts of this research paper.

2. Literature Review

In order to support the stance of role of windows registry in digital forensics investigation, the author has studied different related work. After studying various literatures, the following keys are highlighted and are explained in depth.

2.1 What Is Windows Registry?

The explanation that is derived from the Microsoft's publication regarding registry, is that it's a database that contains the important information category wise pertaining to the application, services and operations that are running on the windows [2]. The format that is used to structure the data in registry is of tree format. The tree is consists of several nodes, these nodes are known as keys. Then there is further classification of these keys, where each key is consist of subkeys and entries of data known as values. In some cases the only a single key is sufficient for an application to run or to perform the operations, and sometime it is necessary for an application to open a key and to use the values that are linked with that particular key. There is no limits to the amount of values that a key can have, and neither it's mandatory that values should be in one particular form, values can exists in any form [3].

Since windows registry deals with the critical operations of the windows operating system therefore it's certainly not wrong to say that the operations are directly linked to the system, and user of the windows. Windows registry is critical to this extent that every time when an application runs on a windows machine the first thing that's been done by an application is that its record in registry, it's technically not possible for any application to start without accessing the registry. Just to make things further clear, if at any point registry fails the operating system of the windows machine will fail [4].

2.2 Structure of Registry:

The structure of the registry is basically comprised of the repetition of the same pattern of folders called subtrees, keys and subkeys. The lowest level of data that is stored in the registry are the entries. Entries are similar to the files. The repetitive container leads up to the path to each entry, as every individual entry in the registry has a unique path, every entry that is within the registry is referred by its name and complete path. [5]

For accessing the windows registry in normal condition (Not for forensics investigation) we use windows registry editor tool "regedit.exe". The following section of the research paper is about the components that a typical registry contains.

2.2.1 Subtree:

The subtree is classified as the primary or the root segment of the registry. In a registry there are basically 5 core sub trees, that is further divided in keys, subkeys and entries everything that is within these keys and subkeys it has some values. The name of the value and the data of the value can consist of backslash characters or keys. The 5 main subtree are as follow.

1. **HKEY_CLASSES_ROOT**
2. **HKEY_CURRENT_USER**
3. **HKEY_LOCAL_MACHINE**
4. **HKEY_USERS**
5. **HKEY_CURRENT_CONFIG**

Figure 1: The main keys in a windows registry.

2.2.2 Key:

Once a subtree is expanded the first layer that a viewer can witness is of the key, key is the division of the registry that must contain minimum one subkey (like Hardware Key). One thing that is very important here is that some subtrees does not have a key at all.

2.2.3 Subkey:

The when keys are further expanded to one level down one can view the subkeys. Moreover, there can be subkeys that are directly under the expansion of the keys as mentioned earlier that some subtrees do not have any key, so in such cases those subtrees have subkeys. The role of the subkeys is that it is used to save the entries and additional subkeys.

2.2.4 Entry:

Once the expansion of subtree reaches the lower level in the registry, the entries appear, these entries appear in the right-hand side pane of the registry window. Each registry is consists of the name of the entry followed by the its Data types in the registry (the Data type of the registry is used for identifying the format of the data and the length of the data which is to be stored in the entry) and finally a field which is called value. Data is stored within the value field of the registry. Each entry is identified by its name and path. The role of the entries in the registry is to maintain the configuration information of the windows program and windows itself. Entries are entirely different than subtrees, keys and subkeys as they exists in form of folders only whereas the actual information is within the entries.

2.2.5 Hive Files:

The Hive Files are those files which contains the files that are permanently stored in the registry of the system. The location to check these hive files is in the hivelist subkey in HKLM\SYSTEM\CurrentControlSet\Control. These files are updated every time a user login the system the storage location of these registry files is in systemroot\System32\ Config folder. Within HKEY_LOCAL_ MACHINE there are four to five hive files that are stored, and there is one file that is stored within the HKEY_USERS. The Hive files that are within the registry are as follow:

SAM: SAM basically stands for Security Accounts Manager, it possess data which is stored in HKLM\SAM which is related to the service of security of the Accounts management.

SECURITY: As the name suggests it carries the information that is relevant to the security of the system. The information pertaining to this hive is saved in HKLM\Security key.

SOFTWARE: everything which is relevant to

the configuration of system software configuration is saved in HKLM\SOFTWARE keys.

SYSTEM: This hive file has the information regarding the system configuration the data for this hive file is saved in HKLM\SYSTEM key. **DEFAULT**: The purpose of this hive file is to maintain the default system information, all the data related to this hive is saved in HKEY_USERS\.DEFAULT key.

HKEY_LOCAL_MACHINE\HARDWARE this particular hive is not saved as file as it is recreated by the system every time system boots up.

2.3 Variability of the Registry:

It's certainly not possible that two registries are the same, it's because each registry saves the information about the hardware and the software which exists on the system or is installed, the values that are within the registry entries are precisely according to the system and it's configuration. There are few entries that are only created when the windows machine is turned on or the time when the user log on.

As mentioned before that each entry has a specific location, that location can be changed, sometime it happens when a program is updated. There are few registry which shifts the whole program to new location when a minor change is made to the program such as enabling of one particular service.

Since there is variation in the location of registry it is not advisable for a programmer or script writer to write a script that directly refers to any entry in the registry, this can cause problem in the operations of the program if specifically not pointed to the required registry entry, there is another possibility with registry is that with the change in the version of the registry the program written to fetch specific registry entry might change, for all such purposes the recommended application programming interference (APIs) is win32 API, it's because win32 API is updated each time version is changed.

2.4 How Registry Data is Used:

One of the most important and critical reason to study about registry is how data is stored in Registry or the mechanism of storing data into the registry. There are several types of data that are stored by a program in the registry. As mentioned in the previous section the main stream way of accessing the data by programs is through Win32 API. Each program working in relation with registry, uses API where the whole function of this API is to retrieve the data from the required entry path and the name from the registry. For making any change to the content of the registry programs uses standard APIs which are compatible with the operating system.

Once the data is fetched using the APIs, the data is interpreted and implemented according to the functionality of the program. For instance if "1" is obtained as a result in the value it might means to enable or disable one particular feature of the program, which was previously operating other way. If in the value of the registry a file location is stored that might means that to save the program to the specified location or move the program to the specified location after the execution of the program.

In windows specifically the windows Server 2003 or higher Operating system the registry is used by the programs and the component of the operating system for the following purposes.

Setup: This includes the setup programs that

are for windows server 2003 or the setup program that are required for other hardware to be installed on the PC, the configuration is added to the registry e.g. every time new information is added to the registry when SCSI adapter is installed or the settings of the display are altered. Moreover, all the components are first read by the registry to ensure that all the prerequisite for installation are available.

Recognizer: Every single time when computer is turned on, the role of recognizer starts it puts the configuration of hardware data in the registry. The hardware configuration data includes the list of hardware that are available on system. The operation of hardware detection is carried out by windows kernel (Ntoskrnl.exe) programs and hardware recognizer (Ntdetect.com).

