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

IJECI

International Journal for Electronic Crime Investigation

VOL.2
Issue: 1 January-March 2018

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

Email ID:
ijeci@lgu.edu.pk

LGU International Journal for Electronic Crime Investigation
Volume 2(1) January-March 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.re-search.lgu.edu.pk

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

LGU International Journal for Electronic Crime Investigation
Volume 2(1) January-March 2018

CONTENTS

Research Article

Research Article

Research Article

Research Article

Research Article

Research Article

LGU International Journal for Electronic Crime Investigation
Volume 2(1) January-March 2018

Ahmad *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 1 January-March 2018

DNA Fingerprints Facial Prints and Other Digital Forensics as Evidence in Criminal Investigation and Court Proceedings

Aftab Ahmad[1], Mujtaba Asad[2], Waqar Azeem[3]

[1]Professor Department of Computer Science, Lahore Garrison University (LGU)
Lahore Pakistan
Email: dr_aftab_malik@yahoo.com
[2]Department of Electronics and Electrical Engineering, Shanghai Jiao Tong University,
Shanghai Minhang Campus, China;
Email: mujtaba.asad@live.com
[3]Department of Computer Science, Lahore Garrison University LGU; Lahore Pakistan
Email: waqar.azeem@lgu.edu.pk

Abstract:

The purpose of this paper is to focus on the legitimacy and importance of digital evidence such as fingerprints, DNA, polygraph, auto-radiography, and facial-prints and their admissibility in investigations and court proceedings. The extracts from criminal databases are also relevant in this context. The modus operandi of criminals, particularly in case of repetition of similar type of offence is also of immense significance. Normally, the criminals operate adopting a specific manner or method. The killers have their own way or mode of committing the offence. The modus operandi changes from person to person or groups to groups in committing the offences. It may determine that the offence is committed by a group or an individual. In view of its impotence, the modus operandi must be included in criminal databases as a separate column. The criminal images sketched by artists on the bases of description of witnesses present on scene of offence have relevance and must be included in the criminal databases for future reference and use.

Keywords: Evidence, DNA, Facial images, fingerprint, modus operandi, criminal history Database.

1. Introduction:

In criminal investigation and court proceedings the role of Information Systems is very important particularly regarding the physical appearance such as fingerprints, face-prints, DNA code, polygraph and Iris Code are of relevance. In order to facilitate further discussion, following explanation is required.

According to [1], Digital Forensic is science useful for using the data and information from digital devices such as mobile phones and computers. The area of knowledge is vastly being used. The major aim of forensics is to process and utilize the information collected from scene of offence in the investigation and later on in court proceedings.

Further, [1] developed a new technique to codify the fingerprint into a unique digital code for using as primary key to search the criminal database. This made the search system faster. The first author of this paper worked with Police Department for ten years and prepared feasibility study for implementation of Computerized Management Control and Information

System leading towards a strong Decision Support System. The major areas of study are given below:

- Technical, operational and Financial Feasibility Study
- Automation of Criminal history based on Fingerprint System
- Automation of Criminal History based on Physical appearance of the criminals

In [2] a new procedure has been developed to codify the person's names from Alpha Characters to digital characters (i.e. numeric characters) for efficient retrieval The present authors have successfully designed an adaptive Algorithm for codification of facial images in digital codes. All the techniques of [1],[2] and [3] are effective applications in the area of digital forensic, storage and retrieval of criminal information. Moreover, [4] presents software for Finger Prints Storage and Retrieval of Criminal Identification and [5] develops Software for Storage and Retrieval of Criminal Information for Police. [1] Appreciates the application of Biometrics Technology in forensic to analyze and examine DNA, facial images and other parameters associated with criminal information system.

There are several application of biometrics discussed in [1] related to forensics such as terrorist identification and missing children. In [14] it is emphasized that other investigation methods are becoming obsolete in view f the digital forensics, where in a detailed discussion is available on the use of digital forensics. In [15] the digital forensic has been termed as a rapid metamorphoses and a matter of educational study having great research potentials to construct new models for applications in various walks of life. The major focus of [16] is about virtualization and importance of digital forensics to develop communities of researchers. The paper [16] also throws light upon digital Forensics.

2. Composite images

The Facial Composite images of criminals prepared by artists are relevant in investigation and court proceedings. The images [18] and [19] sketched by the artists are based on the description by the eyewitnesses. They are used by Police Department to identify and locate the criminals particularly those involved in major crimes. The following composite images (a), (b), (c) and (d) have been discussed in [18],[19] and [20]:

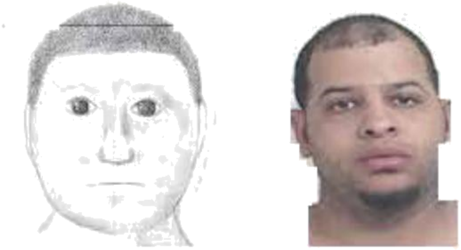


Image (a)

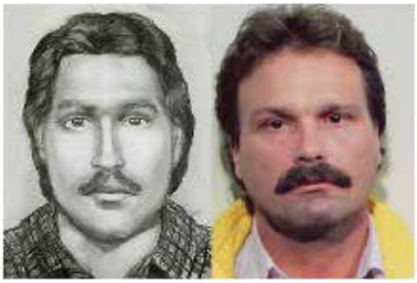


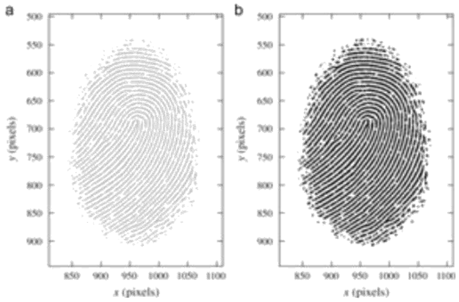
Image (b)

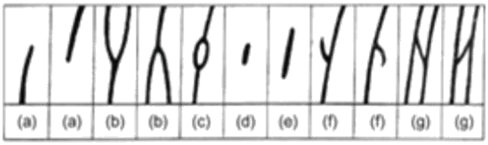
Image (c)

Image (d)

3. The uniqueness of Finger print images play pivotal role in criminal investigation

During the development of human fetus, before assignment of fingerprints impressions on hands and feet, an automatic natural process works which compares the impressions with all record of “natural databases” of all dead persons, all the alive persons and also to be born in future. This is how uniqueness of fingerprints is achieved because nature does not repeat itself. Similarly, Iris possesses the property of uniqueness and used in databases to search the records. The technique [22] of matching fingerprints images has been discussed in depth and the fingerprints sensing is a presented in [23]. A very useful discussions and methodology is given in [24] regarding science of fingerprints. The following images of fingerprints have been discussed in detail in [1] and [4]:





According to [1] and [4] the structure of fingerprints is unique and they contain dots spirals, dashes, ridges, whorls, parabolas, arches and tented arches. All fingers have unique code. Therefore according to [1] fingerprint codes can be used as primary key in Databases to retrieve.

4. Legal Position of Forensic Evidence

The Punjab Forensic Science Agency Act, 2007 provides the procedure for conducting the Forensic Tests and to examine the forensic material to enable the experts to submit their reports in courts, tribunals and investigators [17].

5. Importance of Deoxyribonucleic Acid Test (DNA)

According to [6], Deoxyribonucleic acid is the chemical dispatcher for genetic information. The DNA is unique and identical for every person like finger prints. However, the twin babies have the same DNA configuration. There are several kinds of DNA Test such as maternity test, paternity test, DNA Paternity/ maternity test and DNA grandparent test. The Sibling test tells the information about half sibling or no sibling relation. Figures 1, 2 ,3and 4 show the DNA structures.

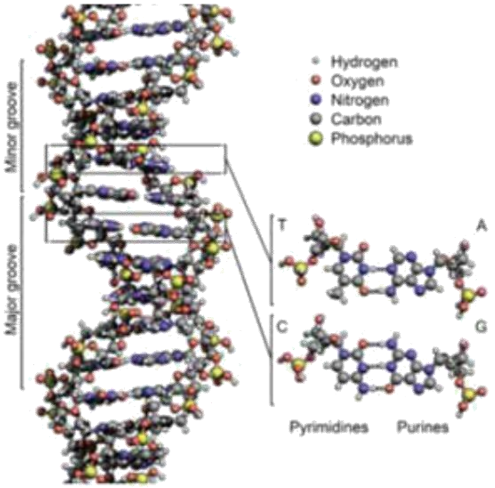


Figure 1: DNA Structure

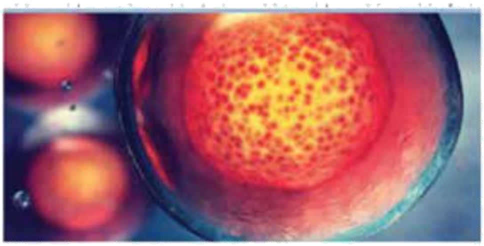


Figure 2: DNA Shape

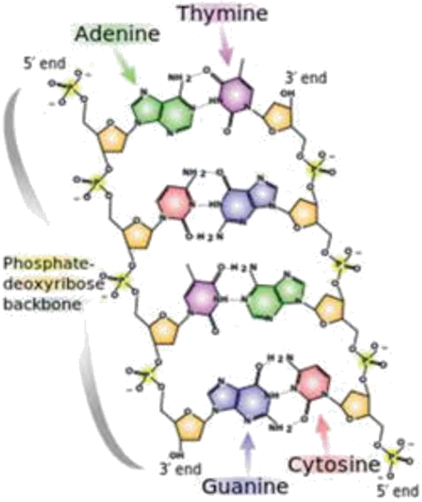


Figure 3: Molecular Structure of DNA from [6]

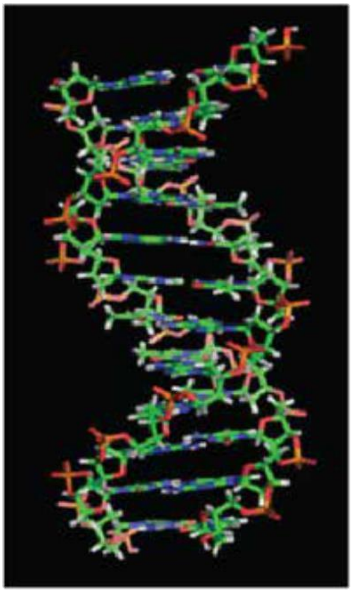


Figure 4: Stairlike Structure

The DNA is used in development, growth, functioning and reproduction of all living beings. In the present age of advancement in forensic science, the investigators prosecutors and courts are giving weight to the relevance of DNA test in USA, UK and now in Pakistan.

According to [7], the profiling of DNA is prepared using Microbiology techniques from blood samples, swab, semen or other materials possessing DNA. The basic Technique discussed in [6] is RFLP abbreviated as Restriction Fragment Length Polymorphism for analysis has been developed by Edwin Southern. It detects that DNA for a particular gene and can be separated from the provided sample.

The use of X-ray for Autoradiography [6] in Polymorphic DNA Test method is based on photography to observe the DNA segments by means of radioactive probes exposed to the photographic plate.

5.1 Acceptance of DNA test as Evidence

In United States the courts allow the councils and attorneys to present the DNA test as evidence. The famous Frye Rule [6] advocates for acceptance of DNA test carried out on scientific basis by experts. This rule is very popular. According to [7] and [8] the opinion by experts is relevant and accepted in courts. The document of DNA [8] carries the approval of House of Commons for the implementation of expert opinion in England and Wales. The evidence of the expert, who has conducted the DNA Test, is required to submit the source of sample. The judges normally make sure this requirement. According to [9] the secondary evidence is admissible in courts.

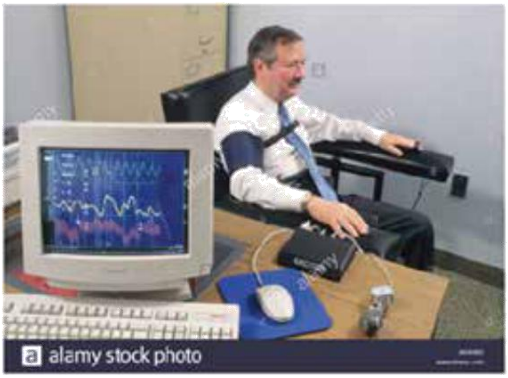
5.2 Evidence

According to [10] the evidence is any fact that contains probative force i.e. it is of that quality which can be presented to court as evidence of some other fact in issue. The purpose of evidence is to exhibit clarity. According to the provisions of Qanun-e-Shahadat Act promulgated in Pakistan in 1984, there are several types of evidence such as Direct, Secondary, Primary or original documentary (public or private), oral or Circumstantial evidence. The DNA is nowadays admissible in courts in Pakistan as evidence.