The role of the kernel program during startup of system is to ensure that the information related to the device is extracted from the registry this information includes the drivers that needs to be loaded and the sequence in which the drivers are supposed to be loaded. Another important feature of the kernel is reveal its own information to the registry, such as what kernel version currently it is, that's being used by the system.

Device Drivers:

The load perimeters along with configuration data is sent and received by the registry through device drivers. The role of the device driver is to report the information regarding the usage of system resources to the registry like the hardware interrupts or DMA channels that are utilized by one particular program. Registry information can be accessed by the device drivers or program so that smart installation and configuration can be provided to the user.

Since there is variability in programs, it is therefore very hard to know how a particular program will interpret the data of the registry. Registry entries are strictly dependent on program not the user, therefore one must not try to alter any registry entry of any program unless he/she is quite sure about the program.]

2.5 Users and the Registry:

For most of the programs today, there is hardly any need of user to go to registry for editing purposes for any particular task, from changing preferences to changing the features and services of program it is all done by the administrative tools and windows interface for the ease of the user. However, there are few rare cases where users has to go to registry settings to make changes to the instance of the operating system.

3. Windows Registry Forensics:

One of the essential steps that's being carried out in computer forensics is related to the analysis of the digital evidence, here at analysis stage different aspects are analysed which includes, the processes that are running on the ram when computer device was taken into custody, the files that are within the system and the files that were deleted, and windows registry analysis. [5]

When it comes to the analysis of windows registry it not only includes the viewing of data that is in registry, but it also involves the extraction and interpretation of data with respect to the context of investigation and with respect to its existence. Therefore, firm knowledge and understanding about the components of the registry is required. [3]

In the initial phase of the investigation several keys should be analysed. The key which should be examined includes the keys which

store the basic information related to the system, information related to the user, information related to the installed applications on the system, moreover, the information should include what drives were mounted on the system and what hardware components have been configured and installed on the system [6].

This process of analysis should be done in a proper sequence to make sure that the process of investigation is completed smoothly. The order of this investigation is as follow.

HKEY LOCAL MACHINE\Software:

In the preliminary phase of investigation, the most important thing is to know about the system and its owner. For digital evidence it is said that the more information that you get is more beneficial for you because it makes the analysis process easier. Before carrying out the forensics investigation it is mandatory to make sure about the directory and its path in which the windows operating system is installed and at same time it is important to know about the owner of the system. The HKEY LOCAL MACHINE\Software key has the information about the software that are installed on the system. Several keys are under this particular hive, the content of this hives can vary from system to system as everyone is not using the same software. Under this software hive there is a subkey of Microsoft\ Windows NT\Current Version subkey that is critically examined and special consideration is given to the data that is found within this particular subkey, because it contains important information related to the software installed, some of the important keys are as follow

- **CSDVersion:** The data that is found inside this value is related to the service pack installed. Windows boot loader use this key along with the **Current Version Key and Current Build Number key**: As every software or a patch has a build number or version so that it can be easily differentiated if it was created before certain time or after that particular time [7].

- **InstallDate**: As the name of the value suggest that this value has to do something with the time stamp which is very important in the forensics investigation, this particular value contains the information related to the date and time when the operating system was installed. The value is stored in Hex form. There are some tools that are used to decode this hex value for knowing the exact date and time when OS was installed, so that if the suspect has formatted the hard drive and has installed the windows again this could be determined.

- **PathName and SystemRoot**: The values within this subkey reference to the system directory. The default directory for system is %SystemDrive%:\Windows.

- **ProductID and ProductName**: The data within these values contains information related to the product key of the Microsoft product that is usually the one that's given as product key on the CD of Microsoft products. These values are the Microsoft product ID and a product name. Whereas the product name is simply the name of the operating system.

- **RegisteredOwner and Registered Organization**: Within these values the information that is stpred is related to the users and the organisation that is using these software in most of the cases it's the information of the actual owner of the software who is using theses software,

these values can be changed as it's under the control of the user every time a fresh installation process is carried out the program asks for the users details, which user has to enter.

- **NetworkCards**: The MAC address of network cards and the name of the particular network card linking to the MAC address is placed within this value. When the MAC address of the network card is deliberately changed during the course of hacking a new subkey is added, and from here we can investigate if the MAC address is changed.

HKEY LOCAL MACHINE\System

Once the information pertaining to the owner and system is gathered, the next step for the investigator(s) should be to check the configuration settings of the machine, and this is where we need to check HKEY LOCAL MACHINE\System hive, this hive maintains information related to the configuration setting that is required for booting the system and several other critical features required for the operations of the system. Some of the important subkeys that are within this hives are as follow [8].

Control:

The subkey of control has the information regarding the controls of the operating system with respect to its operations from booting of an operating system to the networking of the system to windows to windows on windows (WOW). Time zone, system boot date and time, with shut down date and time can be found through this subkey.

• **Enum:** This subkey has the information related to the hardware aspect related to the system, this includes the state of the hardware, legacy devices, and the long list continues. Moreover, settings related to the external storage devices are stored in this key. The accuracy of the information in this subkey is that it gives the exact name, and the model number of the storage device attached to the system. Now if the investigator further wishes to know when the device was installed, he can refer to the windows event log.

ControlSet001: It is one of the main control set, which is used by the default to boot the windows operating system.

ControlSet002: In case windows is unable to boot using controlSet001 this is backup control set which can be used. There are is possibility that there could be more than two numbered control set. There is a possibility that due to the variation in the registry Controlset002 may not appear but may be controlset003 appear as a backup control set. The setting of every control set may vary, so therefore it is highly recommended for an investigator to keenly observe the control setting of the Select subkeys.

Select:As cautioned earlier that if the investigator has to find out which control set setting are used at the boot of windows OS he must check the Select sub key. The role of this subkey in registry is to store information that a control set use to boot a computer. The select hive key contains the four subkeys, the Current, Default, Failed and the LastKnownGood. Among these 4 the current subkey is the one that has the value of the ID of current control set which is used for booting the windows. This is the reason it is important for an investigator to thoroughly check control set before examining the other configuration settings.

Mounted Devices:
The role of this subkey is to list the volumes/drives that have been attached to the system, because of this subkey one can determine the number of partition that were within the system and the auxiliary disks that were attached to the system inform of CD/DVDs drive or any other external medium like USB. This is another point at which the investigator should be cautious as this will show the investigator about the drives that are missing at the time of taking system image into the custody. [9]

HKEY LOCAL MACHINE \ System \ Control Set \ Enum:
Moreover, this Enum subkey contains information related to each devices, services, and drivers that might have been attached to system at any particular point. There are several services that an Enum entry may contain like entry of ATAPI driver even if there is no ATAPI interface on that machine. The purpose of these keys is to map devices and service to the relevant drivers and configuration on the system.

• **USBSTOR**: The role of this key is very significant and one of the most important role as it contains information about all the USB devices that has ever been attached to the system, even if it was not connected at the time of seizing the system. Each key has a subkey that contains the information about USB device such as the ID of the Hardware, Friendly name of the device and some other information related to USB the purpose of hardware ID and friendly name is to highlight the manufacturer name and model name. The moment when the forensics investigator figures out that the path of the file links to an external USB storage device, he should look into this subkey and should take appropriate steps, to know about the device(s) that were attached to the system [10].