6. Admissibility of Polygraph Test

This section focuses on the admissibility of Polygraph in investigation or court proceeding as evidence. The equipment used in this technique is also known as “lie detector”. It measures and computes the changes occurring in physical indicators such B.P, pulse rate, heartbeat, skin conductivity and respiration during question answer session. In USA, Philippine, England, and Wales, the private detectives use this computerized method frequently.

According to [11] 1nd [12], the polygraph test may not be reliable if conducted by unskillful and inexperienced person. Nowadays, some business firms are also using this computerized device to explore wrong full acts at duty place. The FBI also uses the equipment in connection with case related to civil and criminal nature for investigation purposes. The polygraph is successfully used for testing the veracity of any two person making different statements in an issue, In legal language, it is termed as pair-testing. In 1989, the US court of appeal, in the case of US vs Picionnona decided that Polygraph test has advanced to that level to accept it in courts as evidence.



The inferences from polygraph are deduced from the graphical display and variation occurring during investigation. Figure No 5 shows a screen shot.

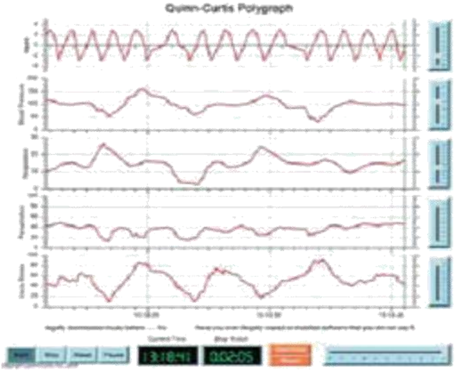


Figure 5 with courtesy of Quin Curtis

[13] Describes the working of the computerized polygraph. The figures 6 and 7 are illustrative and self explanatory.

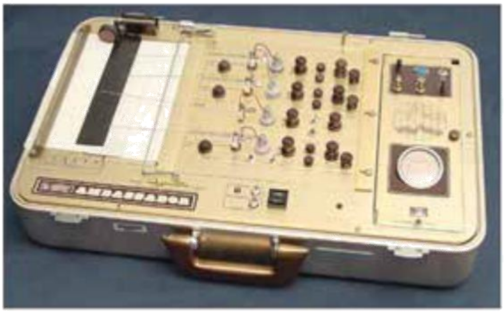


Figure 6: Polygraph test machine

Figure 7: Working with Polygraph equipment

7. Modus Operandi

Modus operandi is particular manner of performing any task or doing something, for example every criminal adopts a specific manner to commit a crime. The killers have their different own ways and steps to commit murder. While using criminal information Systems, it proposed that a separate column must be reserved for indicating the modus operandi because it is very relevant in case of criminal investigation and court proceedings. The plan of action carried out in following a particular technique is also modus operandi the way in which work is operated. The modus operandi is relate to brain function.

8. Case study

The purpose of presenting this case study is most relevant to the thesis of this paper. In this case, the DNA matching test, Polygraph and modus operandi played extremely important role for the investigators, prosecutors and the court to reach to correct decision. It is murder case of 6 year old girl. There have been multiple offences committed by the serial killer such as abduction, unnatural sexual activity, rape, killing and mutilation of human body during killing and after death.

In this case modus operandi led the investigator to make the criminal confess about six other killings in the same manner. The matching DNA test of the deceased girl and the criminal resulted in reaching to conclusion. The Supreme Court of Pakistan played excellent supervisory role while anti terrorist court imposed the death penalty on four counts. The case was contested under the Anti Terrorist Act and under provisions of PPC sections 201, 364-A, 376,377,302 as well as section 7(A) of ATA 1997 for causing fear and terror in the area. The Police collected DNA samples of 1187 suspects for matching but only it matched with one person, the real culprit. After the confession of the criminal in this case, the prosecutor submitted list of 56 witnesses out of which only 22 were crossed examined. This case has included Pakistan in the list of countries that have used scientific technology and forensics to prosecute and sentence a criminal.

9. Conclusion:

The extensive use of digital forensics, fingerprints, DNA test, Polygraph, auto-radiography, facial-prints, Composite images and their admissibility play pivotal role in investigations and court proceedings. These factors formulate essential basis of evidence.

10. Acknowledgement:

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

11. Reference

1. Aftab Ahmad Malik, Asad Mujtaba & Waqar Azeem; “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

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

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

[4] 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;

[5] 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

[6] George Bundy Smith Janet A. Gordon, "The admission of DNA evidence in state and federal courts; Fordham Law Review, Volume 65 | Issue 6 Article 4, 1997; Available at: ttp://ir.lawnet.fordham.edu/flr/vol65/iss6/4

[7] David H. Kaye, DNA Evidence: Probability, Population Genetics, and the Courts, 7 Harv. J.L. & Tech, 101, 107-08 (1993).

[8] Kenneth Clarke QC, MP, Lord Chancellor and Secretary of State for Justice, "Expert Evidence in Criminal Proceeding in England and Wales"; Law Commission No 325, Ordered by The House of Commons to be printed 21 March 2011

[9] Zafar Kalanauri, "Law of Evidence in Pakistan", Published on September 14, 2016

[10] Salmon John William, "Jurisprudence" ; Publisher London Stevens and Haynes 1913 https://archive.org/details/jurisprudence00salm

[11] Polygraph Test Results - Kidzone www.kidzone.ws/science/polygraph/testresults.htm

[12] The Truth about Lie Detectors; American Psychological Society

http://www.apa.org/research/action/polygraph.aspx

[13]. Kevin Bonsor, "How Lie Detectors Work ; https://people.howstuffworks.com/lie-detector.htm

[14] Simpson L Garfinke, "Digital forensics research: The next 10 years"; Digital Investigation, Elsevier, Volume 7, Supplement, August 2010, Pages S64-S73

[15] Mark M. Pollitt, "An Ad Hoc Review Of Digital Forensic Models"; Published in: Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on 10-12 April 2007 IEEE Xplore: 16 April 2007 ISBN: 0-7695-2808-2.

[16]. K Nance, B. Hay and M Bishop, "Digital Forensics: Defining a Research Agenda", Published in: System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference 5-8 Jan. 2009 held at Big Island, HI, USA; published in IEEE Xplore, INSPEC Accession Number: 10467069; DOI: 10.1109/HICSS.2009.160; http://ieeexplore.ieee.org/abstract/document/4755787/

[17]. The Punjab Forensic Science Agency Act, 2007

[18]. The composite images; https://www.google.com.pk/search?q=police%20sk

[19] The Composite images; https://www.artspace.com/magazine/news_events/conversation-piece/5-reasons-to-collect-mel-bochners-framed-amazing-art-print

[20] The Composite images; http:// inderecami.com/police-sketch-artist/

[21] Warda Imran , Hasnaat Malik , “Legal experts say DNA is admissible evidence“, The Express Tribune Pakistan Published: January 25, 2018.

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

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

[24] John Edgar Hoover, “The Science of Fingerprints”, Federal Bureau of Investigation”, John Edgar Hoover.html http://www.scientificlib.com/en/Technology/ Literature/FBI/TheScienceOf Fingerprints .html

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

LGU International Journal for
Electronic Crime Investigation

Research Article
Vol. 2 issue 1 January-March 2018

Use of Cyber Space by Terrorist Organizations

Kaukab Jamal Zuberi
Digital Forensic Research and Service Centre
Lahore Garrison University

Abstract:

Prevention of Electronic Crime Act 2016 of Pakistan, defines and include cyber terrorism as a cyber-crime. Due to its anonymity cyber space is a popular tool used by terrorists. Terrorists use cyber space to launch their propaganda, recruit new workforce, radicalize target groups, raise financing, train the new recruits or upgrade the skills of existing workforce, raise funding for their operations, establish communication infrastructure to communicate within and outside the organization and execute their operations. This article discusses the various ways cyber space is used by the terrorist organizations to execute their plans.

Keyword: Terrorism, Cyber terrorism, Propaganda, Terrorist financing, Terrorist recruitment, Terrorist training, Radicalization, Direct Soliciting

1. Introduction

Prevention of Electronic Crime Act 2016 (PECA) was passed on August 11, 2016 in Pakistan. In this act, 25 new offences and their punishments were introduced. Section 10 of PECA deals with cyber terrorism. According to PECA whoever commits or threaten to commit any of the following offence:

a) Coerce, intimidate, create a sense of fear, panic or insecurity in the government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society.

b) advance interfaith, sectarian or ethnic hatred

c) advance the objectives of organizations or individuals or groups proscribed under the law

Section 10(a) mentions that it is punishable offence to prepare or disseminate information through any information system or device that advances inter-faith, sectarian or racial hatred.

Section 10(b) mentions that recruitment, funding and planning of terrorism, preparing or disseminating information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism, is a punishable offence. Punishments under Section 10, 10a and 10b are mentioned in the Act.[1]

PECA has established cyber terrorism as a criminal offence in Pakistan punishable by law.

Terrorists cannot live on idealism alone. They have to propagate their ideology, gain support, hire recruits, raise funding in order to carry out their plans effectively. Internet is one of the easiest and effective way of propagating, hiring, fund raising and often to carry out the plans. In this article, we shall discuss the means and ways to hire new recruits through internet.

2. Propaganda

Merriam-Webster defines propaganda as “ideas, facts, or allegations spread deliberately to further one's cause or to damage an opposing cause;” [2]

Terrorist organizations use emails, messaging applications, presentations, multimedia files, cartoons, animations and video games developed by themselves or their supporters too propagate their cause. Such tools are then distributed through internet using dedicated websites, chat rooms, secret forums, online magazines, social networking websites, and popular file-sharing websites. Recent video based social media apps are also a popular tool for such propaganda as private video chat rooms can be created on several of these websites. The use of indexing services such as Internet search engines also makes it easier to identify and retrieve terrorism-related content.

Dark web is a popular medium of propagating and distribution of the of these organizations.

There are multiple objectives and large range of audience for the propaganda done by terrorist organizations. The propaganda is targeted at potential or existing supporters. It is focused on recruitment, radicalization and incitement of terrorism through messages which glorify the accomplishment, dedication and achievements of extremist goals.

2.1 Recruitment

Terrorist organizations use password protected websites and internet chat groups for clandestine recruitment. Effective propaganda tools are used to lure marginalized and vulnerable groups in the society. The process of recruitment capitalizes on the sentiments of the targeted groups. It focuses on the sentiments of injustice, exclusion or humiliation. Internet can be used as an effective medium to hire not only young professionals, students and minors which comprise the high ratio of internet users. They lure them through cartoon, internet games and children stories with messages promoting and glorifying the acts of terror, such as suicide attacks

2.2 Incitement

Material prepared to incite an act of terrorism is different from the material prepared to propagate a cause. For example, the dissemination of material on instructive material on the use of explosive would not be considered a breach of law unless the material incites the readers to commit a terrorist act or the material could be used for a terrorism purposes.

Communication through internet can

be very manipulative and dangerous if it is used by trained recruiters of terrorist organizations. They successfully influence the young minds by using latest communication techniques. They use chat room, video chats, private video chats, and other social media websites to incite young victims.

2.3 Radicalization

Radicalization refers primarily to the process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies. Radicalization does not belong to one group or one religion. There are some common root causes for radicalization. They are communal reasons and personal reasons. However, we cannot generalize them. Communal reasons are mentioned as follows:

1. Large minority population which is politically, socially and economically marginalized.
2. Certain communities to be treated as “suspect groups”. Treatment is invasive and overbearing counter terrorism efforts.
3. Cultural or Political hostility against a religion.
4. Unpopular foreign policies, such as support for repressive regimes or involvement in a military campaign.
5. The presence of preexisting recruitment networks

The examples of personal reasons are as follows:

1. Personal ties with radicalized person.
2. A desire for adventure, rebellion, and life experience.
3. Need to belong to a group
4. Feelings of compassion and concern for the suffering of others with whom one feels some kind of personal connection, such as one's co-religionists.
5. Presence of teen angst.

Internet, Prisons and ties with radicalized friends remain some of the most common causes of radicalization. In the end, external factors are more influential in the process of radicalization.

Recruitment, Incitement and radicalization can be viewed as point along with a continuum to terrorism. [3]

3. Financing the Terrorist Operations

A terrorist organization requires resources to survive and conduct its operations. Detailed budget or requirements are seldom listed in terrorist operations and they vary from one operation to another, we can generalize the minimum categories of minimum requirements for such operations. These resources can be divided into three categories:

a) Money and other negotiable instruments.

b) Tangible resources – those goods that have monetary value.

c) Intangible resources – those resources which do not have monetary value. Some of intangible resources are traded for money. For example, a terrorist organization training another organization for money.

The resources also vary as some organizations take care of families of those who die in their operations and other provide handsome salaries and benefits to their recruits. Therefore, the resources vary from organization to organization and operation to operation. A terrorist organization needs financial resources for the following:

- Recruiting new members
- Establishing and maintaining training camps and bases
- Maintain the housing requirements and day to day needs.
- Buy equipment, explosives, conventional and unconventional weapons
- Buy or create forged identity and travel documents.
- Acquire technologies for intelligence gathering.
- Create a communication network
- Bribe government officials and other sources as and when required.
- Day-to-day maintenance expenses for members awaiting commands to launch Operations [4]

Terrorists use various means to raise funding for their operations. Cyber space due to its anonymity and large access is a popular medium to collect funds. Some of the methods used to raise funding include:

- Direct Soliciting
- E-Commerce websites
- Exploitation of online payment tools
- Charitable Organizations

3.1 Direct Soliciting

Direct Solicitation include contacting the potential financers through use of websites, mass mailing, chat rooms and targeted communications [5]

3.2 E-Commerce Websites

E-Commerce websites may sell books, videos, training material or other items to collect money through credit cards and other online payment services like paypal etc. The introduction of crypto currencies has enabled the terrorists to conceal their identity and accept payments from anonymous resources.

Terrorist may also use dark web to sell illegitimate goods and services and raise funds through such websites.[6]

3.3 Exploitation of online payment tools

Terrorists use various hacking techniques to steal identity information (social security numbers, etc.), credit card numbers, wire fraud, auction fraud, hacking mining machines and crypto currency exchanges and online payment facilities like PayPal.[7]

3.4 Charitable organizations

Terrorist create fake charitable organizations and raise money on those organizations. These web based organizations are seemingly legitimate. Some terrorist group create shell companies to raise charities for philanthropic purposes. These companies use names to emotionally exploit the sentiments of the donors. Most of the donors are unaware of the motives behind collection of these funds and they donate their charities in good faith. Social media is also used as a fund raising tools by terrorist organizations. Terrorist receive payments from supports and unsuspecting donors, who believe that they are donating for a humanitarian cause. [8]

4. Training

Due to the ease of access, internet has become a popular medium to distribute training material. This training material vary from videos uploaded on YouTube to pdf documents on compromised websites.

Internet has become a virtual training ground for these organizations. Such websites and social media is used to spread training materials and training videos. Websites suddenly emerge and disappear after serving the purpose. Insufficient information security structures have made websites vulnerable and once these websites are compromised anonymous web pages can be uploaded known to a specific group of individuals.

Ease of access, lack or insufficiently qualified monitoring force, lack of qualified cyber security personnel at public or private organizations have contributed towards the misuse of cyber space for training purpose.

Instructional material on such websites includes tools for counter intelligence and hacking. Terrorists are trained with these technologies to facilitate their anonymity and online communication. [9]

5. Planning

Various internet technologies are used in communicating within and between organizations. The communication is extremely sensitive at this stage and carry the promotion of extreme violence. Plans are discussed within the organization, with other organizations present in the country and across the border. Instructions are shared with maps, directions, photographs, technical details like how to use explosives and other tools to execute a plan. Often these instructions are hidden in graphic or multimedia files using steganography tools. Modern steganography tools are easily available on web. These tools are not expensive and can successfully hide information in graphic and multimedia files which is very difficult to detect. Sometimes, the communication is done through public networks, internet cafes and other social media services and is encoded. Whereas, sometimes the communications is done through proprietary communication tools developed by the organizations.[10]

6. Execution

Execution is the actual attack to disrupt critical infrastructure of a country or a critically important organization and spread terror among the citizen of the country. The attack may be a physical attack or a cyber-attack. In both cases, internet is used to communicate securely to make the attack successful. A cyber-attack is the exploitation of computer network and manipulation of data to disrupt the operations. These attacks are made through hacking, advanced persistent threats, viruses, malwares or other malicious means of access to the network.Terrorists organizations may decide not to disrupt the network once it is compromised. They may decide to steal the sensitive data and use it to their advantage. There is a secondary market on dark web which is always ready to buy such data. Moreover, the terrorist organization may decide to use the stolen data for their own advantage. Such data includes diagrams, drawings, phone numbers and family details of senior military officers etc. [11]

7. Conclusion

Terrorists use internet to recruit, train, plan and execute their operations. Internet is also used in raising finance to fund their operations. In this process they keep their anonymity and utilize secure communications tools available on the social media and in cyber space.

There is a need to develop sophisticated tools to prevent, detect and deter cyber-attacks. Surveillance teams with multi-linguistic knowledge should be created and they should monitor the chat rooms and other social media websites. Cooperation should be developed with similar agencies in different countries.

Pakistan being in the middle of terrorist activity have suffered in last few decades of war in Afghanistan. More than 80,000 Pakistanis have been killed in the war of terror since 2003. Incidents of Cyber terrorism are not reported openly in Pakistan. We need to create teams with private sector contribution to develop preventive mechanism against cyber-attacks.

8. Reference

[1] NATlONAL ASSEMBLY SECRETARIAT. (2016). “Prevention of Electronic Crime Act” May 2016. Islamabad. Available at: http://www.na.gov.pk/uploads/documents/1472635250_246.pdf.

[2] Merriam-Webster https://www.merriam-webster.com/dictionary/propaganda.

[3] Simon Shercliff Sue Hemming OBE The Use of The Internet For Terrorist Purposes page no 6 (2012) United Nations, UNODC.

[4] Jodi Vittori. “Terrorist Financing and Resourcing” page 19-23, Palgrave Macmillan 2011.

[5] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7 (2012) United Nations, UNODC.

[6] Babak Akhgar Andrew Staniforth Francesca Bosco- Cyber crime and cyber terrorism investigator's handbook-Syngress, , Elsevier Inc. Page 153 (2014).

[7] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7 (2012) United Nations, UNODC.

[8] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7 (2012) United Nations, UNODC.

[9] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 8 (2012) United Nations, UNODC.

[10] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 8-11 (2012) United Nations, UNODC.

[11] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7-10 (2012) United Nations, UNODC.

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 1 January-March 2018

A Survey on Attacks and Detection Mechanisms in VANET

Irshad Ahmed Sumra[1], P.Sellappan[2], Azween Abdullah[3]

Department of Information Technology Malaysia University of Science and Technology (MUST), Malaysia. isomro28@gmail.com

Abstract:

Vehicular ad hoc network (VANET) has grown to be foremost up and coming talented and rapidly uprising network or matrix in modern vehicles and this matrix is termed as mobile ad hoc network (MANET). This matrix consists of important and intelligent nodes (vehicles) and certain computing devices named as road side unit (RSU) which are responsible for the communication of vehicles with other vehicles and with RSU as well. Vehicles can communicate with other vehicles on the roads to avoid road accidents and traffic jams on busy roads to save valuable time. This communication is done with the help of unauthentic means of wireless medium which makes the communication possible through air using certain waves like radio waves of high frequency. Because of its immense essence, these matrices are vulnerable to assaults which might cause life threatening circumstances and innocent lives may be lost. If there is any fault in the matrix it can cause serious damage to lives of innocent people so to avoid such significant and serious instances, it is important and necessary that there must be some tools and methods regarding to safety which can observe and find out attacks or assaults like this in the matrix. The purpose of this study is to discuss assaults on VANET and to describe methods to find out the presence of such assaults and to suggest the ways to secure vehicular matrix. Certain and common types of assaults are categorized and discussed and the consequences of such assaults are also explained. This paper also discusses the possible expositions and pros and cons of these expositions.

Keywords: intrudes and intruders, presence of attacks or assaults and attackers, roadside unit, safety, safety measurements, wireless medium, radio waves.

Introduction

Vehicle Ad Hoc Network which is termed as VANET is a certain kind of mobile ad hoc matrix that is responsible for the communication between nodes or vehicles and certain computing devices named as roadside units. Ad hoc networks are spontaneous self-organization of matrix nodes. It must not be necessarily connected to the internet and is usually formed by hybrid wireless matrix and mesh matrix. Every node that is present in the matrix must be installed with onboard circuits (OBC), which helps to accumulate and transmit the nodes' wireless communications, small sensors, embedded systems, and Global Positioning System (GPS). The nodes can then communicate and transmit messages not only to other nodes on the matrix but also to roadside units (RSU), as in traffic signals, which assists in improving the driving experience and ensures the safety of the driver.

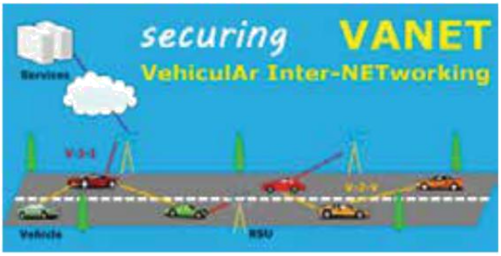


Fig.1 Architecture of VANET

VANET has been becoming one of the uprising technologies in daily routine situations like it is used to find out the traffic jam on a certain road, proper scanning of traffic and administration of traffic. For example if on some busy road there happened to occur an accident, a vehicle (node) that is connected to VANET matrix can send a message to all the other vehicles (nodes) that are connected to same VANET matrix about the accident and deliver them a message to choose an alternate way to travel. Similarly, if traffic is jammed somewhere, a node can deliver a message to other nodes about the traffic jam and intimate them to choose an alternate route. These are the basic routine usage of VANET which may address safety issues but VANET is not limited to this basic routine usage, there are some other applications vitally important that VANET addresses, for example, nodes in this matrix broadcast and share information at all the times, define the facility and utility about the payments, calculates the payments according the two usage and many other things like this. So these applications demand the nodes to communicate and share the information with other nodes, with users of the matrix and with the structure of matrix and the Internet, which results the VANET to be grown and this makes VANET an Internet of Vehicles (IoV). The Internet of Vehicles (IoV) is a collection of multiple matrices which includes inter vehicle matrix (in which nodes communicate with each other V2V), an intra-vehicle matrix (like automotive functions inside the node), and vehicular mobile Internet.

VANET has some distinguished aspects like ability of nodes to be moved freely and easily, its capability of forming new and frequent ad-hoc matrices and topologies that support this feature, of its being capable of judging the moving nodes. For these abilities to be fulfilled there must be distinguished algorithms that can fully and reliably work in such environments for the fulfilment of VANET aspects described above. Safety is a major and most vital concern when dealing with nodes in VANET. The three major components nodes, people and RSU must work together in predicted routine in order to provide a healthy environment. If they are not working in predicted manner then it means safety is breached by an attacker. Safety also means that private data of the user must be confidential. So if safety is compromised it can cause to life threatening risks. But so far, progress on the technology on the issue of safety is has been made but very little.

The first study on the subject of safety was done by by Isaac et al. He proposed certain methods in case of assaults in VANET, but major issues were not solved. In the ending of decade 2000’s, methods were started to be proposed regarding safety. In some of searches during these periods, assaults on safety in VANET were discussed in detail and idea of some systems to find out the presence of intrudes and intruders was proposed. Also presented was the idea to build systems to lower the risk of assaults.

1. Safety Applications in VANET

Mobile ad hoc network MANET has proposed contemporary and advanced safety measurements which if taken risk of compromise on security and safety can be lowered. Problems in VANET can be the deficiency of main spots, for a node to be moved freely and easily, frequent and consecutive correspondence of wireless connection, to be able to work with mutual cooperation, deficiency of a vivid boundary of protection. The major and specialized aspects of VANET are the ones which make above mentioned problems more difficult to resolve. Details of the problems are discussed here:

1.1 Privacy

Vehicular ad hoc network (VANET) has motivated fascination in academic as well as in industry environment. Once these matrices have been deployed in vehicular nodes they might yield a fresh and new driving experience for drivers. But whenever communication happens in an open environment like VANET it challenges the security and privacy. Both privacy and security compromises and it affects the matrix of vehicles.