Services\%AdapterGUID%\Parameters\Tcpip:
In case of attack related to the intrusion in the network or circulation of the malware within the network, this subkey is not less than a gem for the investigator as this subkey contains a lot of valuable information, as it contains the parameter linked to the TCP/IP network. The IPAddress mentioned in this subkey is the actual IP address that is allocated to the network adapter card. The Default Gateway contains the IP address of the gateway linked to the network.

4. Conclusion

Undoubtedly Windows registry has one of the important role in the forensics investigation of personal computers. As the components within the registry contains the important information related to the operations of the computers whether it is linked to hardware of the system, software of the system, drivers installed on the system, or the time stamp every aspect that is within the registry of the windows operating system is critical to the investigation. Just like in any other investigation where minimal things carry great importance [11] Windows registry forensics carries great importance as well.

5. Reference

[1] Harlan Carvey, “Windows Registry Forensics Advanced Digital Forensic Analysis of the Windows Registry”, Syngress Elsevier Inc, Burlington, pp 20, (2011).

[2] Khawla Abdulla Alghafli, Andrew Jones, Thomas Anthony Martin. 2010, “Forensic Analysis of the Windows 7

Registry", Edith Cowan University Research Online. Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1071&context=adf

[3] Microsoft (2018), "Structure of the Registry", [online] Microsoft Windows Dev Center. Available at: https://docs.microsoft.com/en-us/windows/desktop/sysinfo/structure-of-the-registry

[4] Abhijeet Ramani, Somesh Kumar Dewangan (Nov 2014), "Digital Forensic Identification, Collection, Examination and Decoding of Windows Registry Keys for Discovering User Activities Patterns" International Journal of Computer Trends and Technology (IJCTT) volume 17 number 2–Nov2014. Available at: https://mafiadoc.com/ieee-paper-template-in-a4-v1_59f365cc1723dd8ee9ed8ea4.html

[5] Microsoft (2009), "Overview of the Windows Registry", [online] Microsoft Windows Dev Center. Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781906(v=ws.10)

[6] Yang, S., Wang, L., Zhang, S., & Liu, J. (2013). "A Method on Extracting Registry Information from Windows CE Memory Images", 2013 International Conference on Computer Sciences and Applications. Available at: https://ieeexplore.ieee.org/document/6835701

[7] Saidi, R. M., Ahmad, S. A., Noor, N. M., & Yunos, R. (2013). "Windows registry analysis for forensic investigation." 2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE). Available at: https://ieeexplore.ieee.org/document/6557209

[8] Chang, K., Kim, G., Kim, K., & Kim, W. (2007). Initial Case Analysis Using Windows Registry in Computer Forensics. Future Generation Communication and Networking Available at: https://ieeexplore.ieee.org/document/4426183

[9] Shuhui Zhang, Lianhai Wang, & Lei Zhang. (2011). Extracting windows registry information from physical memory. 2011 3rd International Conference on Computer Research and Development. Available at: https://ieeexplore.ieee.org/document/5764089

[10] Deb, S. B., & Chetry, A. (2015). "USB Device Forensics: Insertion and removal timestamps of USB devices in Windows 8." 2015 International Symposium on Advanced Computing and Communication (ISACC). Available at: https://ieeexplore.ieee.org/document/7377371

[11] Dr Aftab Ahmed Malik, International Journal For Electronic Crime Investigation (IJECI) Volume 1 2017. Available at: http://lgu.edu.pk/dfrsc/journal/Journal-IJECI.pdf

Suleman *et al.LGU (IJECI)* 2018

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Classification of Website Phishing Data through Machine Learning Algorithms

Muhammad Taseer Suleman
Lahore Garrison University, Lahore, Pakistan
taseersuleman@lgu.edu.pk

Abstract:

Phishing is the dissemination of malicious web sites used to acquire passwords, credit card details or any sensitive personal information. Clients of web advancements deal with different security dangers and phishing is a standout amongst the most imperative dangers that should be addressed. Phishing sites have certain attributes and designs, in order to, distinguish those components that can help us to recognize phishing. In order to, recognize such elements information mining methods have been utilized. In this work, we depicted examination in arrangement of phishing sites utilizing diverse classification algorithms with genetic algorithms for enhancement, for example, as feature selection and generation. Keeping in mind the end goal to figure out which technique gives the prime outcomes in phishing sites characterization. Websites are characterized as “1” for "Legitimate”, “0” for "Suspicious" and “-1” for "Illegitimate". We have found that machine-learning algorithms along with feature selection algorithms were the best choice for detecting web phishing attacks.

Keywords: Phishing, Spamming, Features, Machine learning algorithms, Genetic algorithms.

1. Introduction

Web phishing is a mechanism of online fraud in which the victim is deceived by the attacker in gaining victim’s personal information like credit card number, financial accounts, address, phone numbers etc. The assailant makes a fake site page by replicating or rolling out a little improvement in the honest to goodness page. The fake sites are planned to look precisely like the bona fide site. The fast advancement of web applications give a ton of advantages to web clients to use these web application for making all their everyday exercises, for example, newspaper perusing, shopping, payment of many types of bills, ticket booking, and amusement and so forth. However, artisan create novel assaults that draws in more web client to be gotten in web of phishing. As per Gupta et al. [1] the entire number of specific phishing sites recognized in the primary quarter of 2014 alone was 125,215, delineating an expansion of more than 11% from the 2013 figures. While a greater part of the phishing effort utilizes malevolently enrolled areas and sub-spaces, they have made genuine money related harm

clients over the globe. Moreover, there had been a huge year on year increment in phishing assaults, which is appear in figure, expanding altogether from 203,983 of every 2013 to 448,126 of every 2017.

As indicated by the Anti-Phishing Working Group (APWG), the APWG Got reports of 630,494 extraordinary phishing locales recognized from the main quarter through the second from last quarter of 2017. The around the web phishing rate was 36.511% in the primary quarter, 32.211% in the second quarter, and 32.122% in the second from last quarter of 2017. Besides, ISP area observed to be the most under assault industry area from first to second from last quarter of 2017 as appeared in Fig 1 below.

Fig 1 Phishing detection rate in 2017

Web phishing attack is comprises for many stages. The choice of victim and the amount of benefit are important parameters in web phishing attack.
Phishing life cycle has following stages:

i. Planning and Setup

In first stage, the phisher determine the objective association, an individual or a country to be targeted for malicious purpose. They uncover the sensitive information with respect to their objective and its system. Normally phishing starts by sending spoofed emails to the victims [2]. Victims are supposed to send required information via replying to the email. However, most of the users do not reveal their information through email.

Another phishing technique can be adopted through creation of phishing websites. A combination of both aforementioned techniques can also be used for phishing as well [3] as shown in Fig 2.

Fig 2 Web-Phishing whole Plot

ii. Phishing

Assailants send mock messages to the dupe, utilizing gathered email tend to which request classified data from the dupe. Another special form of phishing is known as spear phishing. In spear phishing, target is generally a group of specific individuals. In addition, there are many other forms of phishing as depicted in Fig 3.

Fig 3 Different types of Phishing

iii. Break-in or Infiltration

In this stage, the victim taps on the pernicious connection and when he does that, a malware

naturally introduces on his gadget that enables the phisher to get to the system, irrupt and change its arrangements and get to rights to it.

iv. Information Accumulation

When the phisher access on victim's system, they remove the required information. On the off chance that the casualty gives classified record points of interest, the assailant would then be able to get to his record, which may, in the end, prompt budgetary misfortunes to the casualty. Once the attack is successful, the attacker does the information collection. Information may contain passwords, user identity number, contact lists, private images, and credit card information. The whole phishing life cycle is shown in Fig 4.

Fig 4 Scenario of web phishing

Detection of phishing website is a problem of major concern. Various techniques such as fuzzy, neural systems and data mining methods applied, in order to, counter web-phishing attacks [4]. Several machine-learning methods also applied for detection of fake websites. Machine learning approach is based on both supervised as well as unsupervised. We have tested many machine-learning algorithms on the given data downloaded from UCI machine learning dataset. These algorithms include Naïve Bayes (NB), Support Vector Machine (SVM), Neural Net (NN), Random Forest (RF), IBK lazy classifier and Decision Tree (ID3). However, we have observed that phishing detection results can be enhanced by applying feature selection algorithms like Generating Genetic Algorithms (GGA), Another Genetic Algorithm (AGA) etc. In the end, we have shown the difference of accuracy between the results of those machine-learning algorithms applied to the data to those machine-learning algorithms used with feature selection algorithms.

The rest of research article is organized as follows: section II contains the previous related research work. Section III describes methodology of our work. In Section IV we have shown the results. In section V we have concluded our work.

2. Related Work

In [5] Tahir et al. have proposed a hybrid model, in order to, overcome phishing issue. Their proposed hybrid model show beats as far as high precision and less mistake rate. They completed tests in two stages. In the first stage, they separately performed classification algorithm and select the best three models on criteria of execution and high precision. In the second stage, they additionally consolidated each model with their best "Three" singular models.

In [6] authors have proposed the classification algorithm named as PAC (Phishing Associative Classification). They observed the execution of proposed calculation in term of precision measurements with four well-known calculations that are C4.5, PRISM, CBA, and MCAR.

In [7], Authors have portrayed examination in arrangement of phishing sites utilizing

distinctive Machine learning calculations. They have applied various machine learning techniques including Random Forest (RF), C4.5, REP Tree, Decision Stump, Hoeffding Tree and Rotation Forest. From the outcomes, it has been discovered that the Rotation Forest calculation with REP Tree as a classifier and MLP plays out the best on a full preparing and on diminished set, separately.

In [8] authors have utilized information-mining approach like supervised characterization, which enhances the frameworks precision and distinguishes more measure of spam and harmful URLs.

Google in [9] gives a support of safe perusing that enables the applications to check the URLs utilizing a file of suspicious areas, which is consistently refreshed by Google. It is a trial Programming interface, however, is utilized with Google Chrome and Mozilla Firefox, and it is anything but difficult to utilize.

Authors in [10] connected distinctive sorts of machine learning based arrangement calculations, including Naive Bayes (NB), Support Vector Machine (SVM), Neural Net (NN), Random Forest (RF), IBK relaxed classifier and Decision Tree (J48) and broaden Pradeep and Ravendra's work by presenting new order calculation named Neural Net in their test. In the end, they Shield clients from nasty or unstructured connections in Site pages and Texts.

Measured and looked at the execution of the classifier as far as precision. Neural Net demonstrated a decent order exactness contrast with others.

Authors in [11] proposed another calculation Linkguard calculation to give up from phishing assaults. This calculation utilizes attributes of hyperlinks to deduct the attacks. Linkguard algorithm examines the contrast between the visual connection

and genuine connection. Link Guard is valuable for recognizing phishing assaults, as well as can shield clients from nasty or unstructured connections in Site pages and Texts.

3. Methodology

In our work, we utilized dataset for the examination is "Phishing Websites Dataset" ("UCI Machine Learning Vault: Phishing Sites Informational collection," 2016) [12]. This dataset was accumulated fundamentally from Phish Tank archive, Miller Smiles archive, and Google’s seeking administrators.

The dataset is separate into training (70%) as well as testing (30%) datasets. Dataset includes total 11054 instances. All occasions sorted as “1” for "Real”, “0” for "Suspicious" and “-1” for "Phishy". We have used Python 3.6 for data analysis.

The creators illuminate the key features that have been turned out to be strong and effective in foreseeing phishing sites while proposing some new features, tentatively allocating new standards to some outstanding features and refreshing some different features.

Features have been grouped into following categories:

- Address Bar-based features
- Abnormal based features
- HTML and Javascript Based features
- Domain Based Features

The address bar based features is a heuristic approach towards web phishing detection [13].

Abnormal based feature includes abnormal URL, anchor URL, abnormal DNS etc. [13]. We have conducted few experiments on our data in terms of its covariance, variance.

In Fig 5, we have shown various characteristics of our data.

These characteristics include total count, mean, standard deviation (std) and data range (min & max). Therefore, analysis between different features is easy enough.

	having_IP_Address	URL_Length	Shortining_Service	having_At_Symbol	double_slash_redirecting	Prefix_Suffix	having_Sub_Domain	SSLfinal_State
count	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000
mean	0.313914	-0.633345	0.738737	0.700561	0.741632	-0.734938	0.064049	0.251040
std	0.949495	0.765973	0.674024	0.713625	0.670837	0.678165	0.817492	0.911856
min	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000
25%	-1.000000	-1.000000	1.000000	1.000000	1.000000	-1.000000	-1.000000	-1.000000
50%	1.000000	-1.000000	1.000000	1.000000	1.000000	-1.000000	0.000000	1.000000
75%	1.000000	-1.000000	1.000000	1.000000	1.000000	-1.000000	1.000000	1.000000
max	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000

	Domain_registeration_length	Favicon	...	popUpWidnow	Iframe	age_of_domain	DNSRecord	web_traffic	Page_Rank	Google_Index
count	11054.000000	11054.000000	...	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000	11054.000000
mean	-0.336711	0.628551	...	0.613353	0.816899	0.061335	0.377239	0.287407	-0.483626	0.721549
std	0.941651	0.777804	...	0.789845	0.576807	0.998162	0.926158	0.827680	0.875314	0.692395
min	-1.000000	-1.000000	...	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000
25%	-1.000000	1.000000	...	1.000000	1.000000	-1.000000	-1.000000	0.000000	-1.000000	1.000000
50%	-1.000000	1.000000	...	1.000000	1.000000	1.000000	1.000000	1.000000	-1.000000	1.000000
75%	1.000000	1.000000	...	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
max	1.000000	1.000000	...	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000

Fig 5: Count, Mean and Standard Deviation of each dataset feature

In the next step, we have applied different machine learning techniques on our dataset. The dataset, as earlier said, was used to foresee the exactness of the acknowledgment using assorted classifier. For the earlier examination, the component assurance is not used and just classifiers are used to get the required accuracy for each of the classifiers. The data is obviously portrayed however this time particular segment decision methodologies are used for the update of the results or to check for any possible upgrades. The usage of feature decision procedures furthermore help in dimensionality diminish as feature reducing.