If the security has to be provided to the VANET user then privacy would have to be sacrificed. Because the matrix controller authorities may have to have information from the drivers of the vehicular nodes during any event but users demands to hide their personal data like their identification, location access and other sensitive data. So to resolve this conflict i.e.; to stop the vehicular nodes from being tracked by unauthorized jurisdictions and for legal jurisdictions to find out the actual identification of VANET user, there must present a suitable system.

1.2 Scalability

Scalability means the addition of more and more nodes into the VANET matrix without the need of changing previous existing components of the matrix. This matrix of vehicular nodes must be scalable in order to meet its modern criteria. Detailed interfaces of scalable components should be provided by manufacturers. Currently, amount of automobiles is roughly about 1.5 billion, may be more than that. And for those nodes which are connected to VANET is about to exceed 1.5 million and is increasing day by day. Till present, none of the international jurisdiction is delivering the safety measurements and methods to matrices like this, for it is a daring and difficult job to provide a systematize mandate for matrix of vehicular nodes. To provide a suitable and feasible solution for this, native jurisdictions must sit together to define systematize rules regarding safety in network.

1.3 Mobility

The nature of matrix of cars as nodes is such that one node interacts with another node a few times, sometimes only one time so topology of the matrix varies frequently. Nodes are usually noticeable if they move with velocity between 18 to 22 meter per seconds but in reality nodes move with velocity greater than the noticeable velocity in mobile matrix of nodes. So there is a frequent disconnection in association of nodes in the matrix. And this disconnection in the association of nodes is even higher if the nodes are moving in antiparallel orientation, here connection keeps itself only for a fraction of time. Nodes usually are connected for a small interval of time and after that probably they never communicate with one another. This issue creates problems for the VANET system. But the nature of topology of VANET is more foreseeable when it is compared against the nature of MANET.

1.4 Hard-delay constraints

Most of the implementations in VANET must be quick respond generating implementations, they must respond to any situation in a real time. If they do not response back in any case of tragedy or accidental events or in emergency situations, then results can be drastically awful. In addition such implementations must be assault proof. All most all the authors suggest that safety implementations must especially emphasis on intercepting the assaults. To stop the assault is better than to find the assault. But the identification of assault is also important in implementations in certain situations like when any employee who knows the security procedure details of matrix tries to assault the matrix.

1.5 Acquiescence

Most of the algorithms and set of rules and regulations of VANET suppose that nodes will distribute and propagate the information to other nodes. And if it happens creates again a challenge for the safety and security for the matrix and matrices become easier for assaults as in wrong information can be sent from one node to another resulting threats and damages for nodes in the matrices. So most of the safety methods depend upon the acquiescence of nodes because more sensitive data is needed in order to stop and find the presence of assaults.

Second safety issue that is present more in MANET but less in VANET is a lucid boundary of protection. Unlike other security systems, security systems in matrices of vehicular nodes are not consisted of some fix points like it happens in guided matrices, but roadside unit is responsible for the safety in VANET like collecting node data and suggesting resolutions to the problematic events. The safety methods in VANET are more efficient than the safety methods of MANET because of some components provided by RSU and this has been already proposed in many literature reviews.

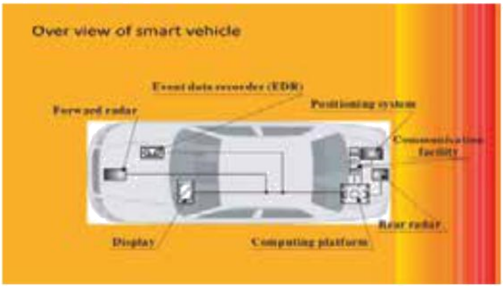


Fig.2 Smart vehicle of VANET

Since the very beginning of the history of VANET and MANET, many different solutions methods and tools have been suggested. Many of these methods were acceptable and adjustable for MANET but largely they seems not fit for VANET because this matrix is highly dynamic in nature contrary to previous matrix. So authors have been trying to propose methods with variations in previous models. Also included the research to protect the matrix from intruders in order to maximize the safety measurements. Previously made safety methods were limited in its working and in the diagnosis of intruders, limited to certain types of intruders, but modification in those methods can result in identification of every kind of intruders like inside intruders who is more dangerous than the outsider intruder. The Internet of Things (IoT) is getting popular day by day. Internet of things is the interconnection of many computing gadgets and matrices enabling them to send and receive and share data even though the types of matrices are different for different electronic devices. These interconnected systems can be embedded systems as well. This can be helpful in many fields such as in home systems, electronic health care systems, embedded sensor networks, doctor patient interaction, alarm systems, automatic lighting, transport systems, ecommerce and many more. And numbers of devices that are interconnected are increasing day by day and in nearest future this number of devices will reach above 25 billion in number. But most of the devices are automobiles and vehicular nodes forming internet of vehicles. Internet of things includes many applications like recognition; transmit messages to other nodes, and setting the rules and regulations for the transmission of messages from node to node. But most devices and applications lack safety methods and procedures. So, some types of assaults are presented in this paper in the following:

1.6 Inter-vehicle-attacks

Inter node communication means the communication between one node and the other node. Nodes have to share information, transmit messages and communicate with each other at all the times. For instance if a node comes across some busy read where the traffic is jam then this node has to transmit a alarming message to all the other nodes particularly in that area. Similarly, if some road accident has occurred at some place then a node which is present there must communicate this message to other nodes in the surrounding region about the accident. Other messages for transmission could be about the slowing down the velocity of the node, change the lane of the road, to stop on the traffic signal, giving alerts about the bad condition of roads etc. so nodes have to communicate with each other if they are connected to the matrix of nodes.

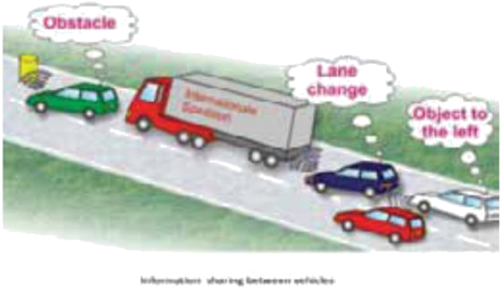


Fig.3 Vehicle to vehicle (V2V) Communication

But intruders can take the advantage of this protective communication. For example, if the intruder is present in node C which is at the last of node A and node B, it can generate false message to node A to slow down while at the same time to node B to fasten its velocity causing an accident between node A and node B. so there must present some more strong methods regarding safety of the matrix against intruders and for the safety of human life.

2. Intra-vehicle attacks: Intra-vehicle communication means the communication of the node within the node. One component of the node transmits the messages to other components of the same node. Advanced vehicular nodes have built in embedded sensors in order to examine the road state, distance between nodes, the presence of any barrier or hurdle, awareness of the fire, to accelerate or retard the velocity of the node,

the interface to exhibits the messages, and an On-Board Unit (OBU) that comprises of node-to-node and road-to-node transmission organization. Assaults within a node like dogging an internal sensor may be dangerous for the node and the surroundings as well. For instance, an assault in the inside system of the node like automatic handling of the node which includes automatic control of steering and horns, automatic speed of the node, information about the fuel etc. can be very harmful for the node and surroundings. In addition, if the node is connected to the internet they there are more chances for a vehicle to be assaulted by an intruder. But these kinds of assaults are not a part of our study.

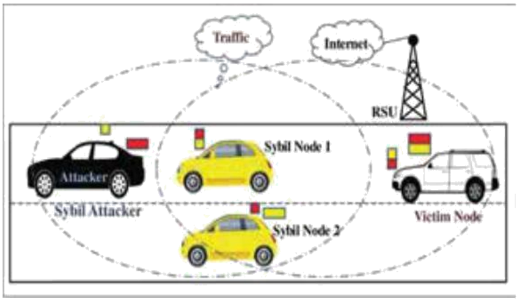


Fig.4 Vehicle to roadside unit (V2R) Communication

2. ATTACK TYPES AND SOLUTIONS

As the growth and expansion of VANET is increasing, the chance of safety concerning issues on moving nodes has been multiplied. Here is presented some of the well-known assaults on the matrix of moving nodes, their categorization with respect to their ambitions and procedures is also discussed.

2.1 Sybil attack

Sybil attack is regarded very hazardous assault in VANET. This kind of assault is concerned with the associating of more than one identity to a single node. A single node can have more than one identity. Because of this, other vehicular nodes in the matrix assume the information is coming from multiple nodes in the mesh or matrix. And they follow the information. The person who makes an assault changes the behavior of the network according to his wish. For instance, assaulter can deliver a message of a busy road to other moving nodes in the matrix, all the other nodes assume that this data is coming from multiple nodes but actually, it is coming from a single node which has more than one identity. These type of assaults are more challenging to be caught. Whenever a node is connected to the matrix it is given a unique identity which is different from the identities of the other moving nodes, so in Sybil assault a node starts to have multiple identities it means they become more than one node in the matrix. And other nodes assume that they are different node in the matrix. These assaults can be made stop by improving the sensor condition of the moving nodes. So the correct information about the node and the position of the node can be received.

2.2 Refusal of Service Assault

Refusal of service assaults is concerned with inaccessibility of certain legal services of a node in the matrix. If a person who assaults the system starts to send the solicitations in amount more than a system can handle then this type of assault is more likely to happen.

Communication is the key of the moving nodes matrix and sending right messages between nodes is the key of trusted communication. If communication breaks for any reason, whole matrix can be destroyed. So if more requests generated by the person who is assaulting the matrix are coming to the system, it may be hard for the system to handle and responded back to these requests in time, so load on matrix increases and communication link goes down. Now nodes cannot deliver the messages of busy roads or about the accidents to other nodes and the purpose of assaulter is fulfilled. The solution to stop this assault is to define a limit of the number of messages a node can send in a unit time to the matrix system. If the number of messages exceeds the maximum limit then it means node is the assaulter.

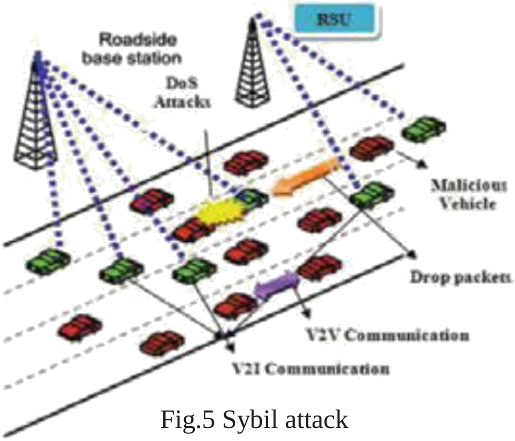


Fig.5 Sybil attack

2.3 Black hole Attack

While refusal of service assault is concerned with making communication link down between the nodes in the matrix, there is also another important sort of assault that can change the behavior of the matrix according to his own wish. In a black hole assault, the person who assaults the matrix enforces other nodes in the matrix to send the information through the assaulter node. All the useful information is now starts to deliver between vehicular nodes through the node of the assaulter. This sort of assault can be made stop if a node that is sending the information can monitor the node who is receiving the node. By monitoring each other these assaults can be minimized.

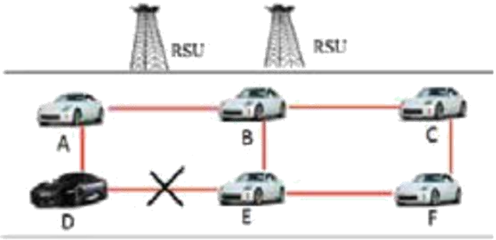


Fig.6 Black hole Attack

2.4 Worm hole attack

A wormhole assault is not carried out by a single node rather it is a combination of two or more than two nodes that are responsible for such assaults. These combinations of nodes claim that they are aware of the shortest route to any target. The purpose of the assaulter is to change behavior of the matrix so that he can gather and handle massive quantity of the matrix load. In the process of this sort of assault, the assaulter obtains a piece of information from a particular node, then changes the information and then delivers it to other nodes. The solution to this assault is that matrix administrator can define a limit of the distance between the sending and receiving nodes. If the distance between the sending and receiving nodes exceeds the maximum defined limit then it means it is suspected to have an assault.

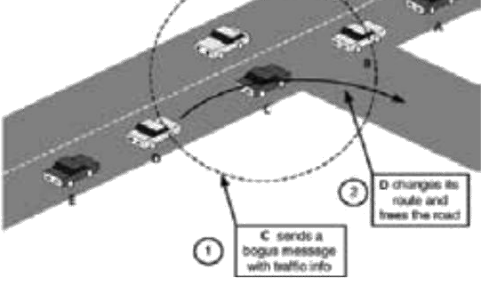

A
B
C
D
E
2
D changes its route and frees the road
1
C sends a bogus message with traffic info

Fig.7 Wormhole attack

Table. I Some Other Solutions On Attacks

S. No.	Solution	Attacks Covered	Technology used	Security Req .
1.	ARAN	1. Replay Attack 2. Impersonation 3.False Warning	1. Cryptographic Certificate	1. Authentication 2. Message Integrity 3. Non-Repudiation
2.	SMT	1. Information Disclosure	1. MAC (Message Authentication Code)	1. Authentication
3.	SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Availability 2. Authentication
4.	NDM	1. Information Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy
5.	ARIADNE	1. DoS 2. Routing Attack 3. Replay Attack	1. Symmetric Cryptography 2. MAC	1. Authentication

3. CONCLUSION

Safety measurements and methods that are applied on the guided matrices are not applicable on the VANET because the properties and feature of VANET are quite different for the guided matrices. The purpose of this study is to discuss the issues and problems of VANET, the type of assaults in the very matrix and proposed procedures and solutions. The assaults and the structure and reasons of the assaults are clearly discussed. This discussion represents the assaulters always try to utilize the matrix of moving nodes and the operation of how the matrix work. And the solutions to these attacks and procedure along with the advantages and disadvantages to stop these assaults are discussed in details. Whenever we move in an open matrix like VANET which is connected to the internet, chances of being assaulted by any attacker increases due to the very nature of the matrix. The intention of the assaulter is to hack the useful and personal information of the user and deliver the false information among the nodes in the matrix and to diminish the matrix. He or she can be attacked in many ways like the ones eh have discussed in this paper. However they can be made stop by some suitable approaches to stop the assaults or to minimize the chances of the assaults. Conclusively, assault or to find the unusual behavior of the nodes in VANET is very complicated and difficult study and methods and procedures for the safety of such assaults is even more complicated and a difficult task to perform. Computational intelligence-based procedures are suitable methods that might be traversed in coming time research for making the VANET safer.

4. REFERENCES

[1] J. Wan, J. Liu, Z. Shao, A. Vasilakos, M. Imran, and K. Zhou, "Mobile Crowd Sensing for Traffic Prediction in Internet of Vehicles," Sensors, vol. 16, no. 1, p. 88, Jan. 2016.

[2] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "AnonySense: Opportunistic and Privacy-Preserving Context Collection," in Pervasive Computing, vol. 5013, J. Indulska, D. J. Patterson, T. Rodden, and M. Ott, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 280–297.

[3] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Computer Communications, vol. 44, pp. 1–13, May 2014.

[4] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, “Fast exclusion of errant devices from vehicular networks,” in 2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2008, pp. 135–143.

[5] Deena M. Barakah , Muhammad Ammad-uddin , "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture," 2012.

[6] B. Yu, C.-Z. Xu, and B. Xiao, “Detecting Sybil attacks in VANETs,” Journal of Parallel and Distributed Computing, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[7] US Dept. Transp, Vehicle Safety Communications Project Task 3 Final Report, 2005.

[8] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “P2DAP-Sybil Attacks Detection in Vehicular Ad Hoc Networks,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 582–594, Mar. 2011.

[9] M. Kadam and S. Limkar, “Performance Investigation of DMV (Detecting Malicious Vehicle) and D&PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map,” in Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), 2013, pp. 379–387.

[10] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, “On data-centric misbehavior detection in VANETs,” in Vehicular technology conference (VTC Fall), 2011 IEEE, 2011, pp. 1–5.

[11] H. Sedjelmaci and S. M. Senouci, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks,” Computers & Electrical Engineering, vol. 43, pp. 33–47, 2015.

[12] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, “CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks,” Expert Systems with Applications, vol. 50, pp. 40–54, 2016.

[13] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, “Machine learning approach for multiple misbehavior detection in VANET,” in International Conference on Advances in Computing and Communications, 2011, pp. 644–653.

[14] A. Studer, M. Luk, and A. Perrig, “Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs,” in Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007, pp. 422–432.

[15] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, “Vehicle behavior analysis to enhance security in vanets,” in Proceedings of the 4thIEEEVehicle-to-Vehicle Communications Workshop (V2VCOM2008), 2008.

[16] S. Park, B. Aslam, D. Turgut, and C. C. Zou, “Defense against sybil attack in vehicular ad hoc network based on roadside unit support,” in MILCOM 2009-2009 IEEE Military Communications Conference, 2009, pp. 1–7.

[17] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “Privacy-preserving detection of sybil attacks in vehicular ad hoc networks,” in Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 2007, pp. 1–8.

[18] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

Nizami *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 1 January-March 2018

Introduction to Digital Forensics and Commonly Used Technologies

Syeda Marrium Nizami[1], Gulfraz Naqvi[2] and Tayyaba Sultana[3]
Lahore Garrison University
mariyum002@yahoo.com, gulfraz.naqvi@gmail.com, tayyabaanwar66@gmail.com

Abstract:

In this paper importance and usage of digital forensic is discussed. As the world is developing and moving towards technology new and better ways or investigation should be introduced. Investigating methods like foot prints are used but with old technology. The new method that is still not commonly used is discussed for awareness. The growth of cybercrime is increasing with advanced methods, to overcome this problem investigation teams should be given special trainings. This will not only reduce the crime but also precious time and money of investigation department.

Keywords: digital forensic, cyber, crime, technology, investigation.

1 Introduction

The description, restoration, examination and performance in court of related data taken from electronic devices such as Systems and mobile phone are included in Digital or computer [1] forensics. That data evolve into digital affirmation bestowed in court outlined to gather people in time and space to create origin for offence against the law. Example if a wife poisoned her husband and killed him. After arresting the suspect the police will examine her computer to view her online activities and the web pages that deal with poison. In this way police will reach to the evidence. Digital proof is not important. If it points to believe on the changes in crime the accused will face the punishment.[2] In some cases it can point the accuse to pay financial damage. And the crime department that testifies in court about digital proof can be the difference between justice dressed and justice declined.

2 Digital Forensic a scientific process

Digital Forensics can be defined as "Digital forensic is an application of computer science and investigative procedure for legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeat-ability, reporting, and possible expert presentation."

This scientific process contains the following terms:

2.1 Search authority

Search authority's examine the officers according to their work and abilities, and then assign then the cases. This is a very sensitive issue that is to be handled with care. Handing over the sensitive to an inexperienced and careless officer can lead to a big failure

2.2 Chain of custody

The process in which the evidence in documented collected and protected is called chain of custody. It is necessary for an evidence to be followed by chain of custody. When the evidences are found on the crime scene complete documentation is done including photography, note taking and sketching.

2.3 Imaging/hashing function

In an electronic crime hashing and imaging functions plays an important role in authenticating, discovering and examining the evidence. The arbitrary size data is converted to a fixed size using this function to quick data lookup as hash functions include hash tables.

2.4 Validated tools

Validated tool is an instrument used testing reliability of the results found where it is hard to trust the results. At such place reliability pays an important role. Then is validity that checks the capability of measure that is measured. The actual place to be examined is searched to find the criminal. After that is normative, that checks that is the information collected is true or not, by asking the same question from more than one person.

2.5 Analysis

The data is gathered using different tools. After gathering it is verified whether the collected information is true or not by using different functions then the analysis are made to reach the culprit.

2.6 Repeatability (Quality Assurance)

After the collecting the data and information, thee collected data is examined again and again so that if there is any false information that can be corrected immediately. This step plays an important role as a small mistake can result a heavy loss.

2.7 Reporting

Reporting means after analysis the reliable and valid data is grouped together in the form of a report that can be presented to the senior officers for discussion. This report is also useful for future cases, it can help the new officers to over look the old cases that happened before and how they were solved.

2.8 Possible expert presentation

As this whole investigation is not that easy, so after all the steps are followed to find the result at the end in this step the experienced experts make presentation that shows the evidences and the past cases for better results.

3 Forensic Computer and Digital Forensics

3.1 Working of forensic investigators

The analysis of digital data and solving computer related problems are done by forensic computer investigators and digital forensic experts. As the name implies forensic investigators investigate the crimes of hacking the source of hacking and the recovery of data. Their job includes the recovery of lost data, tracking hackers, collecting the evidences, making an investigation report, handling the electronics, teamwork and cooperation with detectives. Internal and external investigation is also done by the forensic investigators.

3.2 Education skills and Salary

Forensic investigators are sometimes fulltime or part time haired by the government and private sectors to investigate the hacking attack. It is necessary for the investigator to have a vast [3] knowledge regarding computer hardware and software. They must be familiar with the operating system, BOIS, Linux, Mac OS and windows. The education they required college education and specialized degree programs that are easily available in universities. They can major in the subjects like computer criminology. The reverent experience and knowledge regarding computer studies and hacking is acceptable for becoming a forensic investigator. Information technology, computing, criminal investigation, digital forensic experts certified hacking programs and criminology is suffice for forensic investigators. Their work is to interpret the data catch the hacker and recover the maximum loss that is possible. The salaries of forensic investigators are too high as it is a growing industry and the growth or usage of computers in rapidly increasing day by day. The per year wages of forensic investigators working in government or private sectors reaches up to fifty thousand dollar. They also work for private industries and firms on contrast so they need to be very expert in their jobs. They are not as regular because an [4] investigator can earn money per hour so working all the time is not necessary for them. Forensic investigators have different type of mood they enjoy problem solving and investigating. They never give up because they are so sure about their skills and knowledge in digging deep into a computer system. They are confident that come what may they will find a solution to that problem. [5]

4 Research Challenges

Research challenges describe the impact of forensic research in today’s life. Starting with the forensic tool, visibility and search model employed on it. Forensic researches are very expansive so new method should be introduced with the new technology produces better results on lower cost. There are two main problems with the today’s forensic tool

- These tools do not assist in investigation they were just designed to help investigator to find particular pieces of proofs.
- These tools do not investigate the crime committed on system or against the system; they just work against people where systems are used as proof.

Condition of today’s tool is that it was created to solve a pornography case not hacking one. [6] They are created to find proof where the control of proof in the crime itself. Today’s system can work on the case that contains data in terabytes but it cannot assemble that terabytes data into a report. These tools do not have the history of cases which is very helpful in new cases. Today’s tool needs changes in it to improve investigation and exploration. Because they are playing an important role in cyber defence and intelligence so their proper working is the basic necessity.

5 New research method

If the researchers are to be physically and mentally meaningful digital forensic in the coming era it needs to become more effective better related and better financially supported. These regular tools of the researchers are absorption and modularization. The important factors in cyber [7] researches are:

5.1 Computer forensic

Computer forensics or cyber forensics is defined as the use of investigative and analysis techniques, to gather evidence, to preserve evidence from any computing device in such a way that it can be presented to the court of law.

5.2 Network Forensics

Network forensics deals with the collection and analysis of packets over a network. It is collected for the purposes of information gathering, legal evidence, or intrusion detection. These packets are analysed and evidence is extracted in a scientific way to be support the investigation and if necessary, to present in the court of law.

5.3 Mobile forensics

The investigation process that is carried on mobile phone devices like PDAs, GPS, SIM cards, tablets etc. The process of Mobile forensics seems simple but it's not less complex than computer forensics. Same as computer forensics it starts from gathering electronic data for legal proceedings till the presentation of findings to the court of law. The process ranges from getting the data which is physically present on the device to the data which is deleted, this includes all the pictures, video, SMS, logs that are available on phone and anything which is deleted.

5.4 Digital forensic image

The bit by bit, sector by sector copy of a storage device is called forensics image, this copy everything that's within the storage device from a very small size file in Kilo bytes (KBs) to huge files in TB (Tera Bytes), the data in this copy includes all types of files and folders that are within the system. Moreover, this copy contains the slack spaces, free spaces or unallocated spaces that are within the hard drive, and the story doesn't ends here, it contains all the files that are visible and all files that are not visible, the files that were once part of the system or were installed or anyway existed in the system, indeed these files are the ones that were deleted anyway, but were not overwritten by any other data.

Forensics image is one of the most important element of computer forensics investigation. As soon as forensics image is taken from the place of incident, its hash value is generated, so that when its presented in court for legal proceeding the value should match the hash value of actual evidence so that process of litigation could be carried out.