In Fig 6, we have correlated each feature name with a feature ID. In this study for feature selection algorithm, we used Generating Genetic Algorithm (GGA), Another Genetic Algorithm (AGA), Yet Another Generating Genetic (YAGGA) and Yet Another Generating Genetic Algorithm-2 (YAGGA2). The classifiers utilized were Naïve Bayes, ID3, KNN, Decision Tree, and Random Forest. The Characteristics of highlight choice calculations are that they select the best components on the premise of properties weights.

Feature Name	Feature ID
IP_Address	A
URL_Length	B
Shortining_Service	C
having_At_Symbol	D
double_slash_redirecting	E
Prefix_Suffix	F
having_Sub_Domain	G
SSLfinal_State	H
Domain_registeration_length	I
Favicon	J
Port	K
HTTPS_token	L
Request_URL	M
URL_of_Anchor	N
Links_in_tags	O
SFH	P
Submitting_to_email	Q
Abnormal_URL	R
Redirect	S
on_mouseover	T
RightClick	U
popUpWidnow	V
I frame	W
age_of_domain	X
DNSRecord	Y
web traffic	Z
PageRank	AA
Google Index	AB
Links_pointing_to_page	AC
Statistical_report	AD
Result	AE

Fig 6: Each Feature get associated with a unique ID

Based on the above features in our dataset, we have conducted series of experiments that involved two streams.

1. Machine learning algorithms along with Feature Selection
2. Machine learning algorithms without Feature Selection.

These both streams involved series of stages involved in them with difference of one or more stages. The details of all stages involved are as follows.

V. Read CSV: A simple method involved is the reading of CSV. A comma-delimited Phishing.CSV is given as an input to the system. The data contains as many as 11054 instances.

VI. Cross-Validation: It is a statistical method, which involves evaluation and comparison of learning algorithms through dataset division [14]. The division of dataset brought two segments: Train dataset and Test dataset. K-fold cross-validation is the basic form of cross-validation. In our case, we have also cross over our data through cross-validation also known as X-Validation. The division between train dataset and Test Dataset also came into practice.

VII. Testing: After Cross validation data is passed through the Testing stage. Testing stage involves the application of multiple machine learning algorithms on the specific data [15].

VIII. Classifier: Classifier used to perform classification on the given data. Classification is actually the task of mapping function from input features to finite output values [16]. In our case, our task is to classify the given data according to Phishy, non-phishy (normal) instance based on the previous data learning. In our case, the classifiers are Naïve Bayes, ID3, KNN, Decision Tree and Random Forest.

IX. Model Application: After then we apply different models to our dataset based on the aforementioned various models.

X. Feature Selection: As we have mentioned before, our testing, analysis and result generation based on the comparison of two streams. One with Feature selection and other without feature selection. This is an important stage in the data analysis. Feature selection aims to choose a subset of feature from the available features [17][18]. We have used feature selection algorithm like GGA, AGA, YAGGA, YAGGA-2. We have used these feature selection algorithms along with classification algorithms. In result section, we will show the effect of performance with and without using feature selection algorithm.

XI. Performance: Performance is measured against all the stages that we have mentioned above. This would be the last stage of each stream. Results had been collected and compared, in order to, find best.

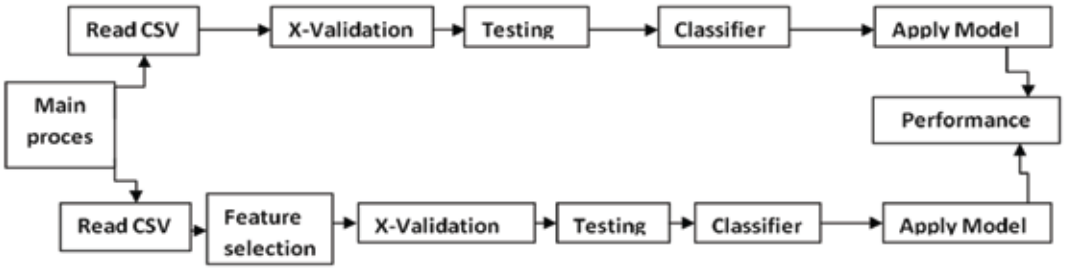


Fig 7: Model for applying Machine learning algorithms with & without Feature Selection Algorithms

4. Results and Discussions

In stage 1 classifiers i.e.; Naive Bayes, ID3, KNN, Decision Tree and Random Forest and are utilized to get the required exactness for each of the classifiers. In stage 2 the information is, on the other hand, characterized yet this time distinctive features strategies i.e.; GGA, AGA, YAGGA, and YAGGA2 are utilized for the upgrade of the outcomes or to check for any believable changes. Results demonstrate that ID3 with YAGGA with 15 features chosen, lessened from 30 highlights, demonstrate the best execution on this dataset for order of phishing sites. The results are shown in Fig 8 with "YAGGA + ID3" shows the maximum accuracy up to 95%.

Classification Algorithm	Unprocessed Data	Feature Selection Algorithms			
		GGA	AGA	YAGGA	YAGGA2
Naïve Bayes	91.08%	93.31 %	75.53 %	92.94%	73.53%
ID3	87.16%	94.63 %	75.53 %	94.99%	74.5%
KNN	89.51%	92.55 %	73.53 %	94.72%	73.53%
Decision Tree	91.65%	94.00 %	59.51 %	93.18%	86.04%
Random Forest	76.33%	89.27 %	57.88 %	92.46%	85.92%

Fig 8: Results of accuracy

5. Conclusion and Future work

Web Phishing attack is of serious concern. This work models the phishing site expectation as a characterization undertaking and exhibits the machine learning approach for foreseeing whether the given site is genuine site or phishing. The phishing dataset was taken from UCI learning website. The dataset contains as many as 11054 instances. In this research, several machine learning algorithms. The results were compared with the application of same machine learning algorithm along with feature selection algorithm. It has been noted that YAGGA along with ID3 has given the best results with approximately 95% accuracy of website phishing detection. In future, we will extend this work for other famous website attacks with the help of machine learning algorithms.

6. References

[1] W. Zhuang, Q. Jiang and T. Xiong,"An Intelligent Anti-Phishing Strategy Model for Phishing Website Detection," 32nd IEEE International Conference on Distributed Computing Systems Workshops, 2012, China.

[2] B. B Gupta, A. Tewari, A.K. Jain, D.P Agrawal," Fighting against phishing attacks: state of the art and Future challenges," Neural Computing and Applications, Vol 28 Issue 12, December 2017.

[3] C.E Drake, J.J. Oliver, E.J. Koontz," Anatomy of a Phishing Email," CEAS, 2004.

[4] G. Varshney, R.C. Joshi, A. Sardana,

”Personal Secret Information Based Authentication towards Preventing Phishing Attacks,” In: Meghanathan N., Nagamalai D., Chaki N. (eds) Advances in Computing and Information Technology. Advances in Intelligent Systems and Computing, vol 176. Springer, Berlin, Heidelberg

[5] M. Islam, N.K. Chowdhury,” Phishing Websites Detection Using Machine Learning Based Classification Techniques.

[6] M.A.U.H Tahr, S. Asghar, A. Zafar, S. Gillani,” A Hybrid Model to Detect Phishing-Sites using Supervised Learning Algorithms,” International Conference on Computational Science and Computational Intelligence (CSCI), 15 Dec 2016, Las Vegas, NV, USA.

[7] S.Wedyan, F. Wedyan,” An Associative Classification Data Mining Approach for Detecting Phishing Websites,” Journal of Emerging Trends in Computing and Information Sciences, Vol. 4 No.12, Dec 2013.

[8] A. Hodzic, J. Kevric, A. Karadeg,” Comparison of Machine Learning Techniques in Phishing Website Classification,” International Conference on Economic and Social Studies, April 2016.

[9] S.B Rathod, T.M. Pattewar,” A comparative performance evaluation of content based spam and malicious URL detection in E-mail,” IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS), 2015.

[10] Google safe browsing API Available. Retrieved 1st June 2018 from https://developers.google.com/safe-browsing/.

[11] J. James, L. Sandhya, C. Thomas,”Detection of Phishing using machine learning techniques,” International Conference on Control Communication and Computing (ICCC), December 2013.

[12] G. Varshney, M. Misra, P.K Atrey,”A survey and classification of web phishing detection schemes,” Security and Communication Networks, Wiley Online Library, October 2016.

[13] G. Varshney, M. Misra, P.K Atrey,”A survey and classification of web phishing detection schemes,” Security and Communication Networks, Wiley Online Library, October 2016.

[14] Phishing Dataset. Retrieved on 25th April 2018 from https://archive.ics.uci.edu/ml/datasets/phishing+websites

[15] M.G. Alkhozae, O.A. Batarfi,” Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code,” International Journal of Information and Communication Technology Research, Vol 1No.06, October 2011.

[16] S. Arlot, A. Celisse,” A survey of cross-validation procedures for model selection,” Statistics Surveys, Vol 4, 2010.

[17] How to evaluate Machine Learning Algorithms. Retrieved 2nd July from https://machinelearningmastery.com/how-to-evaluate-machine-learning-algorithms/

[18] F.Y. Osisanwo, J.E.T. Akinsola, x O. Akinsola , J. O. Hinmikaiye , O. Olakanmi , J. Akinjobi,” Supervised Machine Learning Algorithms: Classification and Comparison,” International Journal of Computer Trends and Technology (IJCTT), Volume 48 No. 3, June 2017.

Munir *et al.LGU (IJECI)*2018

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Social Media and its Impact on our Privacy

Sundus Munir[1] and Hafsah Tariq[2]
Lahore Garrison University, Lahore, Pakistan
sundusmunir@lgu.edu.pk[1], hafsatariq573@gmail.com[2]

Abstract:

Social media is one of the advance technologies which is very common now some days. Social media means open source contents for all over the world. It is on the peak and extremely popular from recent years. Millions of users use the social media on daily basis and share their personal information on the media through the internet. That encourages the attackers to attack on someone's personal data by using different methods like Botnet, Phishing scams, Malware attack, Malicious attack etc. Due to this, both the administrator and the users suffer a lot. It happens because the users are not familiar with the security and privacy terms and conditions. They don't even bother to secure their personal data before sharing it on social media. In this research paper we present the consequences, side effects, usages and its impact on our private lives. It also presents how users can secure their data from attackers and the techniques they can adopt to protect their content.

Keywords: Cyber bulling, Phishing scam, Backlash, Malware, Spyware.

1. Introduction

Social media plays an important role in our daily lives.

[1]. Social media is basically a source that connects the people to the whole world through internet. Social media is commonly used throughout the world in the form of Facebook, WhatsApp, Twitter, Email, Google, Skype, Instagram etc. These are the few applications through which people connect with each other. Social media give useful information to the users related to the whole world and helps out the users to stay connected with the world. **[2]** No doubt social media makes the life of the people much easier. That's why with the advanced technology we have an increasing number of applications that are making people's lives much easier. They forget that every useful thing may also have lots of side effects. In case of social media there are also some serious issues regarding to the privacy and security of the personal content of the users which may cause several problems. The primary thing that comes as an issue is account hacking of the user. Attacker can easily attack the users through websites. The users click on different links without knowing those websites, later on their system is infected and they have to suffer a lot. Attackers are interested in that type of users which are social media lovers and continuously using the social

media content and technologies. This kind of users are an easy target for attackers. Another problem is stalking and harassment. These threats do come from the attackers or any strangers. Mostly stalking and harassment is done by the family members, friends and people around us in our surroundings. Same like the pokes and bully criteria. Another serious problem is being compelled by the organization to turn over the password. This is mostly done when the person is going to start a new job. Another issue is of location-based services. **[3]** Nowadays a number of users use smart phones and all their activities are usually done by the smart phones. Hacker can easily attack the people through their smart

phones by accessing their location-based services. Lots of the apps which are downloaded on daily basis ask for location information and their numbers are increasing day by day. Hackers can also attack the users through these apps. Last but not the least problem is phishing attack. This attack is done by giving fake policies and sending fake friend requests through Emails, Facebook and other sources. Now the question is how to protect ourselves from these attacks? Simply by creating a policy of social media. It can be done by creating different policies, training the users for using the social media in a secure way or by giving limited access to the social media. Through these solutions users can protect themselves from the hackers and other problems. These are the few problems which impacts on the user's privacy. The detailed problems and solutions emerging because of social media including the definition of the term is discussed below.

2. Social Media

"Social" in social media means "conversation". The difference between social media and TV is that viewers are engaged with the makers of the shows which they are watching. In a brief timeframe TV program are supplanted by the web based life world. **[4]** In online communication and conversation users share their opinion and build relationships. Users share their posts, videos, audios and photographs. It involves a combination of technology, telecommunication and social interaction. It is the different form of communication as compared to film, television and newspaper.

3. Privacy

Privacy means the information or data that a user does not want to disclose and share with others. [**5]** It is basically that kind of information that has potential to be misused. It can be the info of a group or individual. If we talk about an individual's privacy, it depends upon the user whether to share his personal information with others or not and in which manner to share that information. It is basically an ability of an individual or a group to share information about themselves. The limitations and materials of the privacy differ among individuals.

4. Purpose of Social Media

Social media is not only used for communication but it can also be used for business connections and promotions**. [6]** By using it user cannot only find the other users but also the organization in which they are working. The purpose of social media is to provide a platform to the users and business industry to come and interact with each other directly. A business can be well promoted through social media.