5.5 Digital audio/video forensic

Audio forensics is defined as the process of acquiring, analysing, and evaluating sound recording gathered from any sound tracking source such as voicemail recordings, answering machines, telephone calls or any audio file present in tape or any medium which could be presented to court of law as an evidence for legal proceedings. Whereas video forensics refer to the investigation carried out on the evidence gathered in form of video. The video evidence could be from any source it could be from any CCTV footage from any mobile phone video recording or any video which could be presented to court to deal with legal matters.

5.6 Memory forensic

The process of analysing the memory is called memory forensics. Memory is analysed by checking the data that’s within the memory dump of the computer or in the volatile memory. When an investigation is carried out on a system, the experts usually take the memory dumps, so that they can keep record of the data which couldn’t be found in hard drive. Capturing of process running on RAM is also called live acquisition.

5.7 Computer technology skills

Digital forensic is study is technical field that can be understood by working on computer science and studding its background. A deep study of how technology works and what is its importance is important quality of a forensic investigator. A person is called a great forensic investigator who knows computer programming languages, knowledge of technology and networking, ways to interact with digital systems.

5.8 Cyber security

Solving the cyber issues like hacking cyber attack on firms this all belongs to the cyber crime so dealing with these issues called cyber security. The people deal in the cyber security is very intelligent and smart because to solve these issues one need to me very technical. Cyber security team consists of mentally strong members who enjoy problem solving.

5.9 Wireless Forensic

It’s a disciple within computer forensics, and specifically within network forensics field. The term wireless forensics was initiated by Marcus Ranum in 1997. The core purpose of this type of forensics is to collect, analyse and present the evidence gathered from network traffic to court of law. The evidence collected for wireless forensics can range from plain data to wide range of data collected from wireless technologies such as Voice over Internet Protocol (VoIP). The process of wireless forensics includes capturing of data that is transmitted over a network, analysing the network logs to unveil any abnormality that is within the network, monitor the source of the packet which may be the cause of attack.

While carrying out investigation on wireless network the security expert must keep this in mind that the same principle of computer forensics is applicable here as well, in which he has to identify evidence, preserve the evidence, and then he must make his analysis on it, which can be put to report form for further proceedings of the findings.

5.10 GPS Forensic

GPS stands for Global Positioning System. GPS devises plays a meaningful role in crime investigation to find the evidences. GPS information in GPS Forensic cases can provide such evidence that can turn over the whole plan of criminal. Today GPS is used in almost all mobile phones like smart phones, PDAs, tablets, etc that can provide the investigator with the location of criminal, first journey, last journey, current location, date and time, deleted data and even the details of mobile phones that are paired.

5.11 Malware Detection System

One of the necessity of systems these days is to have a malware detection system. Malware is mixture of basically two words malicious, and software. Malwares are widely used by the hacker for several means, there are some malwares which just corrupts the files, or delete the files, whereas there are some malwares which enters the system to encrypt the files that are within the systems, depending on the situation to which malware is designed. The situation where files are encrypted the hackers ask for ransom. So there is a need of system that should detect this malicious software in order to make our data protected, and data transmission more secure. There are several renowned organisation working days and nights to come up with system which can detect malwares, and could make processes smoother.

5.12 Password Recovery

Since 1998 the security forces electronic crime department and law enforcements are working together work on a serious issue that is to develop software that can recover the password. Password recovery software is not an ordinary thing. Sometimes a system having all the important and meaningful evidences are protected with a strong password that can be opened by the user only. But today the digital forensic researchers and investigators have made such software that can recover the password like Passware Kit Enterprise, Encryption Analyzer Professional, Passware Kit Forensic, Search Index Examiner etc. The password recovery can also be done without using software; there are also some techniques for this purpose.

5.13 Stenography

The art of hiding data within data is called steganography. Among many other encryption techniques, steganography is the one which is widely used to protect data.

In modern world steganography is widely practiced by hiding data within images, video, audio files etc.

5.14 Data recovery from serious damaged hard drive

To conduct an exclusive investigation the most meaningful evidence that can simplify the case is deleted data. Time age retrieving the lost data was almost impossible. But today the digital forensic methodologies make this impossible task possible. They have introduced with the techniques that can recover the lost and important data. Criminals always clean all the evidences that can be caught and the most important is the crime related information. The easiest task was to delete the data permanently from the drive and the criminal is safe. But this system is totally changed today by the help of digital forensic techniques the deleted or lost data can be easily retrieved.

6 Conclusion

This papers explains the concept of digital forensics and the type of technologies available to analyse a digital evidence collected by forensic team. Digital evidences are becoming increasingly important with the passage of time. In modern days many crimes are being solved with the help of digital evidences. It is very important to analyse the digital evidences carefully and reach to a conclusion through a scientific process.

Governments in most of the countries have passed laws pertaining to digital evidence. In Pakistan, Prevention of Electronic Crime Act (PECA) was approved by national assembly in August, 2016. Proper implementation of digital evidence analysis procedures and choice of right technologies ensures the proper conclusion of an investigation.

This paper explains the digital forensics evidence processing process and some of the technologies available to process the evidence.

7. References

[1] I.D.E.A.L. Technology Corporation. STRIKE (System for TRIaging Key Evidence), http://www.idealcorp.com/; 2010.

[2] Kanich Chris, Kreibich Christian, Levchenko Kirill, Enright Brandon, Voelker Geoffrey M, Paxson Vern, Savage Stefan. Spamalytics: an empirical analysis of spam marketing conversion. Commun ACM 2009;52(9). ISSN: 0001-0782:99e107. https://www.forbes.com/sites/laurencebradford/2017/04/29/6-skills-required-for-a-career-in-digital-forensics/#606402307fa6

[3] Lyle Jim. The CFReDS project, http://www.cfreds.nist.gov/; 2008. McCanne Steven, Jacobson Van. The bsd packet filter: a new architecture for user-level packet capture. In: Proceedings of the USENIX Winter 1993 conference. Berkeley, CA, USA: USENIX Association; 1993. p. 2. https://www.thebalance.com/digital-forensics-job-and-salary-information-974469

[4] Mocas Sarah. Building theoretical underpinnings for digital forensics research. Digit Invest 2004;1:61e8. Nance Kara, Hay Brian, Bishop Matt. Digital forensics: defining a research agenda. In: Proceedings of the 42nd Hawaii international conference on system sciences; 2009 https://www.interworks.com/blog/bstephens/2016/02/05/what-digital-forensics

[5] Nicholas Mikus. An analysis of disc carving techniques. Master's thesis, Naval Postgraduate School, March 2005. http://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3

[6] Opinion by Chief Judge Kozinski. 11860 us v. Comprehensive Drug Testing, Inc, http://www.ca9.uscourts.gov/datastore/opinions/2009/08/26/05-10067eb.pdf; August 2009. https://www.thebalance.com/digital-forensics-job-and-salary-information-974469

[7] Pollitt Mark, Nance Kara, Hay Brian, Dodge Ronald C, p Craiger Phili, Burke Paul, Marberry Chris, Brubaker Bryan. Virtualization and digital forensics: a research and education agenda. J Digit Forensic Pract 2008;2(2). ISSN: 1556-7281:62e73.

[8] Pollitt Mark M. An ad hoc review of digital forensic models. In: Proceedings of the second international workshop on systematic approaches to digital forensic engineering (SADFE'07); 2007. https://www.thebalance.com/how-to-become-a -digital-forensic-examiner-974633

[9] Saltzer Jerome H, Frans Kaashoek M. Principles of computer system design: an introduction. Morgan Kaufmann;
2009. Sencar Husrev, Memon Nasir. In: Identification and recovery of jpeg files with missing fragments, vol. 6; 2009, http://www. frws.org/2009/proceedings; 2009.

[10] Shelton Donald E. The 'CSI Effect': does it really exist? NIJ J March 2008;259, http://www.ojp.usdoj.gov/nij/journals/259/csieffect.htm.

[11] Turnbull Benjamin, Taylor Robert, Blundell Barry. The anatomy of electronic evidence aˆ quantitative analysis of police e-crime data. In: International conference on availability, reliability and security, (ARES '09); March 16e19 2009. p. 143e9. Fukuoka. Using purpose-built functions and block hashes to enable small block and sub-file forensics. In: DFRWS 2010,
2010. https://www.thebalance.com/digital-forensics-job-and-salary-information-974469

[12] Wood Charles Cresson, Banks William W, Guarro Sergio B, Garcia Abel A, Hampel Viktor E, Sartorio Henry P. In: Garcia Abel A, editor. Computer security: a comprehensive controls checklist. John Wiley & Sons; 1987. https://theconversation.com/footwear-forensics-device-could-catch-criminals-who-put-a-foot-wrong-54984

Alyas *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 1 January-March 2018

Data Breaches Security Issues for Cloud Based Internet of Things

Tahir Alyas [1], Nadia Tabassum[2], Sagheer Abbas[3] , Atifa Ather[4]
Lahore Garrison University tahiralyas@lgu.edu.pk[1]
Virtual University of Pakistan, nadiatabassum@vu.edu.pk[2]
National college of business Administration & Economics, Lahore, Pakistan dr.sagheer@ncbae.edu.pk[3]
Comsats institute of information technology, atifaathar@ciitlahore.edu.pk[4]

Abstract:
Now a day's Internet of Things (IoT) and cloud computing are latest popular technologies. Both technologies have great role in our life. Their adoption and utilization are relied upon increasingly inescapable and making them vital segments of the Future Internet. A novel worldview where Cloud and IoT are consolidated and would be helpful for large number of application scenarios. Security in cloud computing and IoT truly challenging, needs a watchful comprehension and it includes numerous zones. Protections of cloud situations can be more powerful, versatile and have a superior financially savvy, yet the vast centralization of assets and information is a more appealing focus for aggressors. In this paper, data breaches architecture for the next generation technologies on cloud-based IoT will be introduced which will address the challenging issues of data breaches in cloud base system.

Keywords: Cloud computing, Resource Pooling, Rapid Elasticity, Public cloud, Hybrid cloud.

1 Cloud computing

Cloud computing is a storage medium and the platform where we can store data and files over internet, it is a medium where data remains more secure and threat free, by using cloud system we can access any of our document or website from anywhere through internet. Cloud computing is a system that allow us to compute and arrange our data and information more quickly and securely and it can be accessed by user no matter where he is, the only requirement to accessing data is associated with the availability of internet. [1].

Cloud computing provides users a platform where he can store his data easily and conveniently. Cloud computing is also convenient in a sense that if user wants to share his/her data or information with someone, he can simply allow him/her accessibility without requiring any hard device.

1.1. Cloud Computing Architecture

Cloud computing architecture is the framework or the total design of cloud computing. Cloud actually consist of all the important characteristics of client server websites like it has a front end, back end and the interface that is used by its clients to communicate like internet and cloud internet.

1.2. Essential characteristics of Cloud Computing:

Some of the most important characters of cloud computing is following:

1.2.1. On-Demand Service

On-demand service is a model or technique in which we just provide facility to cloud users so they can get services from services providers irrespective of time and place, providing availability of internet service to user. The user can facilitate from this service for completion of his tasks. The main purpose of this modal is to enhance the liberty of client so he can avail services on his demand at any place or time. To avoid all the issues or any difficulty we just provide this facility to user on his demand, it means any person or organization can get this facility to avail its project that is more depending on the services or the resources required for the maintenance of that organization or company.

1.2.2. Broad Network Access:

Cloud system is just used in broad network area so that everyone can access services. Most of the companies can use this facility to remain updated for clients or other organizations by using the cloud services and anyone can use these services but it is dependent on the network used like whether it is private or public? if you use the private cloud then all the information will be under the members of the private cloud who are sign in to the cloud services but, if it is public network than anyone can access information and can benefits from services provided to the cloud users. Disadvantage associated with public network arises if you just left to log out you id then your project information can leak out and you may have to face many severe issues related to data security

1.2.3. Resource Pooling:

Resource pooling is a technique in which the consumer can acquire and release the resource when it will be required on demand. The PaaS users can get the resource from the resource pool on demand so that the user can make use of this resource and then give it back to the resource pool. It also reduces all the complexities that cloud has to face by using resource-pooling techniques.

1.2.4. Rapid Elasticity:

Rapid Elasticity is one of the characteristics of the cloud computing in which the cloud or cloud service providers provide their users and buyers all the services in a very reliable and flexible manner. Cloud provides their services to users very easily and their users can easily get the services on demand. The cloud users can have extra storage space to have more resources from cloud provider in order to enhance services which was not possible before because system was complicated and less advance. Now if somebody needs to use the cloud system can also get the extra storage space.