5. Attack on our Privacy through Social Media

5.1 Human Error

Human error is involved when somebody makes a slip that causes an accident or causes something dangerous to happen. By clicking on any unknown website accidently which is not safe can harm the privacy of user.

5.2 Malicious Attack

This attack is due to malware and spyware that causes the disaster. **[7]** According to a research report, about 4,000 attacks happen on daily basis through malicious attackers. It can spread through emailing, or visiting different unknown websites.

5.3 Phishing Scams

It is a kind of attack on social media which attacks the user's personal information like banking details and passwords. Hackers get access to the personal stuff using that specific information and harm to the people.

6. Privacy Issues in Social Media

Privacy attacks are when unauthorized user tries to enter in your account and get some private data. Anyone which is closer to you in family can access your account details by just simply watching your password**. [8][9]** The main issue of the privacy is that large amount of information processes each day without any limitation.

6.1 Challenges to Social Media

There are many challenges social media is facing today, few of them are

- Cookies
- Bugs
- Spyware

7. Impact on Social Media and Invasion of Privacy

One of the very positive impacts of social media is that it provides a platform to geographically distributed users to come on single platform and share their views. Every user has freedom to express their views. The information can be easily spread by one medium to another without using any other source. Usually users don't pay much attention to the privacy and secrecy issues to the websites. **[10] [11]** Government Agencies has rights prior to the knowledge of the user to access the personal information of the user. FBI and NWC3 are the agencies that work for cybercrimes and arrest the cybercriminals. People who hack private details of the user and misuse that information for their personal benefits are criminals. There is strict punishment for the criminal of almost 5-20 years of jail with heavy fine that is unable for a common man to pay.

8. Negative Effect of Social Media on Society

Social media build a false sense of connection according to the Cornell University Steven Strogatz**.**

[12] Report States that it becomes more difficult for user to find a real relationship in the world. Users focus more on fake relationships on social media without knowing each other. By focusing on such websites most of energy is wasted and most importantly the connection between the families becomes weak. Cyber bulling is spreading rapidly nowadays in our youth. According to the CBS News report in 2010 **[13]** 42% of the children are harassed online and become victim.

Another negative impact of social media is that seller companies show somethings and sell different things. There is obviously decrease in productivity in doing so. That makes sense of fraud to the customers.

9. Risk for Youth using Social Media

There are many categories of risk. Following are few of them that are very common for adolescents.

9.1 Online Harassment and Cyber Bulling

Cyber bulling is one of the common ways of communication in which offline harassment is done. **[14]** Which can cause depression, anxiety or may even lead to suicide, etc. whereas online harassment is that where cyber bulling is done openly in front of whole world.

9.2 Sexting

It means sending and receiving the sexual messages, photographs and posts online on the social media that disturbs the other users. This phenomenon is very much popular in the teenage population. According to a research **[15] [16]** 20% of the users who are in their teenage share the sexist videos and text messages online.

9.3 Face book Depression

Researchers nowadays call Facebook with a new name that is face book depression. Most of the teenagers spend almost half of the day on social media using Facebook, different websites are engaged on other false activities. Which later turn into aggression, depression, anxiety and sometimes suicide. Sometimes social media become risky for the users especially if they are novice.

10. Reduce the Impact of Social Media in Life

According to recent research of APS (Australian psychology society) teenagers are highly involved in the social media life, their ages are from 14-19 years and one of the half adults involve in the social media through their mobile phones. They usually use social media 5 days in a week for long hours. **[17]** Using too much social media can affect the self-esteem of the users /youth and put a very bad impact on their lives. Researchers says that 42% of the users use social media on bed before sleeping. It badly affects the health e.g. back bone problem, sleep disorder etc. **[18]** Most of the complaints registered by the teenagers are of harassing and being black mailed by the strangers. The reason is that the 60% of the parents don't give time to their children or don't monitor their child activities on social media. Due to this reason their children get caught by some strangers on social media who harass them by hacking their accounts and get their personal life information. Adolescents don't have idea how to protect themselves and how to use the social media in secure way. For this purpose, parents need to monitor their child on online world. For this purpose, parents may follow few tips:

- Parents must connect with their child through Facebook, Twitter and other accounts on social media. So that they check, what their child is posting online and which YouTube channel they are following. Due to these kinds of clues, parents can save their child from driving in the wrong direction.

- Parents should trust Children specially in teenage and behave like a friend to them. They must feel free to share their favorite things. In this way children also trusts them

and share their personal things easily.

- They can play games, watch movies with their teenagers in free time so they build a strong bond with them.

- Guide them about the difficulties and consequences they may face while using social media. Suggest them to read different blogs or posts on these issues.

11. Manage the Social Media Privacy

The social media lovers share their personal life details in the form of selfies, photos of attending parties etc. to express their joys and enjoyments to the whole world. **[19]** But these lovers forget to save their personal data from the hacker that loves these types of people. They share their content without hesitation on the social media. Cyber attacker's attacks on the social media account by different websites. The user clicks on that particular website without knowing the impact. Then all data goes to the attackers and hackers, they easily steal personal information, identity and on the basis of this information, hacker blackmails the user. Now the question is how the novice users protect themselves from such hackers. Let discuss some social media apps and their privacy:

11.1 Facebook

Facebook is one of the most common and oldest social media networks that gives the facility of uploading photos, status updates, check in, tag the friend, send messages, calling etc. The users can access the Facebook through mobile phones also. **[20]** It takes the personal information of the user like name, birth, gender etc. and this information is publicly available for everyone. In order to secure the personal data, there are four privacy setting like public, friends, and custom, only me etc. To keep ourselves secure from the hackers the users always select the option of only me in the setting.

11.2 Twitter

Twitter is second most important network on the social media through which people interact with the real world and share their information. Twitter posts are public and in order to make the twitter account private, we have to follow some precaution and steps:

- Only those people access you, who have twitter account.

- Tweets no longer remain on twitter.

- Previous tweet will be hidden after some specific time.

12. Safety for Every Device

Nowadays security is no longer saving only one machine but saving lots of machines that can easily be attacked by the hackers. **[21]** Users share data on daily basis, sometimes the quantity or quality of the information shared attracts the hackers and they tend to hack the particular accounts. Nowadays in the 21st century information has become a new currency. Mostly after downloading, every app asks to access the information on your device and users allow that without any hesitation but they are unaware of the consequences. The information can include a lot of things they don't really want to share. Users should try to avoid posting the speaking photos as it increases the chance of attacks According to the researcher by Marketo **[22]**, Facebook is the top social media network because of the fact that over one billion of users have active account with Facebook and almost 13 million of users never ever touch privacy settings of

the account.28% people reveals their posts, pictures on social media and 11% of people complain that some other person uses their account and share inappropriate or irrelevant material.

Here are some advices to protect the privacy:

- User must say no to auto login whenever they login from other devices because it gives the front door to the hackers to visit the user profile and get useful data from that. So, it's essential for the user to always mention "NO" whenever the system asks "remember me".