1.2.5. Measured Service Problem Statements:

Measured service problem is one of the most critical features of cloud computing in which work on all the problems and all the faults faced by clients occurred from the services provided. Measured service is a term that IT experts apply to distribute computing. To have the total measurement about the usage of the resources used in different places to made much application. The idea of measured service is a definition of cloud computing which is supported by National Institute of Standard and technology or NIST.

1.3. Cloud Service Models:

The most commonly used service models through which the cloud system provides different services to the users consumers are following:

1.3.1. Infrastructure-as-a-Service (IaaS):

Infrastructure is just like a support or foundation which is used to provide these type of services to your customers and cloud users like by using infrastructure u can give resources to the equipment’s that are used in different works like virtualization, storage area, networking etc. You can easily offer these resources or facilities to your customers and cloud buyers and users to enhance your services provided to the customers. You can increase your storage area and the network speed provided to the customers so that they can easily use the benefits of the best networking speed available.

1.4 Cloud Deployment Models

1.4.1 Private cloud:

A private cloud is a particular model of circulated computing that incorporates a specific and secure cloud based condition in which simply the foreordained client can work. Likewise as with other cloud models, private fogs will give figuring power as an organization inside a virtualized space using an essential pool of physical handling resource. In private cloud resource pool of cloud services is subject to affiliation for significant control and security [3].

1.4.2 Public cloud:

The most unmistakable model of disseminated computing to various clients is the overall public cloud show, under which cloud organizations are given in a virtualized circumstance, created using pooled shared physical resources and accessible over an open framework, for instance, the web. In public cloud pool resources influencing an unpredictable situations and using shared services.

1.4.3 Hybrid cloud:

A mixture cloud is a consolidated cloud advantage utilizing both private and open clouds to perform specific limits inside a comparative affiliation. All disseminated computing organizations offer certain effectiveness to different degrees; yet open cloud organizations are most likely going to be more affordable and flexible than private clouds. In this way, an affiliation can extend their effectiveness by using open cloud organizations for all non-sensitive operations, simply relying upon a private cloud where they require it and ensuring that most of their stages are faultlessly planned.

1.4.4 Community cloud:

A social order cloud in figuring is a community effort in which system is shared between a couple of relationship from a specific gathering with fundamental concerns (security, consistence, ward, et cetera.), paying little attention to whether administered inside or by an untouchable and encouraged inside or remotely. This is controlled and used by social affairs of affiliations that have shared interest. The costs are spread over less customers than an open cloud (however more than a private cloud), so only a segment of the cost speculation reserves ability of circulated computing are made sense of it.

1.5 IoT Based Cloud system

The Next revolution in the period of figuring will be changing in contrast with customary demand base requirement and things placed everywhere. Many technologies encompasses the human clients will be on the system in one frame or in another frame in the Cloud Computing and Internet of Things structure. Distributed computing and Internet of Things are two distinctive advancements, these are into our everyday life [4].

1.5.1 Data breaches in cloud system

An information break is an episode in which touchy, ensured or secret information has conceivably been seen, stolen or utilized by an individual unapproved to do as such. Information breaks may include individual data or identifiable data exchange mysteries or licensed innovation [5].

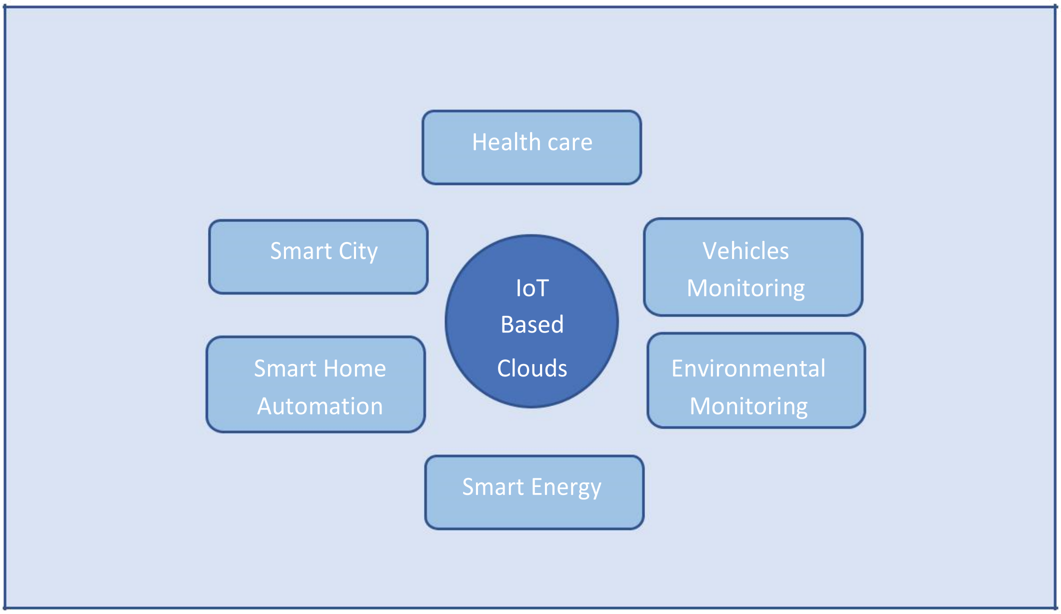


Figure 1. IoT based Cloud System

There are different ways a breach can happen in cloud computing

� Accessing data via malware
� Snuffing private cloud passwords
� employee negligence
� policy failure

An information break happens when there is an "unapproved access to delicate, ensured, or private information". Information ruptures ordinarily have negative outcomes for the business and people included. An information rupture triggers inquiries regarding the earlier cautioning signs, the occasion itself, and the required stance post the information rupture.

1.5.2 Data breach Challenges

The following will be data breaches challenges in IoT based clouds system.

� Privacy
� Security
� Legal aspect
� Social Aspect
� Reliability
� Performance

2 Literature Review

Nowadays, Cloud computing is a proceeding sector that focuses at contributing every type of service on requirement anytime and everywhere. Advancement in this sector has promoted an innovative cooperative cloud in which various inter-dependent clouds offer ascendable services. This paper goal to choose the Trustworthy Service Provider (TSP) by estimating trust based on surroundings assessment from individual authority; these authorities involve third-party feedback, universal consulting feedback and user feedback. As well as, un- fair feedback is clarifying to advance reliability. The multifaceted trust management framework promotes the assortment of a TSP. First of all, to increase the achievement velocity of the job, secondly, to enhance the dignity of the revenue built by the contributor to the users. Thirdly, to increase the standard of service to the users by offering stable service [6].

3 Proposed methodology

Online Reputation networks assist reduce the information imbalance between customers and contributor in Cloud Computing organizations. This paper defines a reputation model that treats with few open problems in up-to-date. First of all, we can provide a peer to peer structure for proceedings with the price of distribution concentrate reputation services, which can be a better design for other organization but not for cloud computing. Secondly, we defined a mathematical model to compute the trust contact from a customer to a contributor. The model too explains trust relationship between updates and peers them to utilize the statistical survey to discover the dependability of their records. Moreover, the reputation and layer.In this environment, various data breaches challenges are there in the form of Privacy, Security, Legal aspect, Social Aspect, Reliability and Performance in IoT based devices like RFID tags, cameras, RFID readers, intelligent sensors, smart meters and intelligent device. These Iot base devices are capable to sense the data breaches and can handle these challenges through security policies layer.

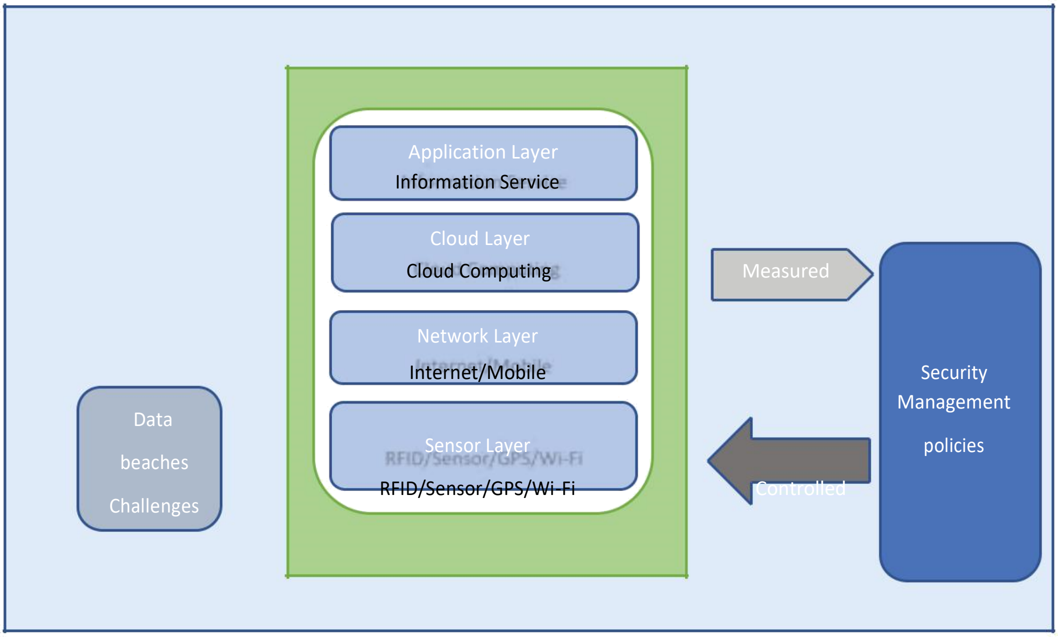


Figure 2. Proposed framework for Data Breaches Security

The middle module is further consisting of four layers, sensor layers, network layers, cloud layer and application layer. Sensing layer is capable to sense the environment of data breaches and communicate it to network layer, this layer will work like bridge between two layers sensing layer and cloud layer. All the data on clouds will route through network layer, the data in cloud can be infrastructure as a service, platform as a service and software as a service or anything as a service will be routed through network layer. In cloud environment, the cloud system management, device management, heterogeneity management, cloud monitoring management, deployment management in clouds can be affected through data breaches security challenges.

Policy and security management are crucial challenge for virtualized network to put up IOT traffic economically and efficiently.

Overall, as societies are going to be more reliant on the uninterrupted and genuine working of IT systems, Internet and communication networks, thus the consequences of successful cyberattacks, these malicious, criminal in nature have become very serious. The possible vulnerabilities can be measured like insecure web interface, poor authorization, insecure different networks, poor encryption, privacy related concerns, insecure cloud/mobile interface, less security configurability and poor physical security. The above-mentioned vulnerabilities cab be controlled by measured policies.

4 Conclusion

We proposed a data breach security model for cloud service providers to identify given parameters of most concern to security challenges in IoT Based clouds system. In this model, information leakages for cloud service providers, empowering clients to recognize parameters are of most worry to them and give a weighting capacity. Multi-characteristic parameters of security issues that are most essential for information break hazard will be shifting in light of security SLAs and in addition in view of customers prerequisites.

5 References

[1] P. R. Pratim , "A survey of IoT cloud platforms," Future Computing and Informatics, pp. 35-46, 2016.

[2] I. Addor and S. Ahamed, "REFERENCE ARCHITECTURES FOR PRIVACY PRESERVATION IN CLOUD-BASED IOT APPLICATIONS," International Journal of Services Computing, pp. 65-79, 2014.

[3] "Integration of Cloud computing and Internet of Things: A survey," Future Generation Computer Systems, pp. 684-700, 2016.

[4] S. Mohanty,, "Everything You Wanted to Know About Smart Cities," IEEE Consumer Electronics Magazine, 2017.

[5] Y. Rahulamathavan and M. Rajarajan, "Assessing Data Breach Risk in Cloud Systems," in *7th International Conference on Cloud Computing Technology and Science*, 2015.

[6] A. Kornfeld Simpson and F. Roesner, "Securing Vulnerable Home IoT Devices with an In-Hub Security Manager," *The First International Workshop on Pervasive Smart Living Spaces*, 2017. [7] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru, “REFERENCE ARCHITECTURES FOR PRIVACY PRESERVATION IN CLOUD - BASED IoT APPLICATIONS (EXTENDED VERSION OF 7398 AT MS 2014),” vol. 2, no. 4, pp. 65–78, 2014.

[8] S. M. Babu, A. J. Lakshmi, and B. T. Rao, “A study on cloud based Internet of Things: CloudIoT,” *2015 Glob. Conf. Commun. Technol.*, no. Gcct, pp. 60–65, 2015.

[9] Y. Rahulamathavan, M. Rajarajan, O. F. Rana, M. S. Awan, P. Burnap, and S. K. Das, “Assessing data breach risk in cloud systems,” *Proc. - IEEE 7th Int. Conf. Cloud Comput. Technol. Sci. CloudCom 2015*, pp. 363–370, 2016.

[10] A. K. Simpson, F. Roesner, and T. Kohno, “Securing vulnerable home IoT devices with an in-hub security manager,” *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 551–556, 2017.

[11] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, 2017.

Sultana *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 1 January-March 2018

Information Security with Cryptography

Tayyaba Sultana[1] , Zaka Ullah[2] , Muhammad Zulkifl Hasan[3], Taimoor Hassan[4]
Department of Computer Science
Lahore Garrison University, Lahore, Pakistan
tayyabaanwar66@gmail.com,zakaullah@lgu.edu.pk,
Zulkifl.hasan@lgu.edu.pk,taimoorhassan@lgu.edu.pk

Abstract:

The purpose of Information Security and Cryptography is to secure the data transmission and network over wireless network. The main feature of data Security is to protect transmission of data over unsecure network. The authorization of access over the data within the network is included in Information Security and which is managed by the administration of network. The users are authorized and have their own ID and password or may be some other validating information which permits them to access the programs and information under their limited authority. Diversity of computer networks is covered by information Security, private and public both, which are used in daily routine jobs directing communications and transactions among individuals, businesses and government agencies. Network might be open for the public to access or they can be private like within a company. Businesses, organizations and other kind of institutions are covered by Information Security. We will study about the cryptography and its principles in this paper. Cryptographic systems with ciphers are presented. The cryptographic algorithms and models are outlined.

Keywords: ID, Diffie Hellman, eavesdrop, Ciphers, Cryptography, IS.

1 Introduction

The most important factor of information security is cryptography because its responsibility is to secure all the information delivered by the networked computers. Information Security denotes to all software and hardware programs, features, characteristics, accountability, operational procedures, access control, measures, management, administrative policy needed to give an adequate level of security for Software, Hardware, and network information. The problems of Information Security can be categorized into four closely knotted areas: nonrepudiation, authentication, integrity control, and secrecy. Secrecy in other words, confidentiality has to do with securing information from unauthenticated users. This is the major thing which is considered when people think about Information Security.

Authentication or verification deals with finding whom you are talking before telling any critical information or making a business deal. Signatures are referred by nonrepudiation. Message reliability: However, the receiver and sender can verify each other, they also wish to make sure that the material of their conversation is not changed either by accident or meanly, in the transmission. Extensions to verify summing techniques that we faced in a secure transport and data link protocols. Cryptography is very essential for Information Security which is an evolving technology. The transmission and processing produces delicate, the extensive use of computerized data storage, in storage and transmission the personal and worthy information is susceptible to the unauthenticated access. Because of ongoing progressions in spying and communication technologies, private individuals and business organizations are starting to secure their information.

In networks and computer systems using different techniques of cryptographic, which until very freshly, were solely utilized by the diplomatic and military communities. Cryptography is dynamic of communication and computer networks of today, securing everything from email of business to transactions of bank and online shopping while modern and classical cryptography employ different techniques of Math to evade listeners from learning the data of messages which are encrypted. Computer networks and systems are required security against such unauthenticated access while processing, storing, and communicating critical and worthy information [1]. Some form of encryption is the only common method for storing and sending data over the media, which are unreliable. The major concern is that most of the attacks contain secret methods of access to information sources, and organizations and corporates are not aware of unauthenticated access to their information systems. The quantum cryptography is used for that purpose. The quantum cryptography security preserves in its capability to interchange the key of encryption with absolute security. Cryptography has its foundation in the antique world. According to [7], a very simple cryptography was used by the Julius Caesar to hide the meaning of messages. According to [7], the Caesar cipher is an analphabetic cryptosystem, hence it replicated each provided plain letter of text, wherever in the real message it happens, by the same cipher text letter alphabet. Though the ideas of receiver and source, and channel codes are advance concepts that have their origins in the information theory. In 1948, Claude Shannon proposed a theory of information based on secrecy, which states that the value of ambiguity that can be presented into a message in encoded form cannot be larger than that of the key of cryptography used for its encoding

[9]. In 1949, Claude Shannon proposed this idea of communication security. It indicates that a scheme of encryption is strongly protect if, for any two messages M1 and M2, any cipher-text C has the same possibility of being the encryption of M1 as being the encryption of M2 [6]. Two major and essential cryptographic ideas was developed by Shannon: diffusion and confusion. According to Salomon[8], any approach that created the numerical relationship between the cipher-text and the key as difficult as possible can be defined as confusion, and diffusion can be stated as a common term for any technique of encryption that extends the numerical characteristics of the plain text over a variety of bits of the cipher-text.

2 Cryptographic Principles

Redundancy Cryptographic principle 1: all messages which are encrypted must consist of some redundancy which is first principle, that is, information not required to understand the message. Message should have some redundancy.

Freshness Cryptographic principle 2: there is a need of some approach to stop the repetitive attacks. One that extent is comprising in every message timestamp effective only for, say, 10 seconds. The receiver can keep messages let's say for almost 10 seconds, to relate new messages with old messages to validate duplicates. The messages can be thrown out which are older than 10 seconds, however any replays delivered more than 10 seconds will be prohibited as too old.

3 Cryptosystem Types

Commonly cryptosystems are classified into two categories, symmetric and asymmetric, which depends only on whether the key at the receiver and at the transmitter are comfortably computer from each other. A different key is used for the purpose of encryption and decryption in asymmetric cryptography algorithm, Bob and Alice can share the same key (K) in the symmetric which is not known to the attackers, and uses it to decrypt and encrypt their channel of communications.

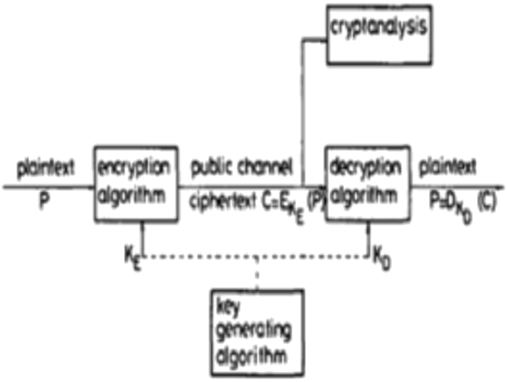


Fig. 1 General secrecy system

Cryptographic systems are used to give authentication and security in communication and computer systems.

As shown in Fig. 1, encryption algorithms encipher the plaintext, or clear messages, into inarticulate cipher text or cryptograms using a key. In order to restore the original information, a deciphering algorithm is used for decipherment or decryption. Ciphers are cryptographic algorithms; cryptography is the science of secure communications; cryptanalysis is the science of breaking ciphers; and cryptology is the science of cryptanalysis and cryptography. Cryptosystems are either symmetric, in which both the cases deciphering and enciphering keys should be kept secure, or asymmetric, in which case one of the keys may be made open public without conceding the other.

Asymmetric cryptosystems there are everyday problems related with the security, distribution and generation of a great amount of keys. Hellman and Diffie provided the solution to this problem of key distribution in 1976 [10]. A kind of cipher which uses two different key was presented: one key of enciphering made open public and the other one of deciphering is kept secret and secure.

The two keys are produced like that it is very hard computationally to reach the secret key from the open public key. if first user wishes to connect with the second user to encipher the data, first user can use public key of second user (from a public directory). Since second user owns the secret key of deciphering, only second user can decipher the cipher text. Above mention scheme is known as asymmetric cryptosystem or public-key cryptosystem [11]. After satisfaction of confirm restrictions by asymmetric algorithms, they can also be utilized for producing supposed digital signatures [12].

Symmetric cryptosystems the deciphering or enciphering keys are either same or simple connected in symmetric cryptosystems (also named as one-key cryptosystems or conventional secret-key) i.e. 684 *IEE PROCEEDINGS, Vol. 131, Pt. F, No. 7, DECEMBER 1984* one of them can be comfortably derived from the other. It is necessary to keep the both keys secret, further protected communication is not possible if either is conceded. Keys must be interchanged between users, regularly over a poor protected channel, the numbers of keys and a private courier can be very huge, if all users pair needs a separate key, even for a restrained number of users, i-e n(n-1)/2 for n users. This will produce a problem of key distribution which is partly resolved in the asymmetric systems. The DES (data encryption standard) [4] and rotor ciphers are the examples of symmetric systems.

4 Cryptographic Model and Algorithm

Encryption model following are the two models of encryption: one is symmetric encryption and other is Asymmetric encryption. Encryption key is equals to Decryption key in Symmetric encryption. While for Asymmetric encryption, Encryption key Decryption key.

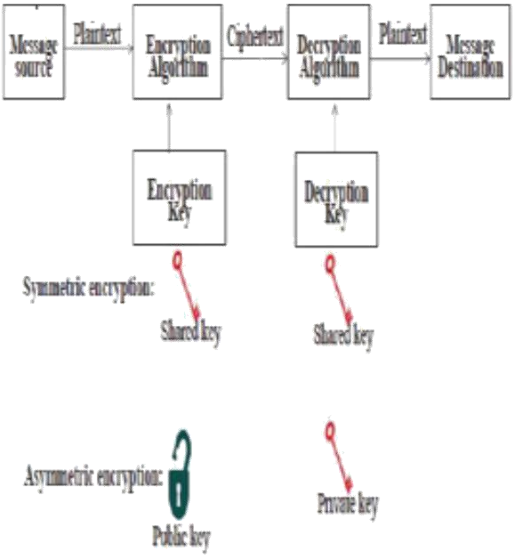


Fig 2: Cryptography

Algorithm there are a huge variety of useful cryptographic algorithms. The most well-known are as follows:

1) **DES*:*** this stands for 'Data Encryption Standard'. This uses a 56-bit key and operates on 64-bits block of data, and it is actually a cipher. It is a system of 'private key'. Furthermore about the DES algorithm.

2) **RSA:** Adleman, Rivest, and Shamir design this public key system known as RSA. Furthermore about the RSA algorithm

3) **HASH*:*** the purpose of using a 'hash algorithm' is to computer a reduced demonstration of a message of fixed length. This is occasionally called as a 'fingerprint' or a 'message digest'.

4) **MD5*:*** it is a message digest function of 128-bit. Ron Rivest developed MD5. Furthermore about the MD5 algorithm.

5) **AES:** This is the modern Encryption Standard (using the Rijndael block cipher) permitted by NIST.

6) **SHA-*1:*** SHA-1 produces a digest of 160 bits and it is also an algorithm of hashing alike in structure to MD5. It is less possible that two various messages will keep the same SHA-1 message digest because of large size of digest. Because of this reason, SHA-1 is preferred to MD5.

7) **HMAC*:*** it is also a hashing approach that utilizes a key in aggregation with an algorithm such as SHA-1 or MD5. Thus one can denote to HMAC-SHA1 and HMAC-MD5.

5 Conclusion

Information Security is the very important factor in information security the reason is it is accountable for protecting all the information over the networked computers. Information Security contains the comestibles created in a fundamental computer network organization, plans assumed by the administration of network to secure the network first and then the resourced which are accessible by network from unauthenticated access, and frequent monitoring and measurement and reliable of its efficiency or lack pooled together. There are a lot of different cryptographic techniques to increase the protection of a network. Cryptography, jointly with the relevant communication protocols, can give a high range of security in digital communication against stalker attacks as far as the communication between two separate computers is concerned.

6 References

[1] DENNING, D., and DENNING, P.J.: 'Data security', ACM Comput. Surveys, 1979, 11, pp. 227-250

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[4] 'Data encyption standard', FIPS PUB 46, National Bureau of Standards, Washington, DC Jan. 1977

[5] Murat Fiskiran, Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Information Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[6] Coron, J. S. , "What is cryptography?", IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.

[7] Pfleeger, C. P., & Pfleeger, S. L.," Security in Computing", Upper Saddle River, NJ: Prentice Hall.2003.

[8] Salomon, D., "Coding for Data and Computer Communications", New York, NY: Spring Science and Business Media. 2005.

[9] Shannon, E. C.," Communication theory of secrecy system", Bell System Technical Journal, Vol.28, No.4, 1949, pp.656- 715.

[10] DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', IEEE Trans., 1976, IT-22, pp. 644-654

[11] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, 11, pp. 305-330

[12] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126

[13] Algorithms: http://www. cryptographyworld. com/algo.htm

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