- User should understand and make the use of the privacy setting for safety features.

- Before user enters the detail on social media, spend time to check privacy settings. Never announce on social media that where are you going and when will you come back.

- If the user gets some suspicious activity on the account, immediately take an action and report to the expert to sort out the issue and resolve the problem.

13. Advantages of Social Media

- Social media gives the world-wide connectivity and give the users a single platform where people can search their older friends or even jobs through Facebook, Twitter etc.

- Social media also give users the commonality of interest where they get their desired information and desired area of work like painting, cooking, handicrafts, ideas, tips, political information etc.

- It gives the facility to share real time information that is very much beneficial for teachers and students. [23] [24] It also provides information about the celebrities. They share their personal experiences so to become more popular and large number of audiences attract toward that particular information.

- It offers the facility of advertisement. Business owners advertise their products for free. Social media is the best approach to attract variety of users.

- It provides the facility of new cyclic speed through which the people can view the news on the social media sites. And day by day cyclic speed increases.

14. Disadvantages of Social Media

- Backlash is one of the most common things on social media.

- Cyber bulling and crime against the children are one of the most important crimes happening around the world recently.

- Data is not secure and anyone can steal it. Personal data can be misused for the alternative purposes.

- There are also many chances of fraud because most of the websites are not secure.

- It is time waster because according to the research [25] 89% people spend their time on the social media instead of their work.

- Its corporate invasion of privacy and sell the user personal detail to the hackers.

15. Conclusion

Everything has a positive or negative impact it depends on us how we practice it. Things are good if we use them in a positive way. The misuse of the social media is on the top because of the irresponsible behavior of the parents towards their child. The parents play an important role in the society and in the life of their child. The children go towards the wrong track just because they don't get love and attention from their parents. Mostly youngsters involve in the cybercrime activities because of the ignorance from their parents. Parents should be treating their child well. They must be living a life like a friend with them. They should trust them by giving little attention through this they can save the lives of innocent ones.

16. References

[1] Jump up to: [a] [b] [c] Harris, Wil. June 2006. Retrieved

[2] from *"Archived copy"*. Archived *from the original on 2012-09-23. Retrieved 2012-09-15.*

[3] **Jump up^** Tracy Mitrano. (2006, November, December). A Wider World: Youth, Privacy, and Social Networking Technologies. Retrieved

[4] **Jump up^** *Boyd, Danah (2014). It's Complicated: The Social Lives of Networked Teens. Yale University Press. pp. 56, 60.*

[5] ^ Jump up to:[a] [b] *Luo, W., Xie, Q., & Hengartner,*

[6] *U. "FaceCloak: An Architecture for User Privacy on Social Networking Sites". IEEE Xplore. IEEE. Retrieved 2009.* Check date values in: |access-date= (help)

[7] ^ Jump up to:[a] [b] *"How to Stop Facebook from Sharing Your Information With Third Parties"*

[8] **Jump up^** *"Facebook Secretly Sold Your Identity to Advertisers".*

[9] **Jump up^** *"About Twitter's suggestions for who to follow".*

[10] **Jump up^** *"tracking our online trackers".*

[11] 9. **Jump up^** *Ciment, J (2013). "Social Media". Culture Wars in America: An*

[12] *Encyclopedia of Issues, Viewpoints, and Voices – via ONESEARCH.*

[13] ^ Jump up to:[a] [b] *"Social Networking Privacy: How to be Safe, Secure and Social - Privacy Rights Clearinghouse". privacyrights.org.*

[14] Boyd, Danah M.; Nicole B. Ellison; "Social Network Sites: Definition, History, and

[15] Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, p. 210-230, 2008

[16] Dwyer, Catherine; Starr Roxanne Hiltz; Katia Passerini; *Trust and Privacy Concern With Social Networking Sites: A Comparison of Facebook and*

[17] *MySpace*, Proceedings of 13th Americas Conference on Information Systems (AMCIS), USA, August, 2007

[18] http://smallbusiness.chron.com negative effect of social media on society and individuals by Brain Jung

[19] Gifford NV Sexting in the USA, Washington, dc:family online safety institute report; 2009,availbat : www.fosi.org/cms/downloads/resource/sexting.pdf.accessed July 16,2010

[20] http://socialmediabeez.com/author/boey/

[21] http://socialnetworking.loveknow.com/advantages_and_disadvantages_of_social_networking

[22] www.thenationalcampaign.org/SEXTECH/PDF.SEXTech summart.PDF. Accessed July 16,2010

[23] Pew Internet and American Life Project research survey, "Why Americans Use Social Media,"

[24] November

[25] 2011, http://pewresearch.org/pubs/2131/social-media-facebook-twitter-myspace-linkedin

[26] Dinerman, Brad; "Social Networking and Security

[27] Risks,"whitepaper,GFIsoftware,

[28] 2011, www.gfi.com/whitepapers/Social_Network ing_and_Security_Risks. pdf

[29] Common Sense Media. *Is Technology Networking Changing Childhood? A National Poll*. San

[30] Francisco, CA: Common Sense

[31] Media; 2009.Available

[32] at:www.commonsensemedia.org/sites/default/file

[33] s/CSM_teen_social_media_080609_FINAL.pdf.

[34] Accessed July 16, 2010

[35] 21. Lenhart A. *Teens and Sexting*. Washington,

[36] DC: Pew Research Center; 2009. Available

[37] at:http://pewinternet.org/Reports/2009/Teens-and-Sexting.aspx. Accessed August 4, 2010

[38] 22. *Social Media and Young Adults*.

[39] DC: Pew Research Center; 2010. Available

[40] at: http://pewinternet.org/Reports/2010/Social-

[41] Media-and-Young-Adults.aspx. Accessed July

[42] 16, 2010

[43] 23.Berkshire District Attorney. *Sexting*. Pittsfield,

[44] MA: Commonwealth of

[45] Massachusetts; 2010.Available

[46] at: www.mass.gov/?pageID=berterminal&L=3& L0=Home&L1=Crime+Awareness+%26+Preven tion&L2=Parents+%26+Youth&sid=Dber&b=terminalcontent&f=parents_youth_sexting&csid=D ber. Accessed September 7, 2010

[47] 24.Excessive chatting on Facebook can lead to

[48] Depression in teenage girls. *Daily*

[49] *Telegraph*.January31, 2010. Available

[50] at: www.telegraph.co.uk/technology/facebook/44 05741/Excessive-chatting-on-Facebook-can-lead-to-depression-in-teenage-girls.html. Accessed September 7, 2010

[51] Sturm Social networking psych studies: research shows teen Facebook users prone to depression. *TrendHunter*. Available

[52] at: www.trendhunter.com/trends/depression-from-facebook.Accessed September 7, 2010

Editorial Policy and Guidelines for Authors

IJECI is an open access, peer reviewed quarterly Journal published by LGU Society of Computer Sciences. The Journal publishes original research articles and high quality review papers covering all aspects of Computer Science and Technology.

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

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

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

LAHORE GARRISON UNIVERSITY

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

VISION

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

MISSION

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

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

